Lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo de aplicaciones web y la gestión de riesgos de seguridad de la información publicada en el ciberespacio de la Fiscalía General de la Nación

Samuel Páez Pisco

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2020

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA

LINEAMIENTOS ESTRATEGICOS DE CIBERSEGURIDAD Y CIBERDEFENSA PARA EL DESARROLLO DE APLICACIONES WEB Y LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PUBLICADA EN EL CIBERESPACIO DE LA FISCALIA GENERAL DE LA NACION

ALUMNO:

SAMUEL PAEZ PISCO

DIRECTOR:

MANUEL HUMBERTO SANTANDER.

GRUPO DE INVESTIGACION
MASA CRÍTICA

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO

BOGOTA – COLOMBIA

2020

MINISTERIO DE DEFENSA NACIONAL

COMANDO GENERAL FUERZAS MILITARES

ESCUELA SUPERIOR DE GUERRA

LINEAMIENTOS ESTRATEGICOS DE CIBERSEGURIDAD Y CIBERDEFENSA PARA EL DESARROLLO DE APLICACIONES WEB Y LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PUBLICADA EN EL CIBERESPACIO DE LA FISCALIA GENERAL DE LA NACION

ALUMNO:

SAMUEL PAEZ PISCO

DIRECTOR:

MANUEL HUMBERTO SANTANDER.

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR EL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTA – COLOMBIA

Contenido

Índice de Tablas.

Índice de Figuras.

RESUMEN EJECUTIVO.

En esta investigación se realiza un análisis descriptivo para la formulación de lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo de aplicaciones web que automatizan los procesos y procedimientos de publicación de información la Fiscalía General de la Nación en el ciberespacio como parte de su gestión. Para esto, este trabajo se basa en las recomendaciones dadas por la OWASP, (Novillo Vicuña J. P., 2019) aplicado en el ciclo de vida de las aplicaciones web y con los lineamientos estratégicos de la entidad como parte del desarrollo tecnológico de los sistemas de información con que cuenta la Fiscalía General de la Nación y ha permitido acercar diferentes servicios a la comunidad enmarcados en el direccionamiento estratégico institucional y que requieren de un análisis de riesgos cibernéticos como requisito para la implementación en el ciberespacio de servicios tecnológicos que hace parte del objetivo estratégico No 4. Mejorar el acceso a la justicia y los objetivos de gestión No 2. Fortalecer la infraestructura tecnológica, así como el No 3. Optimizar los procesos y fortalecer el Sistema de Gestión Integral. (Nación, 2016). Como resultado de este análisis, se formulan lineamientos estratégicos para el desarrollo seguro de aplicaciones web de la Fiscalía General de la Nación.

Abstract.

This research performs a descriptive analysis for the formulation of strategic guidelines for cybersecurity and cyberdefense for the development of web applications that automate the processes and procedures of the Attorney General's Office as part of their management and they generate information publishing services in cyberspace. For this, this work is based on the

recommendations given by OWASP, (Novillo Vicuña J.P., 2019) and related to the life cycle of web applications and the strategic guidelines of the entity as part of the technological development that has been achieved with the implementation of the different projects to strengthen and maintain the information systems that the Attorney General's Office has and has allowed to bring different services to the community through the use of public networks such as the Internet as the main means of dissemination included in action plans framed in strategic addressing that require a cyber risk analysis as a requirement for the implementation in cyberspace of technology services that is part of the strategic objective No. 4. Improving access to justice and management objectives No. 2. Strengthen the technological infrastructure, as well as No. 3. Optimize processes and strengthen the Integral Management System. (Nation, 2016). As a result of this analysis, strategic guidelines are formulated for the safe development of web applications of the Attorney General's Office of the Nation.

Palabras Clave. Strategy, System Information, development of web application.

Introducción.

Con la gestión de riesgos de la publicación de información de la Fiscalía General de la Nación en el ciberespacio, se requiere contar con unos lineamientos estratégicos en materia de ciberseguridad y ciberdefensa para el desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio, es decir, que se asegure el proceso de desarrollo aplicaciones web enmarcado en las directrices dadas por la arquitectura empresarial instituida y que permiten apoyar el cumplimiento de la misión, visión y procesos establecidos; en cumplimiento de políticas y procedimientos del Sistema de Gestión de Seguridad de la

Información que soporte la formulación y la implementación de controles para atender las características de disponibilidad, confidencialidad e integridad tanto de la información como en los servicios que la entidad relacionados con los procesos misionales como lo son: atención a víctimas, protección y asistencia, extinción de derecho de dominio, investigación y judicialización, así como la justicia transicional.

En este sentido, en este trabajo se plantea el problema y se formula el marco teórico de la investigación y en el primer capítulo se realiza el análisis tanto del resultado de la aplicación del instrumento de medición como aquellos elementos de contexto de la formulación de los lineamientos estratégicos y se identifican las debilidades, oportunidades, fortalezas y amenazas, así como los riesgos asociados desde el punto de vista del desarrollo con respecto a la publicación de información en el ciberespacio. En el segundo capítulo se identifican los criterios de seguridad utilizados en el proceso de desarrollo y en el tercer capítulo se formulan los lineamientos estratégicos para el desarrollo de aplicaciones web que soportan e implementan servicios de información en internet como respuesta a uno de los objetivos estratégicos mediante el mejoramiento del acceso a la justicia. Finalmente, en el capítulo tercero se establecen las directrices a tener en cuenta en la arquitectura de software para las aplicaciones web.

1. PLATEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN

1.1. DEFINICIÓN DEL PROBLEMA DE INVESTIGACIÓN.

Enmarcado en el logro del objetivo estratégico No 9 del direccionamiento estratégico de la entidad, (Nación F. G., Plan estrategico 2016-2020, 2018), para el fortalecimiento de la infraestructura tecnológica institucional y en particular en dotar a la entidad de "un sistema de información unificado que garantice la integridad, disponibilidad, confidencialidad y oportunidad de la información a nivel nacional" se destinaron recursos financieros, técnicos y de

talento humano para el desarrollo de una aplicación web unificada para atender las necesidades en materia de aplicaciones web que soporten los procesos misionales y de apoyo.

Así las cosas, se le ha dado mayor prioridad al desarrollo de las aplicaciones web para atender las necesidades de automatización de procesos y delegar la protección de la información en el ciberespacio a los mecanismos de seguridad dada por la plataforma de seguridad perimetral como es el caso de Firewalls, IPS/IDS, balanceadores de ancho de banda y los controles de autenticación de usuarios o de gestión de roles y privilegios soportados por los módulos de la aplicación web, lo que exige que se aborde el desarrollo de aplicaciones desde la óptica de la ciberseguridad y la ciberdefensa, para lo cual, se formula el siguiente problema de investigación: **¿Qué lineamientos estratégicos de ciberseguridad y ciberdefensa son necesarios para el desarrollo seguro de aplicaciones web y la gestión de riesgos de seguridad de la información de la Fiscalía General de la Nación publicada en el ciberespacio?**

1.2. JUSTIFICACIÓN.

La Fiscalía General de la Nación en su gestión de riesgos ha fortalecido su infraestructura tecnológica para llegar al ciudadano pero con los crecientes ataques que sufre el estado colombiano a su infraestructura critica que soporta los servicios de información en el ciberespacio, (tiempo, 2016), ha incluido en su direccionamiento estratégico (Nación F. G., Plan estrategico 2016-2020, 2018) los objetivos con relación al fortalecimiento de las aplicaciones web donde se contempla las características de seguridad inherentes a la información (integridad, confidencialidad y disponibilidad). Sin embargo, no se formula específicamente en los proyectos de desarrollo de aplicaciones web una respuesta a la necesidad de fortalecer la plataforma tecnológica en aplicación de los marcos de referencia, como es el caso del definido por el

ministerio de las TIC como medida de acción para alinearse con la política de seguridad del estado colombiano (Planeación, 2016).

La necesidad de contar con unos lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo de aplicaciones web, obedece a la sensibilidad de la información y servicios tecnológicos asociados a los servicios de investigación y judicialización que requiere los ciudadanos con garantías de seguridad en la publicación de servicios de información en el ciberespacio atendiendo los siguientes aspectos del sector de justicia:

1. Crecimiento del uso de TIC para acceder a servicios en el ciberespacio a nivel global. Esto se evidencia en el estado colombiano con los siguientes indicadores, Estadística de crecimiento de servicios de TIC (TIC M. , 2018):

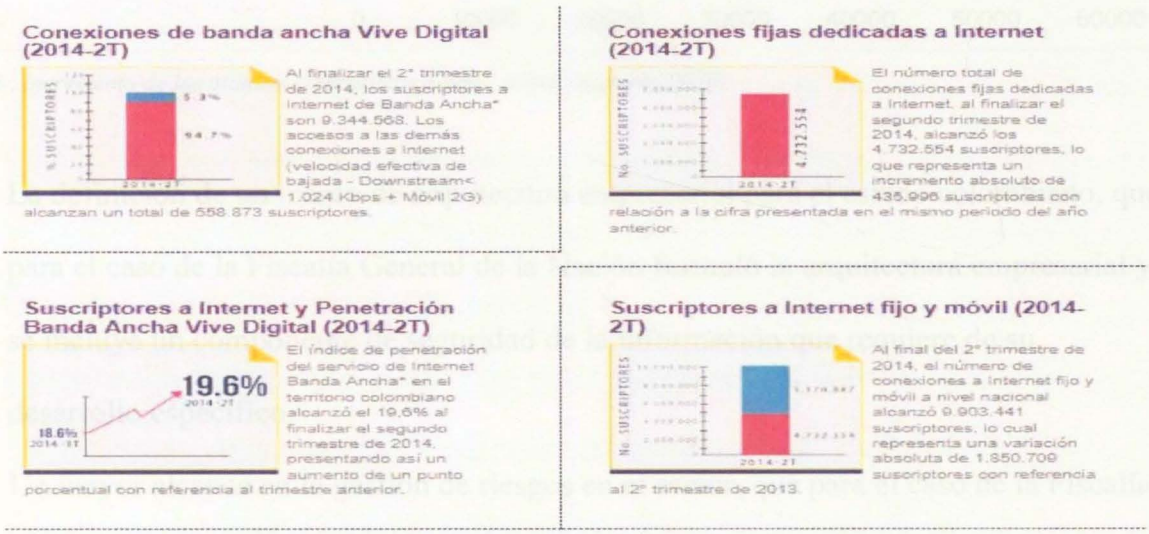

Grafico 1 - Estadística de crecimiento de servicios de TIC (TIC M. , 2018)

2. Incremento de los ataques cibernéticos a nivel global (Systems, 2016) es necesario contar con un adecuado tratamiento los riesgos de seguridad en el ciberespacio en los diferentes componentes de la infraestructura crítica que se utiliza para acceder al ciberespacio como es el caso de nubes públicas, equipos móviles e infraestructura en

la nube, entre otros medios. En este sentido, se evidencia este incremento de los ciberataques de la siguiente manera:

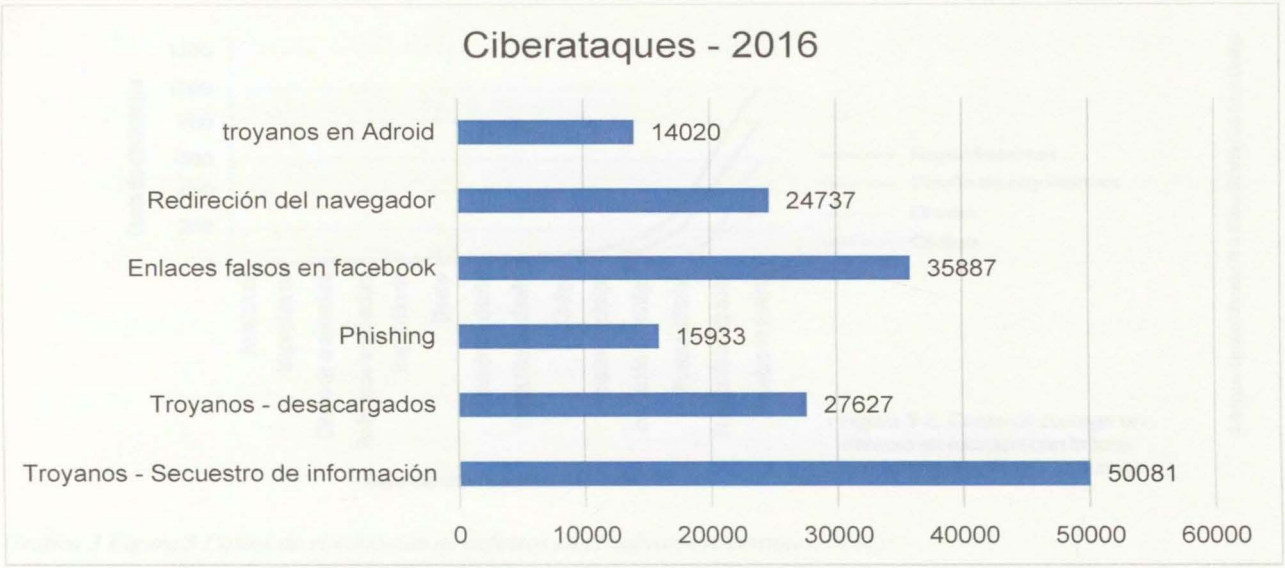

Grafico 2 . Incremento de los ataques cibernéticos a nivel global (Systems, 2016)

3. La definición de un marco de arquitectura empresarial para el estado colombiano, que para el caso de la Fiscalía General de la Nación formuló la arquitectura empresarial y se incluye un componente de seguridad de la información que requiere de su desarrollo específico.
4. Un mayor alcance en la gestión de riesgos en el sector, que para el caso de la Fiscalía se centra en el ciclo de vida de las aplicaciones web con miras de optimizar los recursos y la detección temprana de vulnerabilidades en el funcionamiento y operación de las aplicaciones web que soportan los servicios de información que ofrece la Entidad a la comunidad en donde recae mayor peso en la fase de pruebas tal

como lo evidencia cervantes, (Cervantes, 2016) y se muestra en la Figura 3 Costos de eliminación de defectos en el software (Cervantes, 2016):

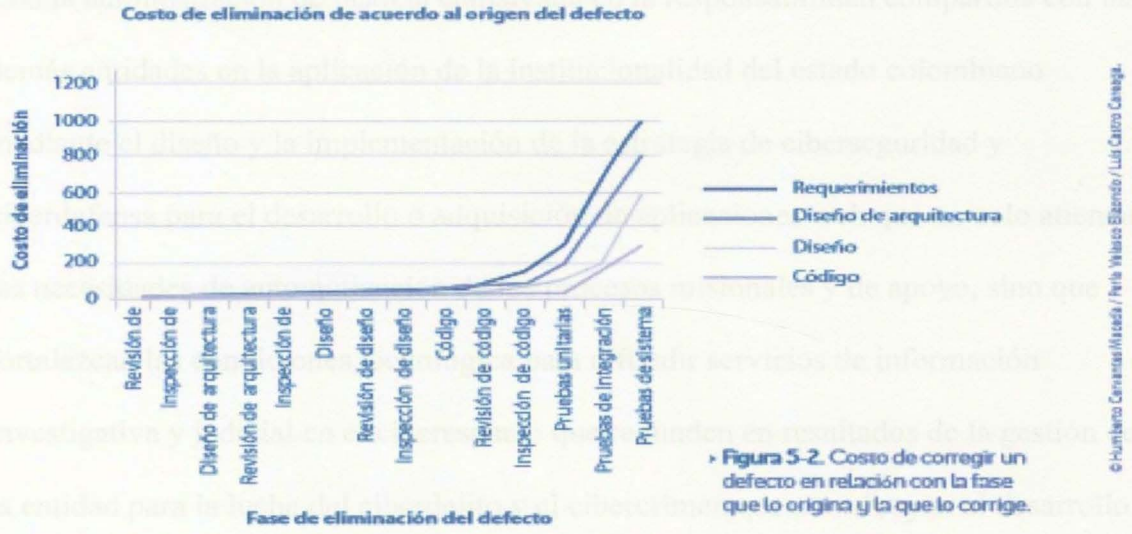

Grafico 3 Figura 3 Costos de eliminación de defectos en el software (Cervantes, 2016):

5. La información disponible en el ciberespacio y los activos relacionados en cuanto a los derechos humanos y fundamentales, la libertad de expresión, el libre flujo de información, confidencialidad y comunicación de la información, protección a la intimidad de los datos personales, así como de los principios constitucionales, de transparencia en la gestión pública del papel que cumple la Fiscalía General de la Nación dentro de la prestación de los servicios misionales de investigación y judicialización del estado como ente acusador dentro del sistema de justicia colombiano.
6. Los servicios y la operación en la prestación del servicio que ofrece la entidad requieren del desarrollo de capacidades de resiliencia basada en alianzas institucionales reflejadas en la responsabilidad de la acción de la policía judicial para

velar por un ciberespacio confiable para generar las condiciones de desarrollo establecidas en la política de seguridad digital del Estado.

7. Con la administración de justicia enmarcada en la responsabilidad compartida con las demás entidades en la aplicación de la institucionalidad del estado colombiano mediante el diseño y la implementación de la estrategia de ciberseguridad y ciberdefensa para el desarrollo o adquisición de aplicaciones web que no solo atienda las necesidades de automatización de los procesos misionales y de apoyo, sino que fortalezcan las condiciones tecnológica para difundir servicios de información investigativa y judicial en el ciberespacio que redunden en resultados de la gestión de la entidad para la lucha del ciberdelito y el cibercrimen que contribuyan al desarrollo de capacidades de las organizaciones, económicos o de los ciudadanos para la defensa del entorno digital colombiano. En este sentido, la Fiscalía General de la Nación debe contribuir a generar las garantías del uso del entorno digital a partir de una acción participativa en el marco legal de ciberseguridad y ciberdefensa para mantener los servicios esenciales del estado colombiano y fomentar el desarrollo de las actividades económicas a efectuar en el ciberespacio.
8. Para la construcción de mecanismos para mantener la cooperación y coordinación con los miembros de la policía judicial que en este caso son la Fiscalía General de la Nación, Policía Nacional de Colombia, INPEC y el instituto de las fuerzas militares (decreto legislativo 1810) y de la rama judicial en el estado colombiano conformado por la Corte Constitucional, Corte Suprema de Justicia, el Consejo de Estado, Consejo Superior de la Judicatura, Jurisdicciones Especiales, Fiscalía General de la Nación,

requieren del intercambio de información de manera segura con lo que se permite crear un entorno digital confiable frente a los riesgos de corrupción, confidencialidad, integridad y disponibilidad de información de índole reservado o clasificada que han fomentado el celo en el intercambio o en el registro en aplicaciones web que limita o dificulta los análisis integrales que redundan en efectividad de las acciones de policía judicial no solo en el ámbito del ciberespacio sino que en todos los procesos de judicialización e investigación.

9. Para fortalecer la resiliencia del sector justicia en el entorno colombiano a partir de la construcción y uso seguro de las aplicaciones web que permiten publicar información de interés en el ciberespacio, con una adecuada definición de los requisitos de ciberseguridad se fortalece las capacidades de uso eficiente de recursos y de esta manera implementar controles que tienen como objetivo evitar desviaciones en la funcionalidad de las aplicaciones web, es decir el desarrollo de funcionalidad que no atienden los requerimientos funcionales o de seguridad y que van en contra de las directrices establecidas en la formulación estratégica de la Entidad de fortalecer la infraestructura tecnológica para lograr los objetivos estratégicos y de operación de la entidad como es el caso de la lucha contra las organizaciones criminales y hacer posible su desmantelamiento así como el flagelo de la corrupción en las entidades del estado como es el caso de las acciones de infiltración dentro de la misma organización, tal como se establece en la estrategia institucional que para el periodo actual se define como plan estratégico 2016 – 2020 (Nación F. G., Plan estratégico 2016-2020, 2018), ver Anexo No 8. Elementos corporativos del plan estratégico 2016 – 2020 de la FISCALÍA GENERAL DE LA NACIÓN.

Por lo anterior, es necesario contar con unos lineamientos estratégicos de ciberseguridad y ciberdefensa para contar con aplicaciones web con características de calidad relacionadas con la seguridad de la información contemplando las diferentes etapas del ciclo de vida de la aplicación.

2. MARCO TEÓRICO.

2.1. Antecedentes.

En cuanto a la formulación de estrategias y su adopción en el ámbito de seguridad, Sanchez, (Sanchez Blas, 2017) en su trabajo de investigación **"Adopción de estrategias de Ciberseguridad en la protección de la Información en la Oficina de Economía del Ejército, San Borja- 2017."**, analiza la adopción de una estrategia de Ciberseguridad en el ámbito militar para la protección de información en la Oficina de la Economía del Ejército de San Borja del Perú, y resalta la importancia de tratar riesgo de la seguridad de la información reservada cuando son interés de cibercriminales. Así mismo lo aborda Márquez, (Marquez Alayo, 2018) lo aborda en su trabajo de investigación **"Ciberseguridad y su Relación en la Seguridad de los Sistemas Informáticos del Ejercito del Perú Caso: DITELE 2013-2014"** desde el punto de vista de los servicios que una organización en el ciberespacio y la relevancia de las infraestructuras críticas relacionadas en publicación de la información en la gestión de la ciberseguridad en la región, y más en cuanto a los servicios donde se exige que exista una relación de los sectores y servicios críticos disponibles para parte de una organización en el ciberespacio, es decir la relación de una economía estable con las comunicaciones que permite la conexión de servidores o centros de datos, al igual que con aplicaciones, bases de datos, entre otros aspectos. En este sentido,

Márquez, (Marquez Alayo, 2018), plantea que la ausencia de metodologías de clasificación de los servicios que dificultan la gestión de la ciberseguridad.

En cuanto a la gestión de riesgos de la ciberseguridad, Rivera, (Rivera Davila, 2019), en su trabajo de investigación **"Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016"** propone una de metodología de gestión en riesgos de ciberseguridad que identifica la influencia en la sociedad de los cambios sociales y tecnológicos lo que conlleva a realizar un análisis de riesgos de ciberseguridad que permite la construcción de indicadores de gestión y la aplicación de controles de calidad para la solución de problemas en las diversas actividades que realiza el ser humano en el ciberespacio, tal como lo describe Villalba, (Villalba Fernández, 2015), en su investigación **"La ciberseguridad en España 2011-2015 una propuesta de modelo de organización. Madrid 2015"** con los beneficios que trae a la sociedad el uso de internet como es el desarrollo de las capacidades de comunicación, investigación científica, entre otros aspectos, y que requieren la atención del estado; como es el caso de las respuestas ante ataques que tiene como objetivo la soberanía y los "sistemas de Tecnologías de la Información y las Comunicaciones de gobiernos, administraciones públicas y empresas con alto valor estratégico" aprovechando las limitaciones de la ubicación de los ciberataques y la atribución de responsabilidades. En cuanto al análisis de las amenazas asociadas a los riesgos, Rubio (Rubio Blanco, 2016), en su investigación **"Un Marco para el Análisis de Riesgos en Ciberseguridad"** muestra que el análisis de riesgos permite analizar las amenazas que enfrentan las organizaciones y de esta manera priorizar el tratamiento en defensa de sus activos, así como determinar los impactos en relación con la gestión de la organización.

En cuanto a estos sistemas de tecnologías de la información y las comunicaciones, el software es un componente a valorar tal como lo plantea Ruiz, (Ruiz Robles, 2017), en su investigación **"Valoración y gestión estratégica de activos de proceso intangibles en ingeniería del software."**, como un factor a gestionar adecuadamente para cumplir con los objetivos del negocio de una organización y su relación con el mejoramiento continuo de procesos entendido como un activo intangible desde el punto de vista estratégico.

Por otro lado, Fernandez (Fernández Pérez, 2018), en su investigación **"Modelo computacional para la evaluación y selección de productos de software."**, resalta que el proceso de evaluación del software resulta costoso y complejo que es necesario tener en cuenta en la toma de decisiones para contar con una "selección objetiva" que satisfaga parámetros de calidad y las restricciones del modelo de operación de la entidad.

En cuanto a la construcción de software, Ramirez, (Ramírez Quesada, 2018) , plantea en su investigación **"Modelos metaheurísticos para el soporte a la decisión en el proceso de construcción de software."** la necesidad de establecer factores para la toma de decisiones en el proceso de diseñar sistemas de información que permitan cumplir con los requisitos de eficiencias y seguridad del sistema que se vea reflejado en una arquitectura basada en componentes y evaluar las alternativas tecnológicas existentes para dar solución a los parámetros de diseño y su dependencia con la construcción del sistema de información, su facilidad de mantenimiento en el futuro y técnicas avanzadas de optimización.

Para el caso colombiano, Serna (Serna Patiño, 2018), en su investigación "ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTÉMICA DESDE LA ORGANIZACIÓN", determina que

para un desarrollo sostenible cae en el ámbito de la ciberseguridad y la gestión de incidentes que afecten la infraestructura critica a partir de un modelo de madurez de la capacidad y las mejores prácticas definidas por el Instituto Nacional de Estándares y Tecnología. Que se relacionan con la arquitectura de la infraestructura como lo describe Bautista, (Bautista Peñaquishpe, SISTEMAS COMPUTACIONALES Y ARQUITECTURAS TECNOLÓGICAS, 2019) , en su investigación "SISTEMAS COMPUTACIONALES Y ARQUITECTURAS TECNOLÓGICAS", basado en el estándar ISO 42010 aplicado en el ciclo de vida de una arquitectura, concepto de arquitectura de software e ingeniería web.

2.2. Bases teóricas.

Lineamiento estratégico: de acuerdo con Serrano, (Y. H., 2019), pág. 25, se define como elementos de alto nivel que busca alinear el comportamiento de los integrantes de una organización en el logro de una visión compartida.

Estrategia: Peraza, (Peraza, 2012) pág. 87, relaciona las siguientes definiciones de estrategia de acuerdo con el planteamiento de:

- Alfred Chandler (1962) y de Francés (2006: 23) como "La determinación de los fines y objetivos básicos de largo plazo de la empresa y la adopción de cursos de acción, y asignación de recursos, necesarios para alcanzar esos fines".
- Porter (1999:16) como "… la definición de una estrategia competitiva consiste en desarrollar una amplia fórmula de cómo la empresa va a competir, cuáles deben ser sus objetivos y que políticas serán necesarias para alcanzar tales objetivos".
- Kaplan y Norton (2004: 93) como "La estrategia de una organización describe de qué forma intenta crear valor para sus accionistas y clientes…".
- Kaplan y Norton (Ob. Cit: 61) indica que "La Estrategia no es un proceso de gestión independiente, sino que es un paso de un proceso continuo lógico que moviliza a una

organización de una declaración de misión de alto nivel al trabajo realizado por los empleados administrativos y de atención al cliente."

- Finalmente propone la estrategia como: "La visión de la organización presenta una imagen del futuro que aclara el rumbo de la organización y ayuda a las personas a comprender por qué y cómo deben apoyar a la organización".

De igual manera, Rodriguez, (Mora Rodriguez, 2016), indica que la estrategia es una herramienta para optimizar recursos asignados en un plan de acción como generador de oportunidades para el logro de objetivos.

Gerencia Estratégica, Peraza, (Peraza, 2012) pág. 89, la define como "la formulación, ejecución y evaluación de acciones que permitirán que una organización logre sus objetivos", sumado al logro de metas, cumplimiento de políticas y asignación de recursos para la ejecución de la estrategia y el apoyo para la toma de decisiones.

Planificación estratégica, Peraza, (Peraza, 2012) pág. 90, se refiere a las actividades de planificación que incluye los factores internos y externos de la organización basadas en la matriz DOFA (debilidades, oportunidades, fortalezas y amenazas).

Matriz de mando integral. Peraza, (Peraza, 2012) pág. 90. Lo establece como una herramienta para la gestión estratégica.

Mapa estratégico. Peraza, (Peraza, 2012) pág. 92 lo establece como un mapa que permite operacionalizar de las estrategias globales de una organización y de las específicas de una unidad de negocio. Adicionalmente, indica que Kaplan y Norton (2001) formulan el mapa estratégico como un proceso de trasformación de los activos intangibles en resultados tangibles.

Sistema de gestión ágil: Villar, (Fidalgo., 2019), se refiere a sistemas que tienen un contexto de diseño de sistemas, de instalaciones, de equipos tecnológicos y de requerimientos no documentados; basados en planteamientos de ingeniería concurrente e ingeniería colaborativa, es decir de la propuesta de integración de herramientas de otras disciplinas con metodologías nuevas.

Ciberseguridad, Existen varias definiciones de ciberseguridad como lo hace Vila, G. (2019), que la formula como: "Prevención de daños, protección y restauración de equipos, sistemas de

comunicaciones electrónicas, servicios de comunicaciones electrónicas, comunicación alámbrica y comunicación electrónica, incluyendo la información contenida en el mismo, para asegurar la disponibilidad, integridad, autenticación, confidencialidad y no rechazo". De igual manera Villar, (Fidalgo., 2019), indica que el comité del sistema de seguridad nacional (Committee on National Security System – CNSS-4009), lo establece como una habilidad de protección o defender el uso empresarial del ciberespacio frente a un ataque que busque interrumpir, destruir o control malicioso de un ambiente computacional o de infraestructura, o atacar la integridad o confidencialidad de información. De igual manera, indica el planteamiento del instituto nacional de estándares y tecnologías, se refiere como un proceso de protección de información para prevenir, detectar y respuesta ante ataques. Adicionalmente, la organización internacional para la estandarización plantea que la ciberseguridad o seguridad del ciberespacio como la preservación de la integridad, confidencialidad y disponibilidad de la información en el ciberespacio. Esto entendiendo que el ciberespacio es un entorno complejo generado por interacción de las personas, software y servicios generados por dispositivos y redes.

De igual manera, la ITU, (Ciberseguridad., 2010), indica que es un "conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno".

El Ministerio de Tecnologías de la Información y las Comunicaciones. (2019), (Comunicaciones., 2019), indica que "Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio". Por

otro lado, Gago, (Gago, s.f.) , indica que la ITU-T X.1205 (2008) lo refiere como "El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. ISACA la define como la "Protección de los activos de información a través del tratamiento de las diversas amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". Gago, (Gago, s.f.),indica que la ISO/IEC 27032 (2012). La establece como la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio, definiendo a su vez ciberespacio como el entorno complejo resultante de la interacción de personas, software y servicios en Internet, a través de dispositivos tecnológicos y redes conectadas a él, que no existen en ninguna forma física". Según Gago, (Gago, s.f.), considera que la ciberseguridad es un aspecto importante en la seguridad nacional que requiere la protección del estado, entendiendo la ciberseguridad como la protección de la información en formato digital y en sistemas de información interconectados en sus componentes de procesamiento, almacenamiento y transmisión.

Regulaciones de ciberseguridad, Robles Carrillo, (Robles Carrillo, EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO, 2015), plantea que las regulaciones de seguridad que requiere el ciberespacio son aquellas que se formulan a partir de un contenido material derivado de la seguridad humana traducida en "seguridad económica, seguridad ideológica, seguridad alimentaria o seguridad medioambiental, entre otras" que se traducen en efectos reguladores ante

la fuerza de los hechos o principio de efectividad en un modelo de economía del conocimiento y en un modelo socio-político con principio de diversidad.

De igual manera, Jangirala, (Jangirala Srinivasa, 2019) (https://www.researchgate.net/profile/Srinivas_Jangirala/publication/328183318_Government_regulations_in_cyber_security_Framework_standards_and_recommendations/links/5c1d53d892851c22a33d339e/Government-regulations-in-cyber-security-Framework-standards-and-recommendations.pdf), entendiendo que la ciberseguridad se refiere a la protección de los sistemas interconectados, así como el software y la información frente a ataques originados en el ciberespacio, plantea que la regulación se debe dar en el ámbito de la tecnología de la información y sus estándares o marcos de ciberseguridad que permiten formular la ciberseguridad y la ciberdefensa.

Ciberdefensa. Existen varias definiciones de ciberseguridad como lo hace Vila, G. (2019), que la formula como la "aplicación de medidas de seguridad para proteger las los diferentes componentes de los sistemas de información y comunicaciones de un ciberataque", de igual manera Ministerio de Defensa, (2010) que la formula como ".. las medidas de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras organizaciones".

Aplicaciones Web. Existen varias definiciones de aplicaciones web como lo hace Acosta, (Acosta, 2018), de acuerdo con el planteamiento de MaxCDN (2016) como un "... software diseñado con el fin de cumplir tareas específicas para los usuarios" como apoyo a la realización de actividades individuales o de una organización. De igual manera, refiere el planteamiento de mozzilla.org (2018) como "Una aplicación web es un software basado en la arquitectura cliente-servidor", que se opera por medio de un navegador web.

Seguridad en aplicaciones web. De acuerdo con Guaman, (Guaman-Quinche, 2016), se trata de establecer mecanismos de protección para mantenerlos la integridad y confidencialidad de los datos, y establece que "Actualmente el 80% de los ataques informáticos son llevados a cabo por código malicioso y las configuraciones por defecto que se realizan en el desarrollo de un sistema web hacen que el ataque sea una tarea sencilla."

Otra posición es la planteada por **Proyecto abierto de seguridad de las aplicaciones web abiertas – OWASP**, que según Novilo, (Novillo Vicuña J. P., 2019), se trata de recomendaciones que atienden la necesidad de gestionar las posibles vulnerabilidades que se presenten en el proceso de desarrollo. Adicionalmente, se identifica la aplicabilidad de la norma ISO/IEC 27002:2013, en sus dominios de ciframiento, operaciones y Adquisición, desarrollo y mantenimiento de sistemas de información, tal como lo planeta Ortiz, (Carlos Ortiz de Zevallos, 2016), que los plantea como resultado de un entorno tecnológico.

Marco de seguridad cibernética (CSF): Amazon Web Services, (Services, 2019), plantea como base de la seguridad cibernética un marco de seguridad cibernética (CSF) de NIST como soporte a la gestión del riesgo y la resiliencia de sus sistemas de información.

Pruebas de aplicaciones Web: Foster, (Foster., 2018), plantea que las revisiones de las aplicaciones web son utilizadas como pruebas de seguridad en busca de vulnerabilidades no detectados en coherencia con una estrategia de escaneo.

Ciberespacio: Existen múltiples definiciones, como la de Carrillo, (Robles Carrillo, EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO, 2015), que lo planeta como un escenario global de carácter "táctico, estratégico y operativo" con capacidad de alterar su realidad o interactuar

con otro tipo de realidad. En su sentido público se identifica como un espacio con una singularidad funcional y sistémica que puede considerarse como un bien público que requiere ser asegurado desde la perspectiva del proceso y con la competencia de una política pública que incluya componentes tanto técnico como legislativos.

Arquitectura Empresarial. La Fiscalía General de la Nación, (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018), establece la arquitectura institucional como "... una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad, a través del desarrollo de los procesos".

Los principios descritos son soportados por la arquitectura empresarial de la Entidad, la cual está alineada con el planteamiento establecido por el Ministerio de las Tecnologías y la Comunicaciones, (TIC M. d., Diseño y Especificación del Marco de Referencia. Diseño Detallado. Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información (TI), a Adoptar en las Entidades del Sector Público Colombiano., 2014) se analiza los componentes del modelo de gestión IT4+, (TIC M. d., 2016) en la que se busca una articulación entre la gestión tecnológica para el desarrollo de los procesos y la estrategia institucional la que encuentra su aplicación en el plan estratégico 2016-2020, en la que en los componentes de aplicaciones web se cuenta con la siguiente arquitectura:

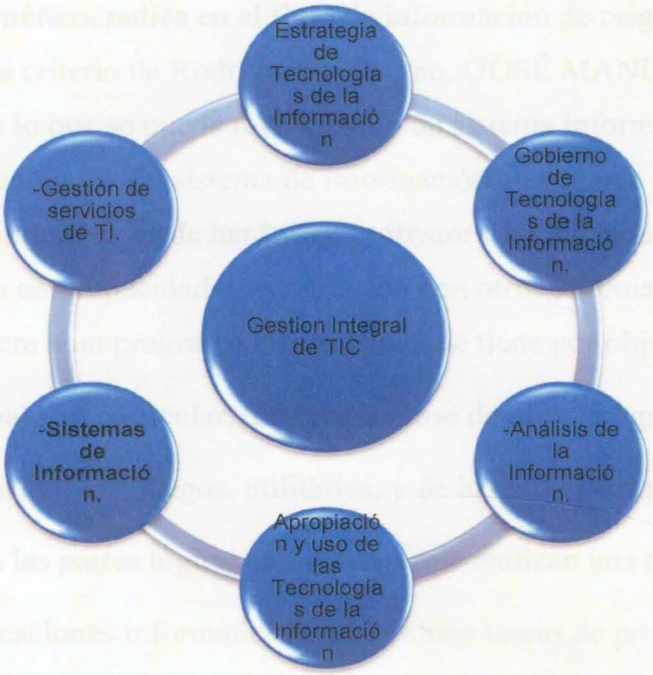

Grafico 4 Gestión IT4+ formulado por Min TIC, (TIC M. d., 2016)

Sistema de Información. De acuerdo con Sarngadharan (Sarngadharan & Minimol, 2009), se define un sistema de información como un grupo de elementos interrelacionados o interactivos que conforman una unidad, que puede ser físicos o abstractos. En el sentido abstracto, es un arreglo ordenado de ideas independientes o de contratos. Pero en el aspecto físico, es definido como un conjunto de elementos que operan conjuntamente para lograr un objetivo; como es el caso de tierras, gente y otros elementos tangibles; como una unidad compleja y organizada, que está compuesta por un ensamble o combinación de partes que conforman una unidad más compleja. Realizando este mismo planteamiento en un contexto técnico y legal, tal como lo plantea Rodríguez y Daureo en su libro electrónico APLICACIONES WEB: ASPECTOS TÉCNICOS Y LEGALES, (JOSÉ MANUEL RODRÍGUEZ RODRÍGUEZ, 2003).

Contexto cibernético, radica en el flujo de información de origen hasta el destino de manera automática, que a criterio de Rodríguez y Daureo, (JOSÉ MANUEL RODRÍGUEZ RODRÍGUEZ, 2003), es lo que se puede referir como un sistema informático, por lo tanto se considera como un "subconjunto del sistema de información", en el que soporta su funcionamiento en sus componentes de hardware, software e interacción humana para el logro de un objetivo específico con capacidad de interacción con otros sistemas informáticos.

Aplicaciones. Se refiere a un programa informático que tiene por objetivo ayudar a un usuario a realizar un trabajo en particular, diferenciándose de otros programas de computación como son los sistemas operativos, juegos, utilitarios, y de los utilizados para escribir programas.

Software. se refiere a las partes lógicas del sistema que realizan una tarea específica que incluyen no solo las aplicaciones informáticas sino también tareas de propósito general como lo es un sistema operativo. En este aspecto, según Braude y Bernstein (Eric J. Braude, 2011), la disciplina que se encarga de estudiar los diferentes proceso a desarrollar en la construcción y gestión del software, se denomina ingeniería de software.

2.3. Marco conceptual.

La Fiscalía General de la Nación ha basado su gestión tecnológica en una arquitectura empresarial, la cual fue definida mediante resolución No 1165 de 2018, (42010, 2018), (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018) y contempla la necesidad de cumplir con la política de seguridad que busca alinearse con la política de seguridad digital del Estado establecidos en el CONPES 3854 (Planeación, 2016), así como de la política de seguridad digital de estado colombiana como marco de gestión de riesgos de seguridad digital así como el desarrollo de capacidades de resiliencia, recuperación y en

particular en respuesta a los ciberataques como aspecto de ciberdefensa tal como los relaciona Owens (Owens, 2007), como es el caso de las actividades de las organización al margen de la ley que utiliza los medios digitales y la economía digital para el desarrollo de sus actividades y que requieren de una política de defensa articulada tal como lo establece Miranda (Miranda, 2010), entendida como "la suma de las hipótesis, planes, programas y acciones tomadas por los ciudadanos estadounidenses, principalmente mediante el accionar del gobierno, para garantizar la seguridad física de sus vidas, su propiedad y su modo de vida y defenderla contra ataques militares del exterior e insurrecciones locales.".

Por esta razón se aborda la gestión de seguridad de información en el ámbito del desarrollo de aplicaciones web, tal como lo plantea, Varela, (Varela Recalde, 2019), con la definición de amenazas relacionadas a los activos de información, así como la gestión de riesgos, y en este sentido, lo menciona Valencia, (Valencia Maldonado, 2014), como herramienta para lograr los objetivo institucionales, financieros, de proyectos y de los servicios que proporciona a la ciudadanía, proyectando una imagen positiva hacia la comunidad, lo conlleva a la construcción de una matriz de fortalezas, oportunidades, debilidades y amenazas. Esto enmarcado en las definiciones de calidad, para lo cual se realizará con base en un marco de referencia OWASP, (Project, Application Security Verification Standard 4.0, 2019). Con esto, se fundamenta los lineamientos estratégicos para el desarrollo seguro las aplicaciones web y la gestión de vulnerabilidades en la publicación de la información en el ciberespacio, es decir, gestionar el ciberiesgo como lo plantea firmas reguladas como IIROC, (Members, 2019).

Para la formulación de los lineamientos estratégicos mencionados, se inicia con el contexto dado a las entidades que son actores en la gestión de la seguridad digital del país como es el caso de la Fiscalía General de la Nación, que al igual que otras entidades requieren de un modelo para su construcción en coherencia con los lineamientos estratégicos que en Colombia se formuló mediante el CONPES 3704, (Social, 2011), y que finalmente se cuenta con la política formulada mediante el CONPES 3854, (Planeación, 2016), esta condición descrita en el modelo

de formulación de una estrategia de seguridad nacional propuesta por Ballesteros, (Ballesteros, 2016), donde se identifica la necesidad de ser adaptado al entorno del país que vive en una multiplicidad de actores del orden nacional. Para este efecto, en el contexto de la política de seguridad del estado, se resalta la importancia de la gestión del riesgo digital,

Para dicha gestión, de acuerdo con Maldonado, (Valencia Maldonado, 2014), se plantea la necesidad de utilizar una herramienta gerencial que facilite el cumplimiento de los objetivos, que para este trabajo se centra en el diagnóstico y el análisis de riesgos. El planteamiento de Maldonado, (Valencia Maldonado, 2014), formula las siguientes actividades para obtener un planteamiento de gestión:

- **Diagnostico situacional o establecimiento de contexto.** Esta actividad incluye el análisis de la "estructura Organizacional, Estructura Física, Procesos, Legislación Interna"
- Formulación de una matriz de debilidades, oportunidades, fortalezas y amenazas, en la que se debe identificar la relación entre los riesgos y oportunidades
- **Análisis de la gestión de riesgos.** Para el caso de la Fiscalía General de la Nación se enmarca dentro del modelo de gestión interna, a pesar de que Maldonado, (Valencia Maldonado, 2014), plantea alternativas como el estándar AS/NZS 9360 y el uso de la norma ISO 31.000:2009. Adicionalmente debe incluir la evaluación de riesgos, tratamiento de riesgos. Para este tratamiento o gestión, Cuzme (Cuzme Rodriguez, 2019) considera varias metodologías como MARGERIT, OCTAVE, ISO/IEC 27005, ISO/IEC 27002, MSAT, Microsoft Security Assessment Tool para infraestructura, aplicaciones, operaciones y personal, o el caso de ISO/IEC 27002 propuesta por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), tal como lo plantea Narvaez, (Narváez Pupiales, 2018), en cuanto a su importancia en la gestión de un Sistema de Gestión de Seguridad de la Información basado en las normas ISO 27799:2008, ISO/IEC 27005:2013 E ISO/IEC 27002:2013, COBIT 5 e ITIL en su versión 3. Este aspecto es relevante como lineamiento en la Fiscalía General de la Nación dado que se enfoca tecnología de la información.

- Monitoreo de las estrategias a aplicar y comunicación de riesgos a los interesados por medio de un plan estratégico.
- **Análisis de los principales impactos.** Estos en lo referente a los aspectos económico, social, educativo y ético.
- Conclusiones y recomendaciones para mejorar la situación actual.

En cuanto al análisis de riesgos, este trabajo se enfoca en **la seguridad en el desarrollo de software,** para lo cual se plantea el modelo planteado por el **Proyecto abierto de seguridad de las aplicaciones web abiertas – OWASP**, (Project, Application Security Verification Standard 4.0, 2019), tal como lo refiere Novillo (Novillo Vicuña J. P., 2019), para "garantizar la seguridad y minimizar las posibles vulnerabilidades que estos sistemas aplicativos presentan al momento de ser desarrollados", que no va en contraposición con otros planteamiento como el de Chandra, (Chandra, 2009) que plantea la formulación de una estrategia de seguridad para el desarrollo del software a partir de un modelo de madurez (SAMM) de carácter cíclico que esté acorde con los recursos disponibles y las actividades o cambios de la organización o por el planteado por McGraw, (Gary McGraw, 2014), que refiere una gestión de seguridad a partir de un modelo de madurez, (Building Security In Maturity Model - BSIMM) que aplicado al desarrollo del software es un referente para compararse con otras organizaciones bajo un mismo criterio. Para el caso de OWASP, se concibe como un estándar de verificación de seguridad de la aplicación (Application Security Verification Standard - ASVS) establecida en la metodología de desarrollo de software seguro OWASP (Open Web Application Security Project), (Project, Application Security Verification Standard 4.0, 2019), que permiten se aplicados en el diseño, desarrollo y pruebas de aplicaciones web mediante en el ciclo de vida del software como es el uso de herramientas para identificar fallos, capacitación de los grupos involucrados en el desarrollo,

análisis de problemas y la compatibilidad con otros estándares como NIST SP 800-63 que propone una guía para la identidad digital basada en la evidencia y la gestión de sesión.

La aplicación del ASVS para maximizar los controles de seguridad y minimizar los costos, se propone en las fases de:

- Definición de requerimientos.
- Diseño.
- Codificación.
- Pruebas.
- Liberación.

De acuerdo con los niveles de verificación de seguridad de las aplicaciones definida por el ASVS v4.0, se cuenta con:

Tabla 1.
Niveles de ASVS 4.0 - OWASP

Nivel	Descripción
1	**Primer paso de automatización** o vista del portafolio con la defensa de vulnerabilidades que son fácilmente detectables como los tops 10 de OWASP para el manejo de aplicaciones que no manejan información sensible. Se verifica por medio de herramientas sin acceso al código fuente.
2	**La mayoría de las aplicaciones.** Se cuenta con las defensas para la mayoría de los riesgos actuales asociados con el software y que cuenten con controles en la aplicación para el manejo de información o con las funciones críticas de negocio.
3	**Alta seguridad.** Se cuenta con aplicaciones con altos niveles de verificación de seguridad de aplicaciones críticas, es decir el funcionamiento de aplicaciones pueden afectar la operación del negocio.

Fuente: Niveles de ASVS 4.0 – OWASP, (OWASP, 2017)

En este sentido, el proceso de construcción seguro de aplicaciones web se aborda desde una metodología de desarrollo de software, tal como lo formula Lascano, (Lascano Rivera, 2017), es un aspecto que influencia en el crecimiento experimentado del uso de los dispositivos móviles, en la que se indica que, un 53% de la población en Latinoamérica utiliza internet a través de cualquier equipo tecnológico.

3. METODOLOGÍA DE INVESTIGACIÓN.

3.1. TIPO DE INVESTIGACIÓN.

A partir de un proyecto de investigación explicativa se formulará los lineamientos estratégicos de Ciberseguridad y Ciberdefensa para el desarrollo seguro de aplicaciones web de Fiscalía General de la Nación en de acuerdo con la necesidad de una metodología de elaboración de una estrategia como lo plantea ballesteros, (Ballesteros, 2016), la que servirá de base teórica para aplicarla en el desarrollo seguro de aplicaciones web atendiendo de igual manera los lineamientos arquitectónicos establecidos en la arquitectura empresarial para el ofrecimiento y el sostenimiento de servicios de administración de justicia en el entorno digital colombiano.

3.1.1. Objetivo principal.

Identificar los lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones web y la gestión de riesgos de seguridad de la información de la Fiscalía General de la Nación publicada en el ciberespacio.

3.1.2. Objetivos Secundarios

- Establecer los lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones web y la gestión de riesgos de seguridad de la información de la Fiscalía General de la Nación publicada en el ciberespacio.
- Definir los criterios para el desarrollo seguro de aplicaciones web utilizados por el equipo de desarrollo de la FGN.
- Identificar los criterios existentes en la FGN para el manejo de vulnerabilidades de las aplicaciones Web para la publicación de información en el ciberespacio.
- Identificar la relación entre los lineamientos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio
- Establecer los lineamientos para el análisis de contexto para la formulación de una estrategia de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones

Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio

- Identificar las alternativas de los lineamientos para la formulación de lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio, se definen de acuerdo con la ISO 27002, en el dominio No 10 para establecer los planes de implementación de los lineamientos estratégicos y la gestión de los riesgos identificados
- Establecer los objetivos de los lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio.

3.2. HIPÓTESIS DE INVESTIGACIÓN.

Es necesario determinar que lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones web y la gestión de riesgos de seguridad de la información de la Fiscalía General de la Nación publicada en el ciberespacio.

3.3. POBLACIÓN Y MUESTRA.

La Fiscalía General de la Nación está compuesta por dos grandes áreas a cargo del despacho del señor Fiscal de la Nación y aquellas correspondientes a la Vicefiscalía, tal como se detalla en el documento No 8 publicada en la página web de la entidad, (Nación F. G., Mapa de Procesos, 2017) en la que se resalta la siguiente estructura:

3.3.1. Despacho del Fiscal General de la Nación. Como cabeza de la entidad le corresponde gestionar entre otras áreas la de planeación y desarrollo, que es la encargada de validar las políticas y estrategias de desarrollo de la entidad:

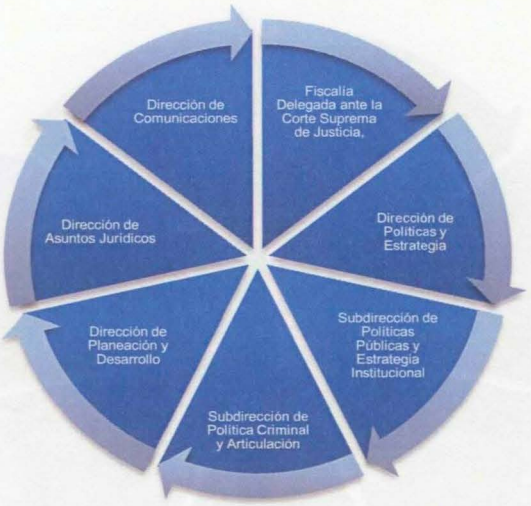

Grafico 5 . Descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017)

Adicionalmente, se encarga de las áreas de control como es el interno o disciplinario, entre otras como:

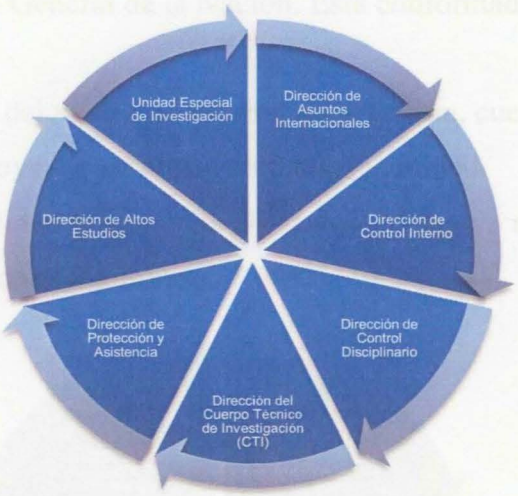

Grafico 6 Continuación de la descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017)

Adicionalmente el despacho del Fiscal General de la Nación se centra la gestión de los recursos administrativos y de apoyo denominada Dirección Ejecutiva, la que cuenta con una Subdirección Tecnologías de la Información y las comunicaciones, entre otras subdirecciones como:

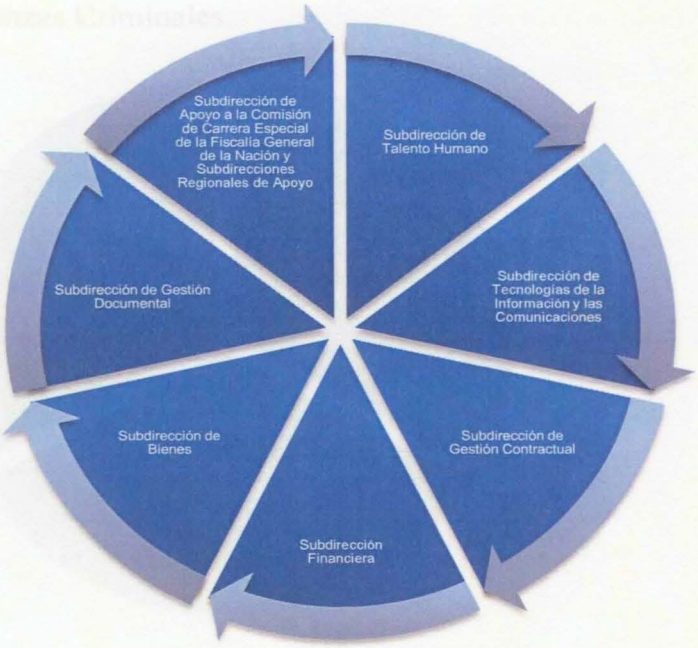

Grafico 7 Descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017)

3.3.2. Despacho del Vicefiscal General de la Nación. Está conformada por las siguientes delegadas:

Este despacho en cabeza del vicefiscal general de la nación, cuenta con las siguientes delegadas encargadas de apoyar la gestión judicial de la entidad.

- Delegada contra la Criminalidad Organizada Dirección de Apoyo a la Investigación y Análisis contra la Criminalidad Organizada.

Grafico 8 Descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017)

- Delegada para las Finanzas Criminales.

Grafico 9 Descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017)

- Delegada para la Seguridad Ciudadana.

Grafico 10 Descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017)

- Órganos y Comités de Asesoría y Coordinación - Entidades Adscritas. La entidad cuenta con unas áreas especializadas en el manejo de los bienes asociados en los procesos judiciales y la investigación forense, tal como se describe a continuación:

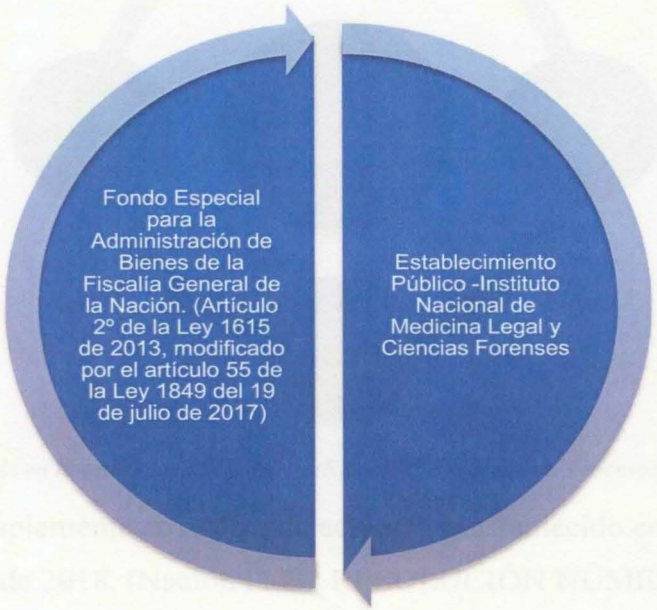

Grafico 11 Descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017)

En su área de gestión de tecnologías de la información y las comunicaciones, se establece su estructura mediante la resolución (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018), se divide de la siguiente manera:

Grafico 12 Descripción basada en la estructura de la FGN, (Nación F. G., Mapa de Procesos, 2017).

En cuanto a la implementa se realiza de acuerdo lo establecido en los artículos 10 y 11 de la resolución No 1165 de 2018, (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018):

ARTÍCULO 11. Establecer la organización interna y las interacciones de operación de las dependencias que lideran la función de Arquitectura Institucional, de la siguiente manera:

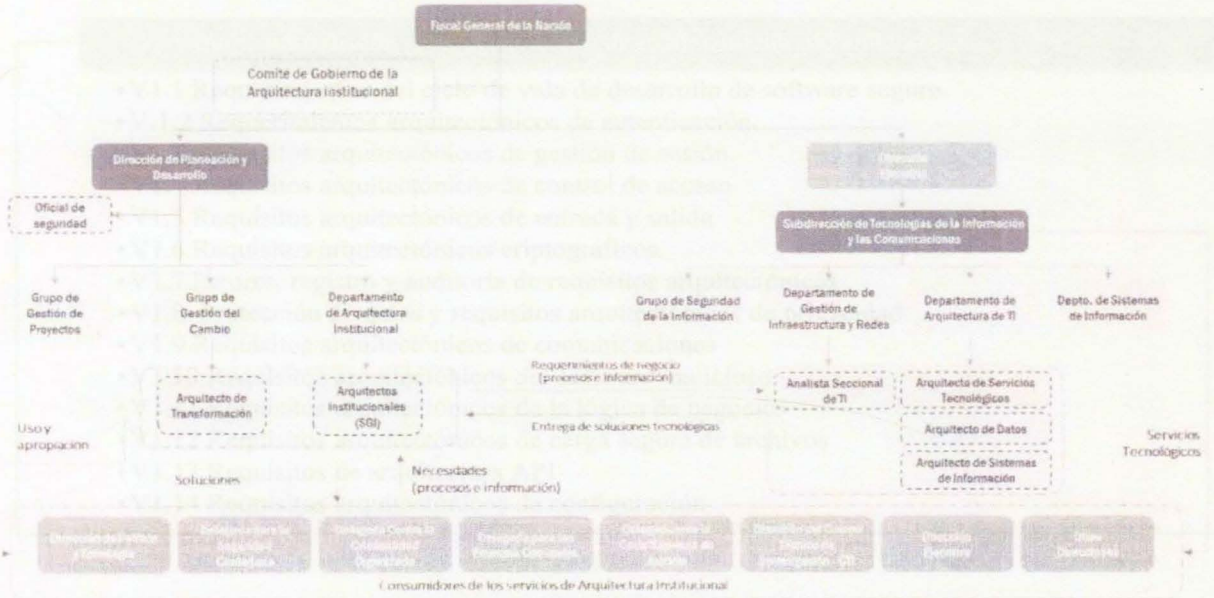

Grafico 13 Descripción basada en la estructura de la FGN, (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2

Asía las cosas la gestión de construcción de aplicaciones web está en cabeza del departamento del Sistema de Información para lo cual cuenta con 37 perfiles que participan en el proceso de desarrollo web, descrito de la siguiente manera

- 17 desarrolladores.
- 6 tester.
- 5 operadores y arquitectos de base de datos.
- 7 ingenieros de soporte.
- 2 asistentes administrativos.

La encuesta se aplica en particular al grupo de desarrolladores y tester, por considerarse que tiene directa relación con el proceso de construcción de las aplicaciones web.

3.4. INSTRUMENTOS.

Para el análisis de los lineamientos utilizados en el grupo de desarrollo descrito en el punto anterior, se establecen las encuestas por cada uno de los aspectos formulados en OWASP

(Project, Application Security Verification Standard 4.0, 2019), con la finalidad de identificar los siguientes aspectos:

V1. Arquitectura, diseño y requerimientos de modelamiento de amenazas.

- V1.1 Requerimientos del ciclo de vida de desarrollo de software seguro.
- V.1.2 Requerimientos arquitectónicos de autenticación.
- V1.3 Requisitos arquitectónicos de gestión de sesión.
- V1.4 Requisitos arquitectónicos de control de acceso
- V1.5 Requisitos arquitectónicos de entrada y salida
- V1.6 Requisitos arquitectónicos criptográficos.
- V1.7 Errores, registro y auditoría de requisitos arquitectónicos
- V1.8. Protección de datos y requisitos arquitectónicos de privacidad
- V1.9 Requisitos arquitectónicos de comunicaciones
- V1.10 Requisitos arquitectónicos del software malicioso
- V1.11 Requisitos arquitectónicos de la lógica de negocios
- V1.12 Requisitos arquitectónicos de carga segura de archivos
- V1.13 Requisitos de arquitectura API
- V1.14 Requisitos arquitectónicos de configuración

V2: Requisitos de verificación de autenticación

- V2.1 Requisitos de seguridad de la contraseña
- V2.2 Requisitos generales de autenticación
- V2.3 Requisitos del ciclo de vida del autenticador
- V2.4 Requisitos de almacenamiento de credenciales
- V2.5 Requisitos de recuperación de credenciales
- V2.6 Requisitos del verificador secreto de búsqueda
- V2.7 Requisitos del verificar fuera de banda.
- V2.8 Requisitos del verificador único o multifactorial
- V2.9 Requisitos del verificador de dispositivos y dispositivos criptográficos
- V2.10 Requerimientos de autenticación de servicio.

V3: Requisitos de verificación de gestión de sesión

- V3.1 Requisitos de Gestión de Sesiones Fundamentales
- V3.2 Requisitos de vinculación de sesión
- V3.3 Sesión de sesión y requisitos de tiempo de espera
- V3.4 Gestión de sesiones basada en cookies
- V3.5 Gestión de sesión basada en token
- V3.6 Re-autenticación de una Federación o Afirmación
- V3.7 Defensas contra explotaciones de gestión de sesión.

V4: Requisitos de verificación de control de acceso

- V4.1 Diseño general de control de acceso
- V4.2 Control de acceso a nivel de operación
- V4.3 Otras consideraciones de control de acceso

V5: Requisitos de validación, desinfección y verificación de codificación

- V5.1. Requisitos de validación de entradas.
- V5.2 Requisitos de saneamiento y sandboxing
- V5.3 Codificación de salida y requisitos de prevención de inyección
- V5.4 Requisitos de memoria, cadena y código no administrado de
- V5.5 Requisitos de prevención de deserialización

V6: Requisitos de verificación de criptografía almacenada

- V6.1 Clasificación de datos
- V6.2 Algoritmos
- V6.3 Valores aleatorios
- V6.4 Gestión secreta

V7: Gestión de errores y requisitos de verificación de registro

- V7.1 Requisitos de contenido de registro
- V7.2 Requisitos de procesamiento de registro
- V7.3 Requisitos de protección de registro
- V7.4 Manejo de errores

V8: Requisitos de verificación de protección de datos

- V8.1 Protección general de datos
- V8.2 Protección de datos del lado del cliente
- V8.3 Datos Privados Sensibles

V9: Requisitos de verificación de comunicaciones

- V9.1 Requisitos de seguridad de comunicaciones
- V9.2 Requisitos de seguridad de comunicaciones del servidor

V10: Requisitos de verificación de código malicioso

- V10.1. Controles de integridad de código
- V10.2 Búsqueda de código malicioso
- V10.3 Controles de integridad de aplicación desplegados

V11: Requisitos de verificación de la lógica de negocios

- V11.1 Requisitos de seguridad de la lógica de negocios

V12: Requisitos de verificación de archivos y recursos

- V12.1 Requisitos de carga de archivos
- V12.2 Requisitos de integridad de archivos
- V12.3 Requisitos de ejecución de archivos
- V12.4 Requisitos de almacenamiento de archivos
- V12.5. Requisitos de descarga de archivos

V13: Requisitos de verificación de servicios web y API

- V13.1 Requisitos de verificación de seguridad del servicio web genérico
- V13.2 Requisitos de verificación del servicio web RESTful
- V13.3 Requisitos de verificación del servicio web SOAP
- V13.4 GraphQL y otros requisitos de seguridad de la capa de datos del servicio web

V14: Requisitos de verificación de la configuración

- V14.1 Construir
- V14.2 Dependencia
- V14.3 Requisitos de divulgación de seguridad no deseados
- V14.4 Requisitos de encabezados de seguridad HTTP
- V14.5 Validar los requisitos de encabezado de solicitud HTTP

De igual manera, se aplica a los siguientes dominios de la ISO 27002:

Tabla 2
Dominios ISO 27002 aplicados a los sistemas de información

A5	Políticas de seguridad de la información
A5.1	Directrices de gestión de la seguridad de la información
A5.1.1	Políticas para la seguridad de la información
A5.1.2	Revisión de las políticas para la seguridad de la información
A6	Organización de la seguridad de la información
A6.1	Organización interna
A6.1.1	Roles y responsabilidades en seguridad de la información
A6.1.2	Segregación de tareas
A6.1.3	Contacto con las autoridades
A6.1.4	Contacto con grupos de interés especial
A6.1.5	Seguridad de la información en la gestión de proyectos
A6.2	Los dispositivos móviles y el teletrabajo
A6.2.1	Política de dispositivos móviles
A6.2.2	Teletrabajo
A9	Control de acceso
A9.1	Requisitos de negocio para el control de acceso
A9.1.1	Política de control de acceso
A9.1.2	Acceso a las redes y a los servicios de red
A9.2	Gestión de acceso de usuario

A9.2.1	Registro y baja de usuario
A9.2.2	Provisión de acceso de usuario
A9.2.3	Gestión de privilegios de acceso
A9.2.4	Gestión de la información secreta de autenticación de los usuarios
A9.2.5	Revisión de los derechos de acceso de usuario
A9.2.6	Retirada o reasignación de los derechos de acceso
A9.3	Responsabilidades del usuario
A9.3.1	Uso de la información secreta de autenticación
A9.4	Control de acceso a sistemas y aplicaciones
A9.4.1	Restricción del acceso a la información
A9.4.2	Procedimientos seguros de inicio de sesión
A9.4.3	Sistema de gestión de contraseñas
A9.4.4	Uso de utilidades con privilegios del sistema
A9.4.5	Control de acceso al código fuente de los programas
A10	Criptografía
A10.1	Controles criptográficos
A10.1.1	Política de uso de los controles criptográficos
A10.1.2	Gestión de claves
A12	Seguridad de las operaciones
A12.1	Procedimientos y responsabilidades operacionales
A12.1.1	Documentación de procedimientos operacionales
A12.1.2	Gestión de cambios
A12.1.3	Gestión de capacidades
A12.1.4	Separación de los recursos de desarrollo, prueba y operación
A12.2	Protección contra el software malicioso (malware)
A12.2.1	Controles contra el código malicioso
A12.4	Registros y supervisión
A12.4.1	Registro de eventos
A12.4.2	Protección de la información del registro
A12.4.3	Registros de administración y operación
A12.4.4	Sincronización del reloj
A12.5	Control del software en explotación
A12.5.1	Instalación del software en explotación
A12.6	Gestión de la vulnerabilidad técnica
A12.6.1	Gestión de las vulnerabilidades técnicas
A12.6.2	Restricción en la instalación de software
A12.7	Consideraciones sobre la auditoria de sistemas de información
A12.7.1	Controles de auditoría de sistemas de información
A13.2	Intercambio de información
A13.2.1	Políticas y procedimientos de intercambio de información
A13.2.2	Acuerdos de intercambio de información
A13.2.3	Mensajería electrónica
A13.2.4	Acuerdos de confidencialidad o no revelación
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información
A14.1	Requisitos de seguridad en los sistemas de información
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas
A14.1.3	Protección de las transacciones de servicios de aplicaciones

A14.2	Seguridad en el desarrollo y en los procesos de soporte
A14.2.1	Política de desarrollo seguro
A14.2.2	Procedimiento de control de cambios en sistemas
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
A14.2.4	Restricciones a los cambios en los paquetes de software
A14.2.5	Principios de ingeniería de sistemas seguros
A14.2.6	Entorno de desarrollo seguro
A14.2.7	Externalización del desarrollo de software
A14.2.8	Pruebas funcionales de seguridad de sistemas
A14.2.9	Pruebas de aceptación de sistemas
A14.3	Datos de prueba
A14.3.1	Protección de los datos de prueba
A16	Gestión de incidentes de seguridad de la información
A16.1	Gestión de incidentes de seguridad de la información y mejoras
A16.1.1	Responsabilidades y procedimientos
A16.1.2	Notificación de los eventos de seguridad de la información
A16.1.3	Notificación de puntos débiles de la seguridad
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información
A16.1.5	Respuesta a incidentes de seguridad de la información
A16.1.6	Aprendizaje de los incidentes de seguridad de la información
A16.1.7	Recopilación de evidencias
A18	Cumplimiento
A18.1	Cumplimiento de los requisitos legales y contractuales
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales
A18.1.2	Derechos de Propiedad Intelectual (DPI)
A18.1.3	Protección de los registros de la organización
A18.1.4	Protección y privacidad de la información de carácter personal
A18.1.5	Regulación de los controles criptográficos
A18.2	Revisiones de la seguridad de la información
A18.2.1	Revisión independiente de la seguridad de la información
A18.2.2	Cumplimiento de las políticas y normas de seguridad
A18.2.3	Comprobación del cumplimiento técnico

Fuente: Aplicada de la norma ISO 27002 de 201, (Lopez, 2013)

Esta valoración se realizará con la siguiente tabla, la cual está basada en la matriz de valoración del modelo se seguridad y privacidad de la información planteada por el Ministerio de las TIC, (TIC M. d., INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD, 2019):

Tabla 3
Matriz MSPI propuesto por MinTIC

Escala de Valoración

Descripción	Calificación	Descripción detallada
No Aplica	N/A	No aplica.
Inexistente	0	No se aplican controles. La que la Entidad no identifica la necesidad de aplicar controles en el desarrollo de aplicaciones web o desestima la necesidad de su aplicación.
Inicial	20	No hay procesos y procedimientos estandarizados. Se identifica la necesidad de actuar de manera reactiva ante un problema de seguridad de las aplicaciones web y se aplica de acuerdo con la experiencia o conocimiento del servidor y es principalmente. Generalmente no se cuentan con procedimientos.
Repetible	40	Se formulan estandares, procesos y controles. En el proceso de desarrollo seguro de aplicaciones web se cuentan con procesos, estandares y procedimientos aplicados por los actores del ciclo de vida de la aplicación web pero no se declaran ni se comunican. Generalmente hay un alto grado de dependencia en los conocimientos del servidor a cargo con posibilidad de que se presenten errores.
Efectivo	60	Se cuenta con procesos, procedimientos y controles formulados y documentados. Se aplican los controles en el proceso de construcción de aplicaciones web por lo que es poco probable las desviaciones originadas por la falta de aplicación oportuna o acertada del control.
Gestionado	80	Se cuenta con controles que se monitorean y se miden. Con la aplicación de los controles de desarrollo de las aplicaciones web es posible monitorear y medir el nivel de cumplimiento de los procesos y procedimientos como apoyo a la toma de decisiones o medidas de acción.
Optimizado	100	Se cuenta con procesos y procedimientos aplicados desde el punto de vista de mejora continua. Esto permiten contar con procesos y procedimientos automatizados y redefinidos con base en recomendaciones de mejores prácticas y un proceso de mejora continua.

Fuente: Basado en la matriz de valoración MSPI de Min TIC, (TIC M. d., INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD, 2019)

3.5. PROCEDIMIENTOS.

Para determinar los lineamientos estratégicos de ciberseguridad y ciberdefensa se aplicaron las encuestas detalladas en el Anexo No 3 basado en el instrumento de medición propuesto por Min TIC, (TIC M. d., INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD, 2019), el cual se adaptó para valorar los diferentes aspectos plateados por OWASP (Project, Application Security Verification Standard 4.0, 2019), y de esta manera facilitar la identificación de las vulnerabilidades y a partir de estos resultados se identifica la acción de las amenazas que tiene el desarrollo de las aplicaciones web en la entidad y la gestión de los riesgos en la publicación de información en el ciberespacio. En cuanto al análisis de riesgos identificados en la publicación de información en el ciberespacio se agruparon en los siguientes aspectos:

- Administrativos.
- Estratégicos.
- Operación.

Una vez consolidada la información, se realizó una ponderación de la calificación para determinar el nivel de madurez, y los riesgos de la publicación de la información.

4. CAPITULO I – ANALISIS DE RESULTADOS DEL DIAGNOSTICO DE LA APLICACIÓN DE LINEAMIENTOS ESTRATEGICOS DE CIBERSEGURIDAD Y CIBERDEFENSA PARA EL DESARROLLO DE APLICACIONES WEB DE LA FISCALIA GENERAL DE LA NACION.

Una vez aplicados el instrumento de medición se identifica un nivel repetible ante los criterios propuestos por OWASP, para lo cual, se cuenta con el siguiente análisis:

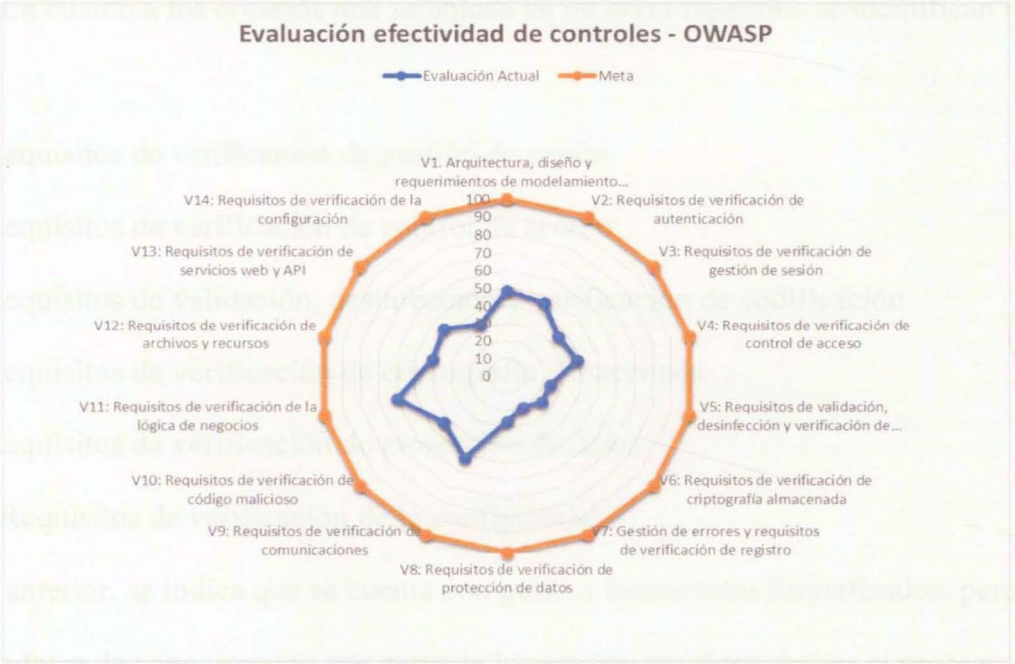

Grafico 14 Aplicación del instrumento de madurez OWASP-2019, adaptado del propuesto por MinTIC, (TIC M. d., INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD, 2019).

Tal como se indica en los resultados de la encuesta realizada, el proceso de desarrollo de aplicaciones web cuenta con nivel de efectividad en los siguientes criterios de evaluación:

V1. Arquitectura, diseño y requerimientos de modelamiento de Amenazas

V2: Requisitos de verificación de autenticación

V9: Requisitos de verificación de comunicaciones

V10: Requisitos de verificación de código malicioso

V11: Requisitos de verificación de la lógica de negocios

V12: Requisitos de verificación de archivos y recursos

V13: Requisitos de verificación de servicios web y API.

Esto obedece a que se ha creado conciencia en la importancia de la gestión de riesgos de la entidad frente a amenazas de los activos informáticos y las arquitecturas de las aplicaciones web cuentan con las bondades que permite abordar este tipo de requerimientos, sin embargo, de acuerdo con la escala de valoración, se aplican los procedimientos, pero no se miden o se valoran. En cuanto a los criterios que se ubican en un nivel repetible, se identifican los siguientes criterios:

V3: Requisitos de verificación de gestión de sesión

V4: Requisitos de verificación de control de acceso

V5: Requisitos de validación, desinfección y verificación de codificación

V6: Requisitos de verificación de criptografía almacenada

V8: Requisitos de verificación de protección de datos

V14: Requisitos de verificación de la configuración

De lo anterior, se indica que se cuenta con guías o instructivos formalizados, pero no comunicados o de conocimiento por parte de los actores involucrados en el proceso de desarrollo de aplicaciones Web. Por otro lado, se identifica en un nivel de madurez inicial el siguiente criterio: V7: Gestión de errores y requisitos de verificación de registro.

Lo anterior, obedece a que se delega esta función a las bondades de las plataformas tecnológicas y no se cuenta con controles en este sentido. El resultado del análisis se detalla de la siguiente tabla:

Tabla 4
Resultado de la aplicación del instrumento de medición.

Criterio	Descripción (aporte del autor)
V1. Arquitectura, diseño y requerimientos de modelamiento de amenazas.	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **48,4** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **efectivo.**
V2: Requisitos de verificación de autenticación	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **45,8** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **efectivo.**
V3: Requisitos de verificación de gestión de sesión	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **35** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **repetible.**
V4: Requisitos de verificación de control de acceso	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **38,8** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **repetible**
V5: Requisitos de validación, desinfección y verificación de codificación.	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **24** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **repetible.**
V6: Requisitos de verificación de criptografía almacenada	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **24** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **repetible.**
V7: Gestión de errores y requisitos de verificación de registro	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **20** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **inicial.**
V8: Requisitos de verificación de protección de datos	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **26** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **repetible**
V9: Requisitos de verificación de comunicaciones	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **52** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **efectivo**
V10: Requisitos de verificación de código malicioso	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **42** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **efectivo**
V11: Requisitos de verificación de la lógica de negocios	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **60** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **efectivo**
V12: Requisitos de verificación de archivos y recursos	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **40,6** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **efectivo**
V13: Requisitos de verificación de servicios web y API	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **43** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **efectivo**
V14: Requisitos de verificación de la configuración	Se evidencia en la encuesta que el grupo de desarrollo en cabeza del departamento de sistemas de información establece un nivel de madurez del **32** de cumplimiento de este criterio, lo que indica que se cuenta con nivel **repetible**

Fuente: Valoración de los factores propuestos por OWASP, (Novillo Vicuña J. P., 2019), aplicado a la FGN

De igual manera en cuanto a la ISO 27002, se obtiene el siguiente resultado:

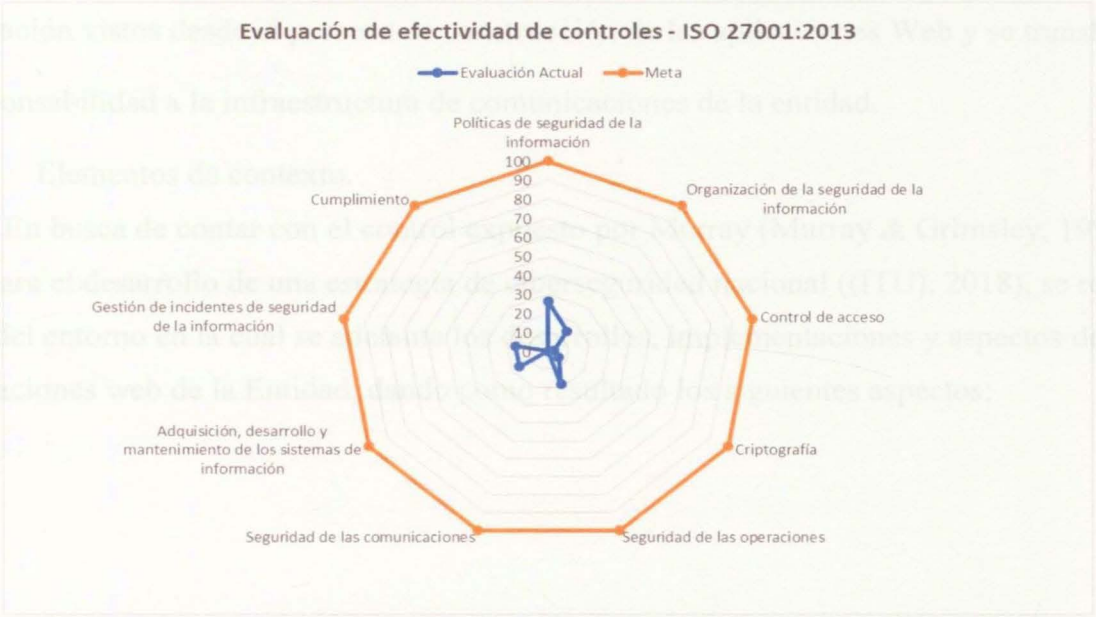

Grafico 15 Aplicación del instrumento de madurez ISO 27002-2013, adaptado del propuesto por MinTIC, (TIC M. d., INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD, 2019).

Para el dominio especifico de las aplicaciones web, se basa en los lineamientos del Ministerio de la Tecnologías de la Información y las Comunicaciones que se alinean con lo planteado con la ISO/IEC 27002 del 2013 se cuenta con un nivel inicial, tal como se identifica a continuación:

Tabla 5
Resultados de instrumento en dominios ISO 27002

No.	Evaluación de Efectividad de controles - ISO 27001:2013			
	DOMINIO	Evaluación Actual	Meta	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A5	Políticas de seguridad de la información	26,6	100	REPETIBLE
A6	Organización de la seguridad de la información	14	100	INICIAL
A9	Control de acceso	3	100	INICIAL
A10	Criptografía	6	100	INICIAL
A12	Seguridad de las operaciones	18,4	100	INICIAL
A13	Seguridad de las comunicaciones	0	100	INEXISTENTE
A14	Adquisición, desarrollo y mantenimiento de los sistemas de información	16	100	INICIAL
A16	Gestión de incidentes de seguridad de la información	16	100	INICIAL
A18	Cumplimiento	0	100	INEXISTENTE

PROMEDIO EVALUACIÓN DE CONTROLES	11	100	INICIAL

De lo anterior, se evidencia que no se cuenta con controles de seguridad en los aspectos de comunicación vistos desde el proceso de construcción de las aplicaciones Web y se transfiere esta responsabilidad a la infraestructura de comunicaciones de la entidad.

4.1. Elementos de contexto.

En busca de contar con el control expuesto por Murray (Murray & Grimsley, 1994) y en la guía para el desarrollo de una estrategia de ciberseguridad nacional ((ITU), 2018), se realiza el análisis del entorno en la cual se adelanta los desarrollos, implementaciones y aspectos de uso de las aplicaciones web de la Entidad, dando como resultado los siguientes aspectos:

Tabla 6
- Elementos de Contexto del desarrollo web

Aspecto	Componente	Análisis (aporte del autor)
Político	Política de seguridad digital del estado colombiano.	Con el reconocimiento del ciberespacio como un dominio que requiere protegerse ante las amenazas emergentes, tal como se indica el informe efectuado por el BID y OEA en el 2016, (BID, 2016) se han desarrollado políticas en el entorno latinoamericano para combatir las incidencias de ciberseguridad, (Conexionesan, 2018) y dotar a los estados de condiciones de seguridad en la publicación de servicios de información en el ciberespacio y de la infraestructura asociada a ello en donde se identifican las siguientes iniciativas: Formulación de estrategias de seguridad. Se cuenta con la interacción de los diferentes actores privados o públicos que soportan los servicios de información, permite implementar políticas y normas legales para reglar la difusión de nuevas tecnologías en Internet, las empresas multinacionales y los beneficios de nuevas operaciones ubicadas en el exterior. Formulación de política de seguridad. Para el caso colombiano se cuenta con la Formulación de la política de seguridad digital (Planeación, 2016) en la que el sector judicial tiene un papel primordial como es la seguridad del ciberespacio frente a los efectos que tienen los delitos informáticos o inclusive de las amenazas de los activos nacionales del ciberespacio. Creación de políticas de protección de la información pública y la infraestructura crítica soportadas en modelos de gestión estatales como las arquitecturas empresariales públicas que exigen más especialización en actividades misionales y de mayor eficiencia en las actividades a desarrollar por terceros y las necesidades de calidad y seguridad del proceso, ocasionando que se contrate los servicios de bajo valor agregado. Desarrollo y fortalecimiento de tecnologías aplicadas en seguridad, así como la gestión de los diferentes proveedores de servicios de información en el ciberespacio. Con la política nacional de seguridad se busca proteger los valores nacionales y en particular en la dimensión jurídica la Fiscalía General de la Nación como apoyo a la gestión de los riesgos internos para mantener la capacidad de servicios esenciales de justicia en el entorno digital. La Fiscalía General de la Nación como líder de la Policía Judicial colombiana, establece políticas y estrategias para combatir el delito y entre ellos los delitos informáticos en correspondencia con la evolución de los ataques cibernéticos. Razón por la cual requiere protección de su infraestructura critica como objetivo de ataques o el mismo intercambio de información entre las diferentes entidades del estado colombiano o con empresas privadas, (Owens., 2007).
Económico	Costo/beneficio de la publicación de información estatal en el ciberespacio.	En la región latinoamericana y específicamente en el caso colombiano, la publicación de servicios de información y de la gestión de la infraestructura critica que lo permite surge un elemento dinamizador de la economía en cuanto a la generación de una demanda de bienes y servicios del sector justicia para el ejercicio de las actividades económicas del país en cuanto a la investigación y judicialización de los delitos.

Económico	Racionalización de los recursos económicos asignado al sector público.	La racionalización de los recursos económicos del sector se traduce en la implementación de alternativas en la formulación y ejecución de proyectos de inversión que incluye el desarrollo de software, generando nuevos mecanismos de control y aseguramiento desde la adquisición, la construcción y el mantenimiento de las aplicaciones web que tienen como objetivo convertirse en un medio de publicación de servicios de información en el ciberespacio. Por lo tanto, la racionalización de recursos tecnológicos se traduce en la disgregación y reutilización de componentes de la arquitectura de las aplicaciones web como característica de los modelos de gestión de soluciones tecnológicas que buscan reducir costos. Por esta razón, las actividades de desarrollo de software generan nuevos vectores de ataque personalizados a las condiciones de desarrollo de la industria de software y del portafolio de servicios que establecen nuevas condiciones de desarrollo económico y social de la región. Otro efecto, corresponde a las donaciones de software que genera compromisos tanto presupuestales y de formación no planificados inicialmente y que generan en algunos casos vulnerabilidades en la búsqueda de soluciones.
Económico	Contratación de servicios de desarrollo seguro de aplicaciones web.	Debido a las limitaciones del conocimiento del personal destinado a los proyectos del desarrollo de información, las entidades buscan como alternativa la contratación del desarrollo en la región, es decir de empresas que tienen las suficientes garantías financieras en condiciones de competitividad que se traduce en una eventual monopolización por las grandes compañías o multinacionales que cuentan con la capacidad de atender los requerimientos de software del sector gubernamental, tanto como funcionales, técnicos y de transferencia de conocimiento en las condiciones impuestas. El nivel de contratación permite medir el comportamiento del mercado del software estatal que se relaciona con las capacidades de desarrollo interno estatal y que mide de igual manera el nivel de conocimiento de las plataformas y herramientas adquiridas por parte de las organizaciones que pueden afectar de manera controlada el desarrollo económico del país y adaptarse a las condiciones del entorno. Por ejemplo, en el caso uruguayo, se centra en las exportaciones. En Brasil, se centra el uso de la informática en las actividades financieras, y en el caso chileno, se evidencia una acción más integral en las actividades económicas. Lo que sí es común en el sector en la región de América Latina, es el desarrollo en los segmentos de servicio, para equipos y sistemas, y software como producto. Ya en 2005, las empresas más grandes de la región, contaban con aproximadamente un millón de empleados y una facturación de 300.000 millones de dólares, que según WITSA (2006), equivale al 30% del mercado mundial de software y servicios. Con los servicios de protección del estado colombiano, la policía judicial colombiana debe dar las condiciones de seguridad para realizar las actividades económicas que se surten en el ciberespacio, como es el caso de los servicios esenciales de las personas naturales o jurídicas. Pese a esto, son pocos los países o las regiones que pueden explotar al máximo los ofrecimientos y potencialidades de las empresas que ofrecen programas o de los servicios de soporte, que, desde las políticas públicas ya definidas en el sector, es el cumplimiento de las leyes de propiedad intelectual.

Social	Conciencia de ciberseguridad en los responsables del diseño e implementación de servicios que se ofrecen a los usuarios del sector justicia.	Con la creación de una conciencia de ciberseguridad en los ciudadanos en particular lo relacionado con la protección de los derechos humanos y de la infancia en el ciberespacio en cuanto otros factores a la explotación sexual o a los ataques de ingeniería social, la Fiscalía General de la Nación monitorear las consecuencias de estas acciones entendida como uno de los vectores de ataque a analizar en los diferentes delitos cometidos en el ciberespacio. Por lo anterior, desde el aspecto social se da más relevancia al fortalecimiento de la infraestructura crítica de las naciones para atender las necesidades de conocimiento de la sociedad, con lo que se ha creado una credibilidad en soluciones tecnológicas a la seguridad del software que apoya los procesos misionales. Otro factor, es la creación de una suficiencia de conocimiento en temas de seguridad a los proveedores de hardware y software comercial, o en algunos casos delegar la responsabilidad del fortalecimiento a los proveedores de plataformas en la nube, para enfocarse en la operación de las aplicaciones web que requiere una organización para funcionar.
Social	Los riesgos que enfrenta la sociedad en el ciberespacio y la atracción que ejerce el mundo hacker en la sociedad.	Con el reconocimiento social que tiene un ciberdelincuente que contrario a las consecuencias de sus actividades delictivas se mantiene el reconocimiento social por el nivel de conocimiento y habilidades que conlleva el logro de cometer un ciberdelito. Esto se presenta por la falta de capacidad de reacción en el ciberespacio para la judicialización del delito cibernético con lo que una estrategia de ciberseguridad y ciberdefensa cobra importancia soportada por la política de seguridad en Colombia. De lo anterior, y tal como se plantea en la política de seguridad digital colombiana se busca crear una conciencia de ciberseguridad y ciberdefensa en el pueblo colombiano con la ayuda de tecnologías y servicios en la nube, especialmente en la población joven con la que crecen y se desarrollan con estas facilidades, lo que hace pensar en una higiene en el ciberespacio.

Social	Acciones de respuesta del estado en el sector justica.	En cuanto a los requerimientos de ciberseguridad, que según lo descrito por Deloite 2016 en la encuesta 2016 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Latinoamérica, en la región se identifican las siguientes tendencias: Cuatro de cada 10 organizaciones cuentan con un SOC (security operation center), es decir menos del 20% de las organizaciones. Existe una limitación importante en cuanto a presupuesto en la región para fortalecer los CISOS. En materia de la gestión de ciber-riesgos, menos del 10% de las organizaciones tienen tableros de indicadores (kpis). Durante el 2016, se incrementaron las acciones de concientización en materia de seguridad. En este sentido y de acuerdo con lo establecido en la política de seguridad digital del estado colombiano, conpes 3854, (República de Colombia, 2016), la Fiscalía General de la Nación cumple un rol en la judicialización en coordinación con los actores de la Rama Judicial y los miembros de la Policía Judicial, que ofrecen servicios de información en el ciberespacio relacionados con los procesos investigativos para combatir los diferentes delitos establecidos en el código penal. Para el caso específico de la FGN, la información a publicar en internet se relaciona con los procesos de denuncia o de investigación solicitada por los ciudadanos como víctimas y que en el ámbito del cibercrimen. Con esto, se considera como respuesta ante un tipo de delito especializado unos procedimientos particulares por sus componentes tecnológicos de información y de comunicaciones obligando a la entidad generar capacidades de investigación y judicialización particulares del sector.
Social	El impacto social de las aplicaciones web en el ciberespacio.	Para comprender el papel que debe cumplir las aplicaciones web de la Entidad frente al proceso judicial que describe la política de seguridad digital del estado colombiano, se centra en el papel que cumple los servicios de información de los delitos que se ofrece a los interesados en el ciberespacio para convertirlos en actores activos en el servicio de justicia y en este aspecto, la FGN cuenta con la arquitectura empresarial en el marco de gobernabilidad de la plataforma tecnológica y de la gestión de los riesgos que se presentan en un servicio de ciberjusticia, en donde no solo es un medio de prestación de servicios, sino que es un entorno que requiere seguridad.

Social	Generación de conocimiento en el desarrollo de aplicaciones web en el sector académico y comercial.	Con la articulación de la academia y el uso de tecnologías en el sector gobierno, se genera un portafolio de problemas específicos para la investigación, el desarrollo e innovación en cuanto al desarrollo seguro de aplicaciones web que soporten los servicios tecnológicos en el ciberespacio. Por esta razón, la Fiscalía General de la Nación cuenta con un departamento de altos estudios que contempla inicialmente proyectos de ID+i en área de la investigación del delito, pero no se evidencia en proyectos específicos del delito ocurrido en el ciberespacio o de lo relacionado con el fortalecimiento de la infraestructura critica de la nación, tal como sucede con los atentados que son objeto los oleoductos o el sistema de trasporte, entre otros. En este sentido, por el rol investigativo y de acusatorio de la Fiscalía en el ámbito de ciberdefensa, debe contar con herramientas informáticas que apoyen el ejercicio de su misión y de las actividades propias de la gestión interna, analizados desde la dinámica de innovación tecnológica (technology push) o de la demanda tecnológica (market pull), aplicada de manera articulada con los modelos de gestión integrada del sector público y la política de seguridad digital del estado colombiano. En cuanto a la gestión de proyectos de Aplicaciones web, se requiere personal altamente calificado bien sea para la gerencia de proyectos de software o de adquisición de tecnología o tercerización para automatizar sus procesos y la mejora de la eficiencia de la Entidad. Así, es necesario desarrollar programas de enrolamiento y desarrollo del talento humano necesario para satisfacer de manera articulada las necesidades en materia de Aplicaciones web, e inclusive mejorar un proceso desde las TIC, y otras áreas de conocimiento. Otro aspecto en cuanto al talento humano es que una vez logrado el nivel de conocimiento requerido, surge un nuevo factor de retención del personal mediante incentivos salariales o de conocimiento. En este sentido, en cuanto a las políticas públicas el desarrollo de la industria de software en América Latina tiene como objetivos: Empleos calificados. Exportación de software y servicios. Valor agregado por la implementación de aplicaciones web
Social	Uso de servicios de información en el ciberespacio.	En cuanto al impacto que tiene el uso de las aplicaciones web y de sus componentes de software en la sociedad es evidente que debe ser analizado con las directrices emitidas por el ministerio de la TIC y de los servicios que se le debe ofrecer al ciudadano y complementar este análisis en el nivel de seguridad. Esto se traduce en los lineamientos de formulación de la estrategia empresarial para el estado y de la importancia en establecer los requerimientos de seguridad a cumplir con los controles de desarrollo, pruebas, implementación y mantenimiento. Con estos criterios y características de las aplicaciones web implementados en las Entidades, aunque genere un incremento en los costos de diseño, desarrollo, implementación y mantenimiento, se ve reflejado en la eficacia, efectividad, integridad y disponibilidad de la información que requiere el servicio que ofrece la Entidad en el sector justicia.

Social	La importancia de la ciberdefensa en la sociedad.	Con la importancia de la infraestructura tecnológica que soportan los servicios de justicia en el ciberespacio evidenciada en el momento de los fallos de disponibilidad para los usuarios de los servicios de investigación y judicialización en el ciberespacio, se ha creado una conciencia inicial de la necesidad de actuar coordinadamente con el estado para salvaguardar la infraestructura y los servicios de información de ataque procedentes de fuerzas hostiles de organizaciones al margen de la ley que tienen un alcance transnacional que generan nuevas barreras en la acción coordinada con diferentes países como son los derivados de la cultura, etnias, sistemas de justicia, condiciones de género, poblaciones minoritarias y del idioma entre otros, así como las condiciones culturales de educación y canales de comunicación, (Batista-Canino, 2016) para adoptar normas, niveles de calidad, compromisos y confiabilidad, es decir el desarrollo de habilidades culturales y técnicas.
Tecnológico	Arquitectura Institucional.	Con la resolución No 1165 se formalizó el esquema de gobierno, (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018) y se enmarca en modelo de arquitectura empresarial establecido por Min TIC, (TIC M. d., Arquitectura TI Colombia, 2019).
Tecnológico	Estrategia de Tecnologías de la Información	Dado que la estructura de gobierno, lineamientos, procesos y servicios establecen las directrices para la gestión de la arquitectura de la entidad, se establece como base el plan estratégico de TIC de la entidad para dinamizar el desarrollo tecnológico que establece el direccionamiento estratégico de la entidad y en particular el contexto de la estrategia de ciberseguridad y ciberdefensa para el desarrollo e implementación de aplicaciones web para la publicación de información en el ciberespacio.
Tecnológico	Gobierno de Tecnologías de la Información.	En el marco de la arquitectura empresarial de la FGN se define las áreas responsables de ejercer el gobierno de tecnologías de la información para atender todos los manejadores de la arquitectura y lograr alinear los diseños con las directrices de la planeación estratégica.
Tecnológico	Análisis de la Información.	La entidad por su carácter investigativo involucra en su gestión los procesos de análisis de datos de comportamiento criminal, enmarcado en el gobierno de la información para planificar una adecuada gestión, datos, servicios y flujos de la información. En el marco del sistema de gestión integral de la entidad, se realiza una identificación y caracterización básica de los componentes de la información.
Tecnológico	Apropiación y uso de las Tecnologías de la Información	De la gestión de la información se generan procesos relacionados con el apoyo para la toma de decisiones con respecto al comportamiento criminal en el estado colombiano.
Tecnológico	Sistemas de Información.	Dentro de la arquitectura empresarial de la FGN se establece lineamientos para la construcción de software como uno de los requisitos a aplicar en el desarrollo de las aplicaciones web que aborda todas las necesidades de automatización de proceso con características de calidad y dentro de ellos las características de seguridad a tener en los productos desarrollados.
Tecnológico	Gestión de servicios de TI.	Dentro de la arquitectura empresarial de la FGN se establece lineamientos para el diseño de servicios tecnológicos que en primera instancia no contempla un factor diferenciador con los servicios tecnológicos que utiliza la entidad y ofrece a la ciudanía en el ciberespacio sino que lo aborda de manera general.

Legales	Leyes relacionadas al sistema de justicia penal del estado colombiano.	Es necesario resaltar que las aplicaciones web de la entidad atienden las necesidades de automatización de los procesos misionales que son implementados en respuesta a la aplicación de la siguiente normatividad: Código de procedimiento penal consignado en la ley 600 de 2000 y en la ley del sistema penal oral acusatorio, Ley 906 de 2004. Ley de justica transicional, ley 975 de 2005. Ley de infancia y adolescencia, ley 1098 de 2006. Ley de víctimas, ley 1448 de 2010. Como producto de lo anterior, el desarrollo de software se ve relacionado con un marco normativo dinámico que debe contemplar las normas en cuanto a los servicios informáticos y de la información propia de la Entidad que soportan los servicios a ofrecer el ciberespacio y que requieren de Ciberseguridad y Ciberdefensa. Por esta razón, se debe evaluar las exigencias y requerimientos a cumplir en cuanto a normas en el momento de desarrollar, implementa o usar un sistema de información en la Entidad, así como cumplir con estándares internacionales que buscan preservar los derechos de los ciudadanos en el ciberespacio y del mismo estado.

Legales	Protección de datos e información del estado y de los ciudadanos.	En lo referente a la ley 1712 de 2014, en su Artículo 2 establece como "principio de máxima publicidad para titular universal", que la información es de carácter pública en lo referente a la "posesión, control o custodia" efectuada por un sujeto obligado y por lo tanto no es reservada o limitada, a menos que por disposición constitucional o legal lo establezca de esta manera. Establece un criterio significativo en la implementación de la seguridad de las aplicaciones web y en particular de los procesos referente su uso y su consulta. En este aspecto, el artículo 3, también indica principios de transparencia y acceso la información pública, con un atenuante como es el concepto de "razonabilidad y proporcionalidad", que indudablemente debe tenerse como criterio de diseño de un sistema de información. Para este efecto, la norma establece los siguientes principios a tenerse en cuenta: Principio de transparencia. De los sujetos obligados, se presume la información de carácter pública, por lo que en las aplicaciones web se debe implementar los mecanismos necesarios para en las condiciones establecidos en la ley, proporcionen y facilite el acceso. Principio de buena fe. Se presume que los accesos se realizan con "motivación honesta, leal y desprovista de cualquier intención dolosa o culposa", sin embargo, en las aplicaciones web, más concretamente en el software se deben implementar mecanismos de registro y control. Principio de facilitación. Dada la exigencia a los sujetos obligados, se debe implementar mecanismos de acceso en el "ejercicio del derecho de acceso a la información pública", sin perjuicio de implementar mecanismos de control. Principio de no discriminación. Las aplicaciones web deben contemplar mecanismos de entrega igualitaria y monitoreada de información a todas las personas que lo soliciten conforme lo establezca la ley y los procedimientos establecidos. Principio de gratuidad. Los servicios que soportan los Sistemas de Informacion deben cumplir con un acceso gratuito a la información pública sin costo adicional por su reproducción. Principio de ce!eridad. Esta es una exigencia compleja de soportar por un sistema de información, debido a factores de demanda y usabilidad, y que se refleje en la agilidad en el trámite y la gestión administrativa. Principio de eficacia. El sistema de información debe propender por facilitar los resultados de la gestión de una Entidad, evidenciando las responsabilidades frente a la "efectividad de los derechos colectivos e individuales". Principio de la calidad de la información. Se deben contemplar los controles y mecanismos de control de desarrollo seguro para permitir que la información sea "oportuna, objetiva, veraz, completa, reutilizable, procesable y estar disponible en formatos accesibles". Principio de la divulgación proactiva de la información. El sistema de información debe facilitar el proceso de dar respuesta a las peticiones de la sociedad y preservar la transparencia, es decir facilitar la publicación y divulgación de "documentos y archivos". Principio de responsabilidad en el uso de la información. Este aspecto recae en los controles de acceso, control y auditoria que debe tener un sistema de información.

Legales	Normas de política de seguridad digital.	En el conpes 3854, (República de Colombia, 2016), se hace referencia a una normativa nacional, parte de los siguientes fundamentos constitucionales: El fin esencia del Estado en la promoción de la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución. La obligación del Estado para respetar y hacer respetar los derechos fundamentales como es el caso del derecho a la intimidad personal y familiar y al buen nombre, (capítulo 1 del título II, Articulo 15). Libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación (capítulo 1 del título II, Articulo 20) El espectro electromagnético es un bien público inajenable e imprescriptible sujeto a la gestión y control del Estado (artículo 76). El espectro electromagnético como parte del territorio colombiano (artículo 101) Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional, entre otros (artículo 217).
Legales	Otras disposiciones.	Marco institucional claro. Con la definición de los objetivos económicos y sociales de la política de seguridad digital del estado colombiano se determina los lineamientos que debe adoptar la Entidad ante la gestión del riesgo en el ciberespacio definiendo el empoderamiento, responsabilidad, recurso humano, ética, cooperación, medidas de seguridad, desarrollo de capacidad, innovación y respaldo de la alta dirección. Con la administración de justicia basada en el procedimiento penal establecidas en las leyes 1273 de 2009 y 1453 de 2011, de las actividades basadas en el comercio electrónico, explotación sexual de menores, racionalización de trámites, derechos de autor, habeas data, firma electrónica, mecanismos de autenticación, entidades de certificación, registro nacional de bases de datos, servicios de comunicaciones, interceptaciones, certificados digitales, protección de datos personales, entre otros, la Fiscalía General de la Nación debe ofrecer los servicios de investigación y reparación del ciberdelito. Ver anexo 12. Relación de normas a cumplir.
Legales	Normas	Se cuenta con la arquitectura Institucional - Resolución 1165 de 2018 de la FISCALIA GENERAL DE LA NACIÓN la cual responde a los lineamientos del ministerio de las TIC que a su vez está basada en la ISO/27001:2013. ISO/31000 NIST 800 ISO/22300 y OWASP

Organizacionales de la FGN	Estratégico	Entendimiento estratégico, este comprende el entendimiento de la estrategia, de la dinámica organizacional y el análisis del desempeño estratégico. Direccionamiento estratégico de TI, esto incluye la identificación de retos y oportunidades de TI, definición de iniciativas estratégicas de TI, Identificación de políticas de TI. Implementación estratégica de TI, con la definición de portafolio de planes, programas y proyectos de TI. Gestión de recursos Financieros, Hoja de ruta de las iniciativas de TI, Definición de la oferta de servicios de TI. Seguimiento y evaluación de la estrategia de TI, para lo cual se debe realizar el seguimiento a desempeño y cumplimiento, y la implementación de tableros de control. Gobernabilidad: Como apoyo en la gestión de la gobernabilidad de la seguridad del entorno digital del estado colombiano, la Fiscalía General de la Nación requiere e su función de ente investigador proteger su información e infraestructura critica para que no se vea afectada por los ciberataques a los servicios e infraestructura de la nación.
	El dominio de Gobierno de TI:	Cumplimiento y alineación, para lo cual se debe realizar la alineación con el modelo integrado de gestión, valor y riesgo de TI, regulación externa, desarrollo e incorporación de políticas de TI. Marco de gobierno de TI, en cuanto a los procesos y calidad de TI, relaciones y toma de decisiones, recursos y capacidad de TI, gestión de talento humano. Gestión integral de proyectos TI. En cuanto al direccionamiento de proyectos TI, seguimiento y evaluación de proyectos de TI. Gestión de operación de TI, en la presentación de servicios de TI y gestión de proveedores de TI.

El dominio de la información	Los servicios de información publicados en el ciberespacio se realizan mediante la página de la entidad y servicios web que consumen las entidades que en su función requieren de ella como es el caso de la policía judicial compuesta por la Fiscalía General de la Nación, Procuraduría General de la Nación, Contraloría General de la República, Migración Colombia, Entidades públicas que ejerzan funciones de vigilancia y control, Alcaldes e inspectores de Policía y Autoridades de tránsito, (Nación F. G., Manual Único de Policia Judicial, 2019). En cuanto a los servicios de información a los cibernautas se cuenta con información de denuncias en línea, consulta de las noticias criminales, datos estadísticos de la gestión de la lucha contra la criminalidad, información de procesos contractuales, información de algunos bienes de extinción de dominio, información organizacional de la entidad. La mayoría de la información de los indicadores contenidos en este informe proviene de los sistemas de gestión de casos, sobre todo el SPOA y el SIJUF.A partir de los servicios, información y los datos, se de establecer los componentes de información, su flujo en la entidad que contemple los aspectos de seguridad, trazabilidad, aseguramiento, control de calidad y trasparencia. Planeación y Gobierno. Que incluye gestión de la calidad y seguridad. Diseño, que incluye arquitectura, diseño detallado y diseño de canales de acceso. Ciclo de vida, en cuanto a su gestión, flujos de intercambio entre los componentes de información, consolidación, mantenimiento y evolución. Análisis y aprovechamiento, en sus aspectos de publicación y transacciones, tendencias y relaciones, así como el análisis y toma de decisiones. En cuanto a las aplicaciones web que soportan los servicios de información en la entidad, se encuentra descritos en el plan estratégico, (Nación F. G., Plan estratégico 2016-2020, 2018), en donde se relaciona: SPOA para apoyar la gestión de casos con la Ley 906 de 2004 y la Ley 1098 de 2006 SIJUF para apoyar la gestión de casos por la Ley 600 de 2000 SIJYP para apoyar los procesos de la Ley 975 de 2005 -Ley de Justicia y Paz-) SIG para apoyar la gestión de actividades de policía judicial SISAC para apoyo del análisis criminal de la información de las investigaciones penales. SIAN para el apoyo de anotaciones judiciales SIAN SIAF para apoyar la gestión administrativa FEAB para apoyar la gestión del Fondo Especial de Bienes SICNEXT para apoyar la gestión de los procesos de extinción de dominio.

El dominio de aplicaciones web:	Una vez definido el direccionamiento estratégico, los apoyos, aspectos misionales y la necesidad de portales digitales, que contemple los aspectos de calidad y seguridad, trazabilidad, aseguramiento, control de calidad y trasparencia.se debe establecer: Planeación y gestión, en donde se debe planear las aplicaciones web, establecer la organización y gestión, alineación con los procesos de TI. Diseño, en cuanto a la arquitectura y diseño detallado. Ciclo de vida, en cuanto a los requerimientos, desarrollo, pruebas, implantación y despliegue, así como su mantenimiento. Soporte, entrega, gestión de cambio, servicios de soporte. Aplicaciones web, la entidad cuenta con aplicaciones web para satisfacer las necesidades de automatización y control de la información los cuales requieren de un proceso de integración que permita aplicar estándares como CMMI, así como de lineamientos para su gestión dentro de una arquitectura empresarial con una arquitectura definida para implementar nuevas funcionalidades o el desarrollo de nuevos aplicaciones web en el marco de un ciclo de vida de software, que garanticen aplicaciones que se ajusten de manera natural a los procesos establecidos para emplear en su implementación y soporte.
El dominio de servicios tecnológicos	Los aspectos de calidad y seguridad, trazabilidad, aseguramiento, control de calidad y trasparencia se establecen de acuerdo con: Arquitectura en su diseño y catálogo de servicios tecnológicos. Calidad, con la capacidad para proveer servicios e infraestructura, alineación con necesidades, reutilización de servicios e infraestructura. Operación, con la continuidad y operación de servicios tecnológicos de terceros. Soporte y mantenimiento. Servicios Tecnológicos desde la óptica de estándares como ITIL V3 paras linear la gestión de la infraestructura tecnológica, los servicios tanto misionales como de apoyo que redunden en adecuada operación y capacidad de los servicios de TI, y la prestación de servicios de soporte.
El dominio de uso y apropiación	Movilización de los grupos de interés. Con la visión compartida, liderazgo visible y redes de involucramiento. Formación y desarrollo de capacidades, con las competencias y prácticas de TI, gestión de conocimiento. Desarrollo de programas y herramientas de gestión del cambio, con la gestión de impactos, alistamiento hacia el cambio, sostenibilidad del cambio. Gestión de indicadores de uso y apropiación, con el monitoreo de uso, medición de impactos. Uso y Apropiación, aunque se cuenta con estándares y lineamientos para el Uso y apropiación de TI enmarcados en una gestión del cambio donde se involucre las áreas benefactoras de TI, es necesario establecer este aspecto desde el punto de vista de las aplicaciones web.
Estrategia de TI,	la Entidad cuenta con el direccionamiento estratégico del cual se desprende las necesidades de contar con plataformas tecnológicas que atienda los estándares y principios de formulación para alinearse con las necesidades del entorno nacional, e decir con las estrategias del Estado y del sector.

	Gobierno de TI	Sistema integrado de calidad de la Entidad, se evidencia un marco que recoge la definición de estándares y lineamientos de gobernabilidad de TI y de gestión de proyectos, en la que se debe buscar dar un apoyo efectivo a la ejecución de los procesos de la entidad en coherencia con el cumplimiento de las políticas, procesos y estructura organizacional de TI. Proceso sistemático. A partir del sistema de gestión integral en su componente de sistema de gestión de seguridad de la información define los procesos de manera sistemática para identificar los activos a proteger en el ciberespacio, la valoración de riesgos y las acciones necesarias para mitigarlas
	ley orgánica que establece las funciones de la Fiscalía General de la Nación	- Generación de capacidades de Ciberseguridad y Ciberdefensa. - Cooperación internacional y cooperación entre múltiples partes interesadas, para desarrollar una estrategia escrita para la cooperación internacional que aborde la ciberseguridad y el cibercrimen, donde se identifiquen prioridades, socios internacionales y objetivos. Fortalecer las funciones de la cancillería, en materia de cooperación internacional para la ciberseguridad. Crear la posición de coordinador de la política cibernética internacional, cuya tarea principal será la implementación de la estrategia de cooperación internacional. Establecer un mecanismo de cooperación formal entre el gobierno y el sector privado, que sea seguro para el intercambio de información de incidentes de ciberseguridad nacional e internacional. Implantar un plan de capacitación internacional apoyado por los altos niveles del gobierno para disminuir la brecha del conocimiento. Facilitar el intercambio de datos con respecto a incidentes de ciberseguridad (International Watch and Warning Network, Forum for Incident Response). Colombia deberá adherir al sistema I-24/7 de INTERPOL para todas las unidades de las fuerzas de seguridad del cibercrimen en Colombia. Fortalecer el conocimiento académico en ciberseguridad. Establecer un marco para facilitar el intercambio directo de información entre equipos de respuesta e incidentes cibernéticos de otros países. Asegurarse que todas las actividades internacionales que involucren el intercambio de datos personales respeten las leyes internacionales de derechos humanos (derecho a la privacidad).

	Otros aspectos tecnológicos.	De acuerdo con el planteamiento de Goldblat, uno de los factores para lograr un adecuado desempeño en las organizaciones, y en particular en la Fiscalía General de la Nación, es contemplar un modelo para la mejora de procesos en materia de TI, como es el caso CMMI, (Goldblat, 2013), en donde se busca mantener un adecuado nivel de calidad de los productos o servicios a partir de las personas, procesos y herramientas. En este sentido, se debe enmarcar este modelo dentro de las limitaciones propias del sector público como lo es la programación de los ciclos fiscales y la disponibilidad de recursos, buscando un punto de equilibrio de dichos recursos expresados en tiempos, presupuesto, herramientas tecnológicas y exigencias en la calidad en los requerimientos, (Goldblat, 2013). La Fiscalía General como parte del sector justicia se debe preocupar por la adaptación de su gestión de riesgos de ciberseguridad de acuerdo con los avances tecnológicos y amenazas cibernéticas que esto conlleva. En cuanto al componente de talento humano requerido para el desarrollo, la implementación y uso de aplicaciones web, es necesario resaltar que se fundamentan en el conocimiento, las habilidades, motivaciones y entrenamiento de este componente, (Goldblat, 2013), con lo que se buscará implementar métodos de desarrollo de software más eficientes y consistentes. Otro componente son los procesos, que tomando el planteamiento de Goldblat, se deben orientar los esfuerzos de los gerentes y administradores de TI hacia el mejoramiento de los procesos así como mantenerlos en un alto nivel de madurez, (Goldblat, 2013). En cuanto al uso de herramientas que permitan articular las capacidades del talento humano y los procesos, son precisamente las aplicaciones web, aplicaciones y software los que deben acelerar y automatizar los procedimientos de trabajo. En este nivel, para establecer una metodología confiable y oportuna de desarrollo se propone como estándar SCRUM, con miras a lograr una reducción de tiempo y atender de manera adecuada la complejidad de los requerimientos y la variabilidad de acuerdo con la evolución de la Entidad.
	Formulación de Control Objetives for Information and Related Technology COBIT 5.0	La Fiscalía General como parte del sector justicia se debe preocupar por la adaptación de su gestión de riesgos de ciberseguridad de acuerdo con los avances tecnológicos y amenazas cibernéticas que esto conlleva.

control de la Información y de la tecnología utilizada	Con la, que tiene como objetivo el, es de gran importancia analizar los aspectos de seguridad, es así que plantea un marco de referencia para establecer los procesos, mejores prácticas y gestión de riesgos para fortalecer la gobernabilidad, formulación de políticas y control de la implementación y sostenibilidad de la infraestructura tecnológica mayormente alineada con la arquitectura empresarial de la entidad y con el direccionamiento estratégico en la que se da principal atención a la seguridad en términos de requisitos de negocio a controlar como: Requisitos de negocio Descripción en términos de seguridad de información en la Entidad. Confidencialidad. Protección de información contra la relevación no autorizada. Integridad. Precisa, completa y valida de acuerdo con los valores del negocio. Disponibilidad. Congruente con los procesos del negocio, oportuna, correcta consistente y utilizable. Confiabilidad. Disposición de información veraz y apropiada para la toma de decisiones. Efectividad. Disponer de información relevante, oportuna, consistente, correcta y utilizable en los procesos Eficiencia. En la estrategia 2016-2020, es establece como una austeridad estratégica para el logro de los objetivos organizacionales. Cumplimiento de normativa Cumplimento de a normas, leyes, regulaciones y acuerdos vigentes. Una vez identificados estos requisitos de la alta gerencia, en cuanto a la planeación de la estrategia de seguridad de la información, se tienen en la entidad los procesos enmarcados en la arquitectura empresarial en términos de las siguientes tareas: 1. Evaluación de riesgos. 2. Planeación de calidad. 3. Administración de la capacidad. 4. Administración del desempeño. Dentro de los procesos de gobernabilidad de la información se resaltan las siguientes actividades:

Manejadores en el uso de recursos.	El lineamiento estratégico contempla aspectos como talento humano, tecnologías y la estructura a formular, tal como lo plantea Owens (Owens, 2016), y sus aspectos a tener en cuenta en los siguientes términos: - En la estrategia se deben definir las prioridades dado un entorno limitado por diversos factores, Owens (Owens, 2016), con el fin de establecer criterios de asignación de recursos para incluir los intereses y amenazas que en el momento de analizar los riesgos lo harían parecer iguales. - Capacidad de la plataforma tecnológica. - Perfiles de usuarios con acceso a la información y servicios asociados como lo son usuarios de consulta, administrativos y de auditoría de las aplicaciones web. - Desarrollo de sistemas. En este aspecto la entidad establece dentro la arquitectura informática los componentes para permitir el diseño, desarrollo e implementación de aplicaciones web en cuanto a comunicaciones, procesamientos, almacenamiento y auditoria, mediante una infraestructura propia para el desarrollo o la adquisición de aplicaciones web. - Manejo del cambio y gestión de los riesgos identificados en el proceso de desarrollo de aplicaciones web. - Administración de la configuración. Dentro del modelo de ITIL implementado en la entidad en materia de gestión de servicios de TI, se permite definir el portafolio y catálogo de servicios que se ofrecen a los usuarios internos.

Lineamientos Min TIC	En cuanto a los siguientes objetivos estratégicos, (Nación F. G., Plan estratégico 2016-2020, 2018) se encuentra un especial interés por cumplir con los lineamientos dados por el Ministerio de las Telecomunicaciones de la Tecnologías y las Comunicaciones, (Ministerio de las TIC, s. f.), que se basa en TOGAF. (Martín Darío Arango, 2015), y que corresponden con lo formulado por la IEEE, (42010, 2018) en cuanto a sus componentes de arquitectura empresarial para apoyar los objetivos institucionales que se resumen de la siguiente manera: 1. Priorización de la investigación y judicialización, en la que se busca aumentar la efectividad de las capacidades de lucha contra los focos de criminalidad reflejados en la rentabilidad de recursos digitales para el crimen organizado, la corrupción, la afectación de la seguridad ciudadana, la evolución de las economías ilegales. 2. Fortalecimiento y racionalización de la gestión misional para mejorar el acceso al sistema de justicia colombiano y la acción penal en el territorio colombiano. 3. Fortalecimiento de la gestión institucional, mediante la optimización de los procesos de la entidad, así como del uso de los recursos financieros de la entidad y de la infraestructura tecnológica. Con la implementación de la resolución 1165, (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018). En cuanto a los principios establecidos en el marco de referencia se identifica los siguientes: Excelencia al servicio. Optimización de relación costo / beneficios. Racionalización de recursos. Estandarización de lineamientos, políticas y procedimientos de gestión de TI Viabilidad de planes y diseño de soluciones de TI. Implementación de un esquema de gobierno integral. Fortalecimiento de la infraestructura ya existente, Desarrollo de capacidades de crecimiento articulado entre los componentes de la arquitectura. Desarrollo de capacidades de control de seguridad de la información. Mantener la sostenibilidad de la arquitectura empresarial. Cumplimiento del decreto 2693 de 2012 en cuanto a los lineamientos generales de estrategia de gobierno en línea.
Históricos	No se evidencia una relación directa, salvo los procesos de investigación y acusación frente a los juzgados en los diferentes contextos de las actividades delictivas efectuadas en el estado colombiano y en particular en materia de delitos informáticos. Para esto la Fiscalía General de la Nación cuenta con bases de datos que soportan los procesos de investigación.

Militares	Se identifica como actor en los procesos de investigación y judicialización, pero no se identifica lineamientos formales para ofrecer servicios de intercambio de información para uso del ministerio de defensa como coordinación de las acciones de respuesta frente a los ciberataques en entono digital colombiano. Sin embargo, con un enfoque de capacidad de ciberdefensa, se evidencia en el marco de la estrategia de protección y defensa de las infraestructuras criticas cibernéticas una cooperación en intercambio de información, es decir las necesidades de interoperabilidad de acuerdo con los diferentes organismos institucionales bajo la tutela de la presidencia de la república en materia de seguridad digital del estado colombiano en el siguiente sentido:

Servicios	Actores	Información en el ciberespacio
Investigación y Judicialización	Rama Judicial. Fiscalía General de la Nación. Medicina Legal. Instituto Colombiano de Bienestar Familiar. Contraloría General de la Nación. Procuraduría General de la Nación. Policía Nacional de Colombia.	Noticias criminales. Ordenes de investigación. Reportes técnicos. Debido proceso.
Investigación de delitos informáticos.	El Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia. Dirección Nacional de Inteligencia.	Noticias criminales. Ordenes de investigación. Reportes técnicos.
Protección de intereses nacionales en el ciberespacio.	El Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia. La delegada de protección de datos en la Superintendencia de Industria y Comercio. El Comité de ciberdefensa de las Fuerzas	Servicios críticos del estado colombiano en el ciberespacio.

		Militares Las Unidades cibernéticas del Ejército Nacional. La Armada Nacional y la Fuerza Aérea Colombiana. La Comisión Nacional Digital y de Información Estatal. Registraduría Nacional de Estado Civil	
	Coordinación de servicios de ciberseguridad y ciberdefensa.	El Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional El Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL)	Servicios críticos del estado colombiano en el ciberespacio.
	Cultura de seguridad digital en el estado colombiano.	La Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones.	
Enfoque nacional de gestión de riesgos	La Fiscalía General de la Nación enmarcada en el cumplimiento su responsabilidad de la policita de seguridad digital del estado colombiano y los lineamientos dados por el ministerio de TIC en materia de arquitectura empresarial permite el desarrollo de capacidades con la política de ciberseguridad y ciberdefensa para proteger los servicios de información en el ciberespacio contribuyendo al enfoque de gestión del riesgo nacional para contar con un ciberespacio cada vez más confiable y con capacidades de ciberdefensa.		

Fuente: Análisis de los elementos de contexto para la formulación de lineamientos estratégico basado en PEST (Propuesto por el autor)

4.2. Análisis DOFA.

De acuerdo con el análisis efectuado en los numerales anteriores, se establece que dentro del proceso de construcción de aplicaciones la conciencia y uso de los controles sugeridos por OWASP, (Novillo Vicuña J. P., 2019), se ubica en un contexto de desarrollo con recursos propios y en un proceso de gestión tecnológica establecido en el sistema integral de la entidad, al cual se realizó un análisis de riesgos descrito en el anexo No 1, el cual fue la base de la formulación del siguiente análisis de las debilidades, oportunidades, fortalezas y amenazas en la que se identifica:

Tabla 7
Análisis DOFA en el desarrollo de aplicaciones Web

Aspecto	Relación	Descripción	Descripción (aporte del autor)
Fortaleza	F1	Desarrollos hechos con recursos propios	La Entidad cuenta con un equipo de desarrollo para atender las necesidades de construcción e implementación de aplicaciones web.
Fortaleza	F2	Procesos definidos.	La Entidad cuenta con proceso definidos en un sistema de gestión integral que permite definir los responsables de cada uno de ellos.
Fortaleza	F3	Implementación de la arquitectura empresarial de la Entidad.	La entidad tiene formulada una arquitectura empresarial que atiende los lineamientos establecidos por el ministerio de las TIC.
Fortaleza	F4	Implementación del SOC	La entidad cuenta con un centro de operación de seguridad que le permite monitorear la infraestructura tecnológica de la entidad.
Oportunidad	O1	Cumplimiento de los lineamientos de MinTIC.	Con el mejoramiento continuo en los procesos se pueden incluir los lineamientos en materia de gestión tecnológica en el estado.
Oportunidad	O2	Interoperabilidad con CSIRT.	Con la operación del SOC de la entidad se debe fortalecer la interacción con las organizaciones
Oportunidad	O3	Implementación de normatividad en ciberseguridad.	Teniendo en cuenta que la Entidad cuenta con política de seguridad de la información se debe alinear a las recomendaciones en materia de seguridad digital dada por el ministerio de las TIC e incluir los lineamientos estratégicos de ciberseguridad y ciberdefensa.
Amenaza	A1	Cambios en la normatividad con impacto en las aplicaciones web.	Con la evolución del marco jurídico en materia penal requiere de constantes ajustes de la funcionalidad de las aplicaciones web que afecta la terminación de desarrollos de aplicaciones web que se encuentran en curso.
Amenaza	A2	Pérdida de recursos en proyectos de aplicaciones web en el ciberespacio.	Ante una deficiente definición de requisitos de desarrollo o ante los cambios de los requisitos de desarrollo o falta de continuidad de los proyectos de desarrollo de aplicaciones web se pierden los recursos asignados al proyecto de construcción o ajuste de una aplicación web.
Amenaza	A3	Incremento en el gasto operacional.	Con los ajustes en los procedimientos, guías, instructivos y formatos producto de la mejora continua, hace que se incremente el nivel de requerimientos de ajustes en las aplicaciones con el entrenamiento en el uso por parte del usuario final.
Amenaza	A4	Poca flexibilidad ante	Con el establecimiento de marcos legales que

		el entorno cibernético.	tienen aplicación en el ciberespacio exige que las aplicaciones web requieran de ajustes en su arquitectura para cumplir con los requisitos de negocio del caso.
Amenaza	A5	Flujos de información sin integración y control.	Ante la necesidad de intercambio de información con terceros se establecen flujos de información desde las aplicaciones de manera desarticulada
Amenaza	A6	Existencias de aplicaciones web por cada proceso de la Entidad	Se construye aplicaciones web por cada una de las áreas sin tener en cuenta la funcionalidad de las aplicaciones que se encuentran en producción.
Amenaza	A7	Pérdida de integridad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	Modificación de la información publicada en el ciberespacio debido a la falta de controles de seguridad en el ciclo de vida de las aplicaciones web.
Amenaza	A8	Pérdida de confidencialidad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	Se permite el acceso a información pública reservada publicada en el ciberesapacio concerniente a un caso en particular.
Amenaza	A9	Pérdida de disponibilidad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	Se permite el acceso a información pública reservada publicada en el ciberesapacio concerniente a un caso en particular.
Debilidad	D1	Falta de conocimiento en el funcionamiento de tecnologías utilizadas en el diseño y desarrollo seguro de aplicaciones web.	Falta de validación de seguridad de los componentes de software para el desarrollo de aplicaciones web limitándose al cumplimiento de la funcionalidad.
Debilidad	D2	Falta de la definición de un proceso de publicación de servicios en el ciberespacio.	Se desarrollan servicios tecnológicos para atender requerimientos de intercambio o publicación de información de acuerdo con los requerimientos de desarrollo formulados.
Debilidad	D3	Soporte limitado a los aspectos tecnológicos asociados a los servicios de información en el ciberespacio soportados por plataformas obsoletas.	Puesta en funcionamiento de servicios de información en el ciberespacio con el rezago tecnológico de plataformas obsoletas.
Debilidad	D4	Falta de identificación o de conocimiento de las vulnerabilidades de las plataformas que soportan las aplicaciones web en el Ciberespacio.	Por la falta de identificación de vulnerabilidades de las plataformas que soportan el ciclo de vida de las aplicaciones web se publica información en el ciberespacio soportada por plataformas tecnológicas con vulnerabilidades.

Fuente: Identificación de Debilidades, Oportunidades, Fortalezas, Amenazas basado en DOFA (propuesto por el autor)

De lo anterior, en este trabajo se analizan las amenazas identificadas enmarca en el proceso de gestión integral de TI en la entidad de acuerdo con lo establecido por Min TIC, (TIC M. d., 2016) con el siguiente detalle:

Tabla 8

Identificación de vulnerabilidades en los desarrollos de aplicaciones Web

Relación	Amenaza identificada	Vulnerabilidades identificadas (aporte del autor)
A1	Cambios en la normatividad con impacto en las aplicaciones web.	AD-02: Cambiar las prioridades establecidas por la alta dirección para el desarrollo de aplicaciones web de la entidad que soportan los servicios de información. AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición. PR-01: Retrasar la ejecución del cronograma del proyecto de desarrollo de aplicaciones web por falta de planeación y control.
A2	Pérdida de recursos en proyectos de aplicaciones web en el ciberespacio.	AD-03: Perder los recursos para la implementación de proyectos de fortalecimiento de las aplicaciones web que soportan los servicios de información en el ciberespacio. AD-04: Perder de gobernabilidad de las aplicaciones web por rotación o cambio de personal. AL-02: Cambiar de manera no programada en el alcance del proyecto de publicación de servicios en el ciberepacio y el control de cambios en las aplicaciones web. AL-03: Publicar servicios de información con altos costos soportados por los sistemas legados u obsoletos. AL-04: Cambiar el alcance de los requerimientos del sistema de información debido a que el equipo de trabajo define su propio alcance. AL-06: No realizar las actividades programadas en cumplimiento de los planes de desarrollo de las aplicaciones web. ES-05: Perder la vigencia de gestión de riesgos de la publicación de servicios de información en el ciberespacio. ES-06: Fortalecer el sistema de calidad implantado. PR-02: Priorizar de manera no planeada o equivocada de la atención de requerimientos de desarrollo de aplicaciones web. TE-02: Perdida de aplicabilidad del modelo de seguridad en el ciclo de vida de las aplicaciones web de la Entidad
A3	Incremento en el gasto operacional.	AD-05: Cambiar los requerimientos funcionales en la construcción de las aplicaciones web debido a la reestructuración de las áreas misionales o cambios en los procesos de la entidad. AD-08: Actualizar e Implementar una arquitectura de gobierno flexible como producto de la arquitectura empresarial. AL-05: Formular y estimar requerimientos técnicos o funcionales equivocados. ES-02: Duplicar la funcionalidad de las aplicaciones web en los desarrollos. ES-03: Perder la integración de procesos o procedimientos de la Entidad PR-03: Interrumpir o desviar las actividades del proyecto de desarrollo de aplicaciones web. PR-04: Generar reprocesos y sobrecostos en la ejecución del proyecto de desarrollo de aplicaciones web. A9: Usar componentes con vulnerabilidades conocidas. A10: Realizar registro y monitoreo insuficientes en el sistema de información. TE-04: Implementar aplicaciones web con controles innecesarios. TE-13 – Usar de Componentes con Vulnerabilidades Conocidas

		TE-16: Reutilizar componentes de software estándar y seguros
A4	Poca flexibilidad ante el entorno cibernético.	AD - 07: Perder la documentación técnica actualizada en los desarrollos internos efectuados en la Subdirección de TIC. AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición. AL-07: Definir de manera no adecuada los requerimientos de integración entre las aplicaciones web de la entidad. AL-09: Automatizar y fortalecer procesos de la entidad con el apoyo de la implementación de aplicaciones web misional. ES-01: Perder la integración de los componentes de la estrategia con la arquitectura empresarial y el direccionamiento estratégico de la Entidad. TE-01: Perder la escalabilidad de los componentes de desarrollo de aplicaciones web. TE-04: Implementar aplicaciones web con controles innecesarios.
A5	Flujos de información sin integración y control.	AD - 07: Perder la documentación técnica actualizada en los desarrollos internos efectuados en la Subdirección de TIC. AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición. A1: 2017: Perder integridad de los servicios de información en el ciberespacio. A4: explotar vulnerabilidades de procesadores XML por parte de entidades externas XML (XXE). A5: Perder el Control de Acceso como producto de los ataques de explotación de la falta de controles. A6: Configurar controles de Seguridad de manera incorrecta. A7: Explotar comandos del navegador por medio de Cross – Site Scripting (XSS), A8: Permitir la deserialización Insegura afectando el comportamiento funcional del sistema de información. TE-03: Implementar componentes de las aplicaciones web con vulnerabilidades de seguridad TE-05 – Permitir Inyección de código en las aplicaciones web que soportan los servicios de información en el ciberespacio TE-06 – Perder la autenticación y gestión de Sesiones TE-07 – Permitir la Secuencia de comandos en sitios cruzados (XSS) TE-08 – Permitir la Referencia Directa Insegura a Objetos de in sistema de información. TE-09 – Permitir la Configuración de Seguridad Incorrecta TE-10 – Perder de información por exposición de Datos Sensibles TE-11 – Implementar aplicaciones web con ausencia de Control de Acceso a las Funciones TE-12 – Permitir la Falsificación de peticiones en sitios Cruzados (CSRF) TE-14– Permitir las redirecciones y reenvíos no validados
A6	Existencias de aplicaciones web por cada proceso de la Entidad	AD-01: Perder credibilidad en las aplicaciones web de la Entidad. AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de

		aplicación en los proyectos de desarrollo de aplicaciones web
A7	Pérdida de integridad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web. AL-08: Implementar requerimientos de seguridad no autorizados en la adquisición, desarrollo, implementación y uso de las aplicaciones web. ES-04: Generar políticas de seguridad de la información no alineadas para la publicación e intercambio de información.
A8	Pérdida de confidencialidad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web AL-08: Implementar requerimientos de seguridad no autorizados en la adquisición, desarrollo, implementación y uso de las aplicaciones web. ES-04: Generar políticas de seguridad de la información no alineadas para la publicación e intercambio de información. A2: Perder confidencialidad en la autenticación de las aplicaciones web. A3: exponer datos sensibles.
A9	Pérdida de disponibilidad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web. AD-01: Perder credibilidad en las aplicaciones web de la Entidad. PR-05: Perder disponibilidad de los componentes de las aplicaciones web PR-06: Contar con recursos propios para el desarrollo de aplicaciones web críticos para la entidad. A0: Perder funcionamiento de las aplicaciones web. A0. Operar con una arquitectura de aplicaciones web desactualizada. TE-15: Implementar aplicaciones web con componentes que no tiene estabilidad

Fuente: Identificación de Amenazas en el desarrollo de aplicaciones web, (aporte del autor)

4.3. Riesgos de seguridad de la información de la Fiscalía General de la Nación en el Ciberespacio.

Con la identificación de las amenazas realizadas en el numeral anterior, se identifican los riesgos asociados a los servicios disponibles en el ciberespacio y el proceso de construcción de las aplicaciones web y se identifican de la siguiente manera, ver detalle en el Anexo No 1.

Tabla 9
Relación de Debilidades, Oportunidades, Fortalezas y Amenazas

Relación	Amenaza identificada	Formulación del riesgo (aporte del autor)
A1	Cambios en la normatividad con impacto en las aplicaciones web.	AD-02: Cambiar las prioridades establecidas por la alta dirección para el desarrollo de aplicaciones web de la entidad que soportan los servicios de información. AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición. PR-01: Retrasar la ejecución del cronograma del proyecto de desarrollo de aplicaciones web por falta de planeación y control.
A2	Pérdida de recursos en	AD-03: Perder los recursos para la implementación de proyectos de fortalecimiento de las aplicaciones web que soportan los servicios de

	proyectos de aplicaciones web en el ciberespacio.	información en el ciberespacio. AD-04: Perder de gobernabilidad de las aplicaciones web por rotación o cambio de personal. AL-02: Cambiar de manera no programada en el alcance del proyecto de publicación de servicios en el ciberepacio y el control de cambios en las aplicaciones web. AL-03: Publicar servicios de información con altos costos soportados por los sistemas legados u obsoletos. AL-04: Cambiar el alcance de los requerimientos del sistema de información debido a que el equipo de trabajo define su propio alcance. AL-06: No realizar las actividades programadas en cumplimiento de los planes de desarrollo de las aplicaciones web. ES-05: Perder la vigencia de gestión de riesgos de la publicación de servicios de información en el ciberespacio. ES-06: Fortalecer el sistema de calidad implantado. PR-02: Priorizar de manera no planeada o equivocada de la atención de requerimientos de desarrollo de aplicaciones web. TE-02: Perdida de aplicabilidad del modelo de seguridad en el ciclo de vida de las aplicaciones web de la Entidad
A3	Incremento en el gasto operacional.	AD-05: Cambiar los requerimientos funcionales en la construcción de las aplicaciones web debido a la reestructuración de las áreas misionales o cambios en los procesos de la entidad. AD-08: Actualizar e Implementar una arquitectura de gobierno flexible como producto de la arquitectura empresarial. AL-05: Formular y estimar requerimientos técnicos o funcionales equivocados. ES-02: Duplicar la funcionalidad de las aplicaciones web en los desarrollos. ES-03: Perder la integración de procesos o procedimientos de la Entidad PR-03: Interrumpir o desviar las actividades del proyecto de desarrollo de aplicaciones web. PR-04: Generar reprocesos y sobrecostos en la ejecución del proyecto de desarrollo de aplicaciones web. A9: Usar componentes con vulnerabilidades conocidas. A10: Realizar registro y monitoreo insuficientes en el sistema de información. TE-04: Implementar aplicaciones web con controles innecesarios. TE-13 – Usar de Componentes con Vulnerabilidades Conocidas TE-16: Reutilizar componentes de software estándar y seguros
A4	Poca flexibilidad ante el entorno cibernético.	AD - 07: Perder la documentación técnica actualizada en los desarrollos internos efectuados en la Subdirección de TIC. AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición. AL-07: Definir de manera no adecuada los requerimientos de integración entre las aplicaciones web de la entidad. AL-09: Automatizar y fortalecer procesos de la entidad con el apoyo de la implementación de aplicaciones web misional. ES-01: Perder la integración de los componentes de la estrategia con la arquitectura empresarial y el direccionamiento estratégico de la Entidad. TE-01: Perder la escalabilidad de los componentes de desarrollo de aplicaciones web. TE-04: Implementar aplicaciones web con controles innecesarios.
A5	Flujos de información sin integración y control.	AD - 07: Perder la documentación técnica actualizada en los desarrollos internos efectuados en la Subdirección de TIC. AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición. A1: 2017: Perder integridad de los servicios de información en el ciberespacio. A4: explotar vulnerabilidades de procesadores XML por parte de

		entidades externas XML (XXE). A5: Perder el Control de Acceso como producto de los ataques de explotación de la falta de controles. A6: Configurar controles de Seguridad de manera incorrecta. A7: Explotar comandos del navegador por medio de Cross – Site Scripting (XSS), A8: Permitir la deserialización Insegura afectando el comportamiento funcional del sistema de información. TE-03: Implementar componentes de las aplicaciones web con vulnerabilidades de seguridad TE-05 – Permitir Inyección de código en las aplicaciones web que soportan los servicios de información en el ciberespacio TE-06 – Perder la autenticación y gestión de Sesiones TE-07 – Permitir la Secuencia de comandos en sitios cruzados (XSS) TE-08 – Permitir la Referencia Directa Insegura a Objetos de in sistema de información. TE-09 – Permitir la Configuración de Seguridad Incorrecta TE-10 – Perder de información por exposición de Datos Sensibles TE-11 – Implementar aplicaciones web con ausencia de Control de Acceso a las Funciones TE-12 – Permitir la Falsificación de peticiones en sitios Cruzados (CSRF) TE-14– Permitir las redirecciones y reenvíos no validados
A6	Existencias de aplicaciones web por cada proceso de la Entidad	AD-01: Perder credibilidad en las aplicaciones web de la Entidad. AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web
A7	Pérdida de integridad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web. AL-08: Implementar requerimientos de seguridad no autorizados en la adquisición, desarrollo, implementación y uso de las aplicaciones web. ES-04: Generar políticas de seguridad de la información no alineadas para la publicación e intercambio de información.
A8	Pérdida de confidencialidad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web AL-08: Implementar requerimientos de seguridad no autorizados en la adquisición, desarrollo, implementación y uso de las aplicaciones web. ES-04: Generar políticas de seguridad de la información no alineadas para la publicación e intercambio de información. A2: Perder confidencialidad en la autenticación de las aplicaciones web. A3: exponer datos sensibles.
A9	Pérdida de disponibilidad de la información publicada en el ciberespacio por fallas en las aplicaciones web desarrolladas.	AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web. AD-01: Perder credibilidad en las aplicaciones web de la Entidad. PR-05: Perder disponibilidad de los componentes de las aplicaciones web PR-06: Contar con recursos propios para el desarrollo de aplicaciones web críticos para la entidad. A0: Perder funcionamiento de las aplicaciones web. A0. Operar con una arquitectura de aplicaciones web desactualizada. TE-15: Implementar aplicaciones web con componentes que no tiene estabilidad

Fuente: Resumen de la identificación de riesgos del proceso de construcción de aplicaciones web basado en DOFA. Para ver el mayor detalle de la formulación de los riesgos se puede consultar el Anexo No 2.

Los riesgos identificados no se detallan en la matriz de la gestión de riesgos de la entidad debido a que tienen una visión de alto nivel y para la gestión en el proceso de construcción de aplicaciones web orientadas a soportar los servicios de información de la FGN en el ciberespacio requieren de un mayor detalle, la cual se tiene como resultado del análisis del proceso de gestión de TIC de la Entidad y se resalta los riesgos que tienen un impacto positivo de la siguiente manera:

- Administrativo
- Operativo
- Alcance
- Estratégicos
- Cumplimiento
- Técnico

1.3. Criterios identificados en el desarrollo de aplicaciones web.

1.3.1. Formulación (Producción). En este sentido no se cuenta con una estrategia de ciberseguridad y ciberdefensa, sin embargo, se cuanta con una política de seguridad de la información y una policita de tratamiento de datos personales. (Nación F. G., Políticas de seguridad de la información del sitio web y protección de datos personales, 2018).

1.3.2. Implementación. En la entidad se realiza seguimiento a la ejecución de las políticas referidas en el punto anterior.

1.3.3. Mantenimiento (Seguimiento y evaluación). En la entidad se evalúa periódicamente la actualización de las políticas establecidas.

De acuerdo con la definición de arquitectura critica dada por la ley española 8 de 2011 (consolidada, 2011), en la que se refiere a las instalaciones, redes, aplicaciones web y equipos de TI que soportan los servicios esenciales del estado sin que cuenten con soluciones alternas, se

analiza la infraestructura propia y contratada de la Fiscalía General de la Nación como la necesaria para mantener su operación y prestar el servicio a la comunidad como es el caso de los sistemas de almacenamiento donde se mantiene la información de los diferentes procesos que se adelanta, y que por cultura, en algunos casos se mantiene un registro físico, pero que con las políticas de cero papel y fortalecimiento tecnológico determinado por la infraestructura empresarial de la entidad tiende a migrar a medios digitales. Esto requiere de medidas para fortalecer su resiliencia para ofrecer información disponible, confiable e íntegra que pone a disposición la entidad en el ciberespacio, entre la cuales se encuentra:

Tabla 10
Componentes de aplicaciones Web

Componentes de las aplicaciones web	Descripción (aporte del autor).
Aplicaciones	Desarrollos propios o adquiridos de la entidad para atender los servicios de información que requieren los procesos.
Servidores de archivos	Repositorios de información para la gestión o análisis de datos.
Servidores de aplicaciones y bus de datos	Componentes de software que permiten compilar y exponer servicios de información.
Motores de bases de datos	Software que permite administrar el modelo de datos del sistema de información.
Sistemas operativos	Sistemas operativos que permite administrar los recursos de hardware.
Plataforma de hardware (servidores y balanceadores)	Componentes de hardware del sistema de información.
Plataforma de seguridad perimetral	Componentes de filtrado y monitoreo del sistema de información.
Plataforma de comunicaciones - WAN – LAN.	Incluye canales dedicados, conexión a internet y redes LAN de servidores
Data Center	Espacio físico que permite mantener en funcionamiento los componentes físicos del sistema de información.
Recurso Humano	Desarrolladores, administradores de las plataformas y administradores de las aplicaciones web.

Fuente: Componentes de aplicaciones Web basado en ISO 42010, (42010, 2018).

En este aspecto, la Fiscalía tiene una doble responsabilidad, una misional en cuanto a los delitos informáticos y la otra en la protección de su infraestructura critica en materia de Aplicaciones web es decir las aplicaciones web que son necesarios para el funcionamiento de la entidad y que soportan los servicios de información en el ciberespacio que están alineados a poyar el logro de los objetivos estratégicos y operativos de la entidad. Todas estas, frente a amenazas procedentes de nuevas modalidades de ciberterrorismo o de ciberdelincuencia que ponen en riesgo el entorno digital del Estado y de la ciudadanía.

En este punto, es necesario establecer a partir de las aplicaciones web del estado los mecanismos de control y gestión para la salvaguarda de los derechos constitucionales, valores nacionales, vulnerabilidades y el uso o aplicación de los avances tecnológicos como pilar de

desarrollo económico y social, que en este momento está en cabeza del ministerio de Defensa, de Justica y del Derecho, de Tecnologías de la Información y de las Comunicaciones.

Es así que es necesario analizar para las aplicaciones web las dimensiones nacionales establecidas en el conpes3854, (República de Colombia, 2016), de la siguiente manera:

a. Gobernabilidad y coordinación efectiva.
b. Preparación y prevención.
c. Conocimiento de la situación actual.
d. Resiliencia, recuperación y respuesta.
e. Una visión estratégica global para la ciberseguridad.
f. Enfoque nacional de gestión de riesgos.
g. Marco institucional claro.
h. Proceso sistemático.
i. Estrategia de protección y defensa de las infraestructuras criticas cibernéticas.
j. Efectiva cooperación en intercambio de información, es decir las necesidades de interoperabilidad con:
    i. El Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional
    ii. El Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia
    iii. El Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia
    iv. El Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL)
    v. La Delegatura de protección de datos en la Superintendencia de Industria y Comercio
    vi. La Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones.
    vii. El Comité de ciberdefensa de las Fuerzas Militares
    viii. Las Unidades cibernéticas del Ejército Nacional

ix. La Armada Nacional y la Fuerza Aérea Colombiana.

x. La Comisión Nacional Digital y de Información Estatal.

Lo anterior se debe aplicar al ciclo de vida del software de la Fiscalía General de la Nación en la que se identifica componentes de acuerdo con lo planteado por Roger S. Pressman, (Pressman R. S., 2010), de la siguiente manera:

Tabla 11
Criterios aplicados en el ciclo de vida

Criterios aplicados en el ciclo de vida	Descripción (aporte del autor)
principios de excelencia	se cuenta con el direccionamiento de la Fiscalía General de la Nación, (TIC, 2016), donde se establece la misión, visión y valores institucionales de la Entidad, en la que se enmarca los proyectos de ejecución para satisfacer las necesidades descritas en la ley No 489 de 1998, de la Ley 1437 de 2011 y el artículo 209 de la constitución política de Colombia, que se traducen en necesidades de excelencia al servicio ciudadano, una adecuada relación de costo/beneficio, estandarización, racionalización, interoperabilidad, viabilidad del mercado, federación, co-creación, escalabilidad, seguridad de la información, sostenibilidad, neutralidad y calidad tecnológica.
Estructura empresarial	De acuerdo con el ministerio de las TIC, (TIC, 2016), que incluye los dominios de Aplicaciones web, Servicios tecnológicos, Uso y Apropiación, Estrategia de TI y Gobierno de TI.
Base de conocimiento.	Teniendo como base el lineamiento de MinTIC, en materia de Arquitectura Empresarial, la Entidad cuenta con una arquitectura institucional que incluye herramientas de TIC, los cuales se deben contextualizar desde el punto de vista de ciberseguridad y ciberdefensa que contemple la normatividad, lineamientos, estándares, modelos de gestión, mejores prácticas, soluciones, modelo de organización, casos de éxito y guías (TIC, 2016).
proveer un portafolio de instrumentos y herramientas de ciberseguridad y ciberdefensa	En este sentido se debe, que debe incluir de acuerdo con lo establecido en el marco de referencia de Min TIC los siguientes aspectos, (TIC, 2016): Estándares, lineamientos, guías, modelo de gestión de TI, soluciones, indicadores del ámbito, normatividad del entorno regulatorio y casos de éxito. Modelo de organizacional y lineamientos generales para establecer directrices a implementar en las entidades del estado colombiano. Mejores prácticas internacionales aplicables al entorno público colombiano. Modelo de gestión de tecnologías de la información, y estándares como instrumento. Modelo de gestión de Tecnologías de la Información, para el mejoramiento de la gestión organizacional.
Comunicación.	En el proceso de inicialización del proyecto y en la formulación de los requerimientos se identifica como factores a tener en cuenta el lineamiento legal para la publicación de información en internet por parte de la Entidad desde las aplicaciones web, es el cumplimiento de la ley de transparencia y del acceso a la información pública nacional No 1712 de 2014 adoptada mediante resolución No 039 del 22 de diciembre de 2017, (Nación F. G., Declaración de índice de información clasificada y reservada , 2018) , en donde se establece un índice de información clasificada y reservada, (Nación F. G., Índice de información clasificada y reservada, 2017), que de acuerdo con lo establecido en el capítulo III. Excepciones acceso a la información de la ley en comento, se permite declarar su situación de información pública, publica reservada y publica clasificada por daño de: Derechos a personas naturales o jurídicas. A los intereses públicos Otros direccionadores en la etapa de definición de requerimientos se identifican a la calidad del establecimiento en cuanto a: Definición de requisitos poco descriptivos. Falta de definición de requerimientos técnicos. Falta de definición de requerimientos de seguridad. Diseño de arquitecturas poco claras.

	Cambios el diseño de la arquitectura sin análisis integral del sistema de información.
Planeación.	En cuanto a la estimación, planes de desarrollo y seguimiento uno de los factores a tener en cuenta son las desviaciones en la construcción debido a la modificación de los requerimientos que tienen impacto en la planificación debido a la priorización de requerimientos o el cambio de los lineamientos normativos, lo que implica que las metodologías agiles de desarrollo se ajuste mejor al proceso de desarrollo e implementación de las aplicaciones web en la Entidad.
Modelamiento.	Para el análisis y diseño del sistema de información, la Entidad se han encontrado los siguientes beneficios: Se detecta de manera temprana desviaciones en el diseño propuesto por la priorización o cambios en los requerimientos ocasionados por mejoramiento de los procesos, actualizaciones de plataforma tecnológica, normatividad de seguridad o necesidad de cooperación con otras entidades del estado. Alta interacción entre los desarrolladores y el usuario final. Se cuenta con logros tempranos de desarrollo. Equipos de desarrollo autoorganizados por proyecto. Establecimiento de roles como propietario de producto en el recae la responsabilidad de comunicar los requisitos funcionales, la priorización de atención y probar los desarrollos efectuados. En cuanto al ro de equipo de desarrollo permite organizar las actividades por iteración y las tácticas para entregar los compromisos establecidos. Finalmente, en el rol de líder técnico o maestro scrum, permite la gestión del proyecto y facilitar la comunicación con el propietario. Adaptación al entorno de la Entidad.
Construcción.	En cuanto al proceso de construcción con SCRUM y una vez definida la estructura base, así como las tácticas de reutilización de código, se establecen los patrones arquitectónicos del desarrollo para cumplir con los requerimientos de ciberseguridad para la publicación de información en internet.
Despliegue.	En esta fase del desarrollo de las aplicaciones web, la gestión de cambios cobra especial importancia, especialmente en cuanto a: Aprobación por parte de los interesados. Resultado de pruebas técnicas y de seguridad. Controles de seguridad. En el análisis de la publicación de información en la nube o de la publicación de servicios de información en el ciberespacio, por tratarse la Fiscalía de una entidad pública, son los lineamientos establecidos por el conpes 3854, (Planeación, 2016), en cuanto a: Gestión del riesgo. Esto se enmarca en el sistema de gestión integral de la Entidad en sus componentes de Gestión de la Seguridad de la Información de la Entidad y las necesidades de publicación e intercambio de información con otras entidades del ámbito nacional y en el marco de la ejecución de convenios internacionales. Tratamiento del riesgo, enmarcado en la gestión del riesgo en la entidad, se identifica como infraestructura critica que soporta los servicios que ofrece la entidad en el ciberespacio hacia la comunidad, por lo que en los controles en cuanto a la disponibilidad, confidencialidad e integridad de la información soportada por las aplicaciones web claramente apoyan el logro de los objetivos institucionales que permiten dar seguridad jurídica en la nube que contribuye en la función de estado en ofrecer un entorno adecuado en el ciberespacio para fomentar el desarrollo económico y social del estado colombiano. Respaldo de la alta dirección. Esta se identifica en el plan de desarrollo 2016 – 2020 de la Entidad.

Fuente: Identificación de componentes basado en lo planteado por Roger S. Pressman, (Pressman R. S., 2010)

Teniendo en cuenta que el enfoque de la estrategia de ciberseguridad y ciberdefensa de la Fiscalía se debe ubicar dentro de la seguridad de la información busca un enfoque integral dado por la arquitectura empresarial que incluye los diferentes procesos que permiten proteger la información en el entorno digital la cual no solo abarca las aplicaciones web sino la información

y los servicios publicados por la entidad en el ciberespacio, para lo cual se formula como parte de la del dominio de seguridad de la arquitectura empresarial de la Entidad la cual complementa la dimensión estratégica para gobernar y generar valor tal como lo establece la guía general de un proceso de arquitectura empresarial, (Vive digital colombia, 2016),tal como se describe a continuación:

Tabla 12
Diagnóstico del modelo propuesto por Min TIC

Arquitectura propuesta por MinTIC.	Componente	Descripción de los dominios a aplicar en la Fiscalía General de la Nación (Aporte del autor).
Arquitectura misional o de negocio.	Con la arquitectura de Negocio de la Fiscalía General de la Nación se define los elementos de negocio para implementar la misión, estrategia y procesos de la entidad.	En el dominio de negocio se identifica la cultura organizacional y el entorno de la Entidad para ofrecer los servicios misionales o esenciales reflejados en la formulación de la estrategia, catálogo de servicios misionales, organización y procesos
Arquitectura de Tecnologías de la Información y las comunicaciones	Arquitectura de Información.	En el dominio de la información se identifican la información a proteger en particular a las Fuentes y modelos de información para su registro, procesamiento y almacenamiento.
	Arquitectura de Aplicaciones web.	En el dominio de aplicaciones web se detalla las necesidades de desarrollo y actualización de aplicaciones y controles de para el registro e intercambio de datos.
	Arquitectura de Infraestructura tecnológica.	En el dominio de los servicios tecnológicos necesarios para el desarrollo de aplicaciones y el uso de software base como sistemas operativos, motores de bases de datos, datacenter, redes y componentes de continuidad tecnológica como la infraestructura de copias de seguridad.
	Arquitectura de solución	En el dominio de estrategia de TI y el dominio de gobierno de TI se indica la necesidad de diseño y alcance arquitectónico integral. En el domino de Seguridad de la información. Como protección de datos, gestión de incidentes, seguridad en la red, privacidad, cumplimiento de políticas y estándares. En el dominio de Uso y apropiación se establecen modelos para la gestión de la información frente a los servicios misionales de la Entidad.
	Arquitectura de Software	Especificación para diseño detallado y construcción enfocado en aplicaciones y componentes.

Fuente: Componentes de la arquitectura empresarial en la Fiscalía General de la Nación basado en el modelo propuesto por Min TIC, (Vive digital colombia, 2016).

4.4. Resultado del análisis de la hipótesis de investigación.

Teniendo en cuenta que el instrumento de medición indica que no se cuenta con un nivel de madurez adecuado en el desarrollo de aplicaciones web que soporta los servicios de

información en el ciberespacio, se concluye que es necesario determinar que lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones web y la gestión de riesgos de seguridad de la información de la Fiscalía General de la Nación publicada en el ciberespacio.

2. CAPITULO II – IDENTIFICACIÓN DE LINEAMIENTOS ESTRATEGICOS DE CIBERSEGURIDAD Y CIBERDEFENSA UTILIZADOS PARA EL DESARROLLO DE APLICACIONES WEB Y LA GESTIÓN DE RIESGOS DE LA INFORMACIÓN DE LA FISCALIA GENERAL DE LA NACIÓN PUBLICADA EN EL CIBERESPACIO.

Como parte de la estrategia de entidad se identifican los lineamientos generales establecidos en la entidad para la implementación y sostenimiento de las soluciones de tecnologías de información a partir de la gobernabilidad y control en el desarrollo de las aplicaciones web con los lineamientos formulados en la arquitectura empresarial con los siguientes componentes:

5.1. Relaciones entre los lineamientos estratégicos de desarrollo de aplicaciones web y los riesgos de seguridad de la información de la Fiscalía General de la Nación.

Teniendo en cuenta la gestión de las tecnologías de la información y las comunicaciones que para el caso de la Fiscalía General de la Nación se fundamenta en su arquitectura empresarial en el decreto No 01165 de 2018, (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018), se resalta la gestión de la seguridad de la información de manera transversal, que en su dominio de estrategia requiere de la formulación de los lineamientos estratégicos, que en relación con el dominio de la información, da como resultado la necesidad de gestionar está en el ciberespacio, y el proceso de desarrollo de aplicaciones web. Por tal motivo, se propone una relación entre la gestión de la seguridad de la información, que para el caso de la Fiscalía estableció como norma de referencia la norma **27002 de 2013, (ISO/IEC 27002:2013), en la que se debe enmarcar el dominio No**

10 que corresponde a las adquisiciones, desarrollo y mantenimiento de los Sistemas de Información, y el desarrollo seguro de aplicaciones web con la gestión de los riesgos asociados, la cual se fundamenta en este trabajo en el planteamiento de OWASP.

En particular, el proceso de desarrollo web se relaciona con la organización de seguridad, la implementación de los controles de acceso, la gestión del cifrado y operación para realizar una adecuada gestión de adquisiciones, desarrollo y mantenimiento de las aplicaciones web, e inclusive la interacción con la infraestructura crítica que las soporta, tal como lo relaciona López, (Lopez, 2013).En este sentido, se identifican los siguientes aspectos de relación:

- La necesidad de contar con unos los lineamientos estratégicos que integre las actividades de ciclo de vida del software definidas en la Fiscalía y la gestión de riesgos de ciberseguridad para fortalecer el proceso de **adquisiciones, desarrollo y mantenimiento de los Sistemas de Información**.
- En la fase de identificación de los requisitos del desarrollo de una aplicación web se identifica una relación muy cercana con la definición de requisitos de seguridad de la información y de la aplicación de los mecanismos de protección tanto de la información como de los activos asociados, que para este trabajo se centra en aquella que la entidad requiere publicar en el ciberespacio producto de las actividades de la lucha contra el ciberdelito y cibercriminalidad.
- Una vez publicada, se identifica la relación entre los mecanismos de control para evitar transmisión de información incompleta o de la modificación de información o de enrutamiento errado o de la alteración de mensajes entre los componentes de las aplicaciones web, así como la reproducción o copia de mensajes no autorizados con las vulnerabilidades a tratar en el proceso de disponer activos de información de la entidad en el ciberespacio.
- De igual manera, con puesta en producción de la aplicación web se verifica el funcionamiento de las aplicaciones web para detectar vulnerabilidades en su estabilización y evaluar el resultado de los procesos de cambios programados.
- Las baterías de vulnerabilidades a controlar dependen de la protección de los ambientes de desarrollo, pruebas, preproducción y producción, así como de la documentación de los planes de pruebas formulados en los desarrollos de las aplicaciones web de la entidad.

- Existe una estrecha relación con la definición de los roles y acceso de los actores internos y externos en el proceso de construcción de las aplicaciones web de la entidad, así como el papel que cumplen el ciclo de vida de la aplicación web, las diferentes plataformas tecnológicas y de la ejecución de los planes de remediación.
- En la construcción de aplicaciones web, la operación de la plataforma crítica y en los procesos de continuidad de negocio, un papel que se requiere definir y documentar son las actividades desarrollados por terceros de acuerdo con los procedimientos de la entidad y su efecto en los mecanismos de auditoria del acceso de terceros a las aplicaciones web de la entidad.
- Para el caso de la Fiscalía General de la Nación, los requerimientos de ciberseguridad que se deben atender en la arquitectura de las aplicaciones web de la entidad corresponden a la interacción con los requerimientos funcionales de las aplicaciones web analizados desde el punto de vista de la gestión de los riesgos de la seguridad de la información en internet, como los relacionados con riesgos legales y operativos que afecten el funcionamiento de la Entidad, los cuales, según la norma se pueden controlar mediante:
  - Análisis y especificación de los requisitos de cumplimiento del marco normativo.
  - Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - Protección de las transacciones por redes telemáticas.
- Desde el punto de vista de la efectividad en la automatización y la implementación de los controles de la funcionalidad de las aplicaciones web que soporta los servicios publicados en el ciberespacio, existe estrecha relación con los lineamientos establecidos en el índice de clasificación de información pública declarada por la entidad en su página web (Nación F. G., Declaración de índice de información clasificada y reservada , 2018), y por consiguiente, en la implementación de los requerimientos de seguridad como lo es el seguimiento de la codificación para validar la calidad de las garantías de servicios misionales y verificar la actualización de los componentes utilizados en la construcción del software, que para el caso de la Fiscalía General evitar las desviaciones de los desarrolladores para no destinar esfuerzos para solucionar los requerimientos de

ciberseguridad en cuanto a la arquitectura de la aplicación web, que en primera instancia se aborda con el análisis de las historias de usuario, los requisitos y el diseño de la arquitectura definida, tal como lo que se resalta en los artefactos definidos por (Cervantes, 2016):

Tabla 13
Actividades en el proceso de construcción de aplicaciones Web

Actividades	Artefactos	Descripción del proceso en la FISCALÍA GENERAL DE LA NACIÓN (aporte del autor)
Especificación de historia de usuarios.	Historias de usuario	En el ciclo de vida de la arquitectura del sistema de información se realiza la especificación mediante historias de usuario para establecer los requisitos.
Priorización de historias de usuarios.	Historias de usuario	De acuerdo con la disponibilidad de recursos se formulan los planes de trabajo de acuerdo con las prioridades de entrega de los proyectos de desarrollo de aplicaciones web.
Especificación de tareas.	Backlog del proyecto	Por cada proyecto se establece las tareas a realizar las cuales se controlan por cada equipo de desarrollo asignado.
Estimación de esfuerzos.	Backlog del proyecto	De acuerdo con la complejidad para atender los requisitos se estima los costos en recursos y arquitectura para el diseño o cambios en la arquitectura de la aplicación a intervenir.
Planeación de entregas	Backlog del proyecto	Mediante reunión con los interesados se establecen los compromisos de entrega.
Planeación de Sprint.	Backlog del proyecto	Por cada una de las iteraciones se establece los compromisos a entregar en una semana.
Refinamiento de historias de usuarios-	Backlog del proyecto Backlog del sprint.	Con la validación de los usuarios se realizan las pruebas y se determina los ajustes a realizar en las historias de usuario o se determina los requisitos de desviaciones en la arquitectura propuesta.
Junta diaria del sprint.	Backlog del sprint.	Con el líder o master de SCRUM se realiza el seguimiento diario para resolver los inconvenientes encontrados en el proceso de desarrollo o las decisiones a tomar para atender los requisitos definidos.
Desarrollo del producto.	Backlog del sprint.	En este componente se incluya las actividades de diseño, desarrollo y pruebas unitarias de acuerdo con los requisitos definidos.
Revisión del sprint.	Desviación de la arquitectura. Incremento en el desarrollo.	Se analiza el sprint para realizar los ajustes o modificaciones en la arquitectura para satisfacer los requisitos definidos
Retrospectiva del sprint.	Generación de base de datos de conocimiento.	Esta etapa no se realiza dentro del proceso de desarrollo, pero si se tiene en cuenta la experiencia del desarrollador y los arquitectos para nuevos proyectos.
Refinamiento del backlog.	Historias de usuario.	De acuerdo con los cambios a realizar se actualiza la arquitectura del software teniendo en cuanta los riegos y los impactos de los cambios acordados.

Fuente: Artefactos de entendimiento de requisitos basado en los artefactos definidos por (Cervantes, 2016).

- Se requiere en la entidad, dar cumplimiento con la arquitectura empresarial del estado colombiano (TIC M. d., Diseño y Especificación del Marco de Referencia. Diseño Detallado. Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información (TI), a Adoptar en las Entidades del Sector Público

Colombiano., 2014), con los lineamientos dados por el ministerio de las TIC, que se refleja en la entidad en su arquitectura que cuenta con los siguientes principios:

a. Los establecidos en el artículo 209 de la constitución.
b. Artículo 3 de la ley 489 de 1998.
c. Ley 1437 de 2011.
d. Formulación, implementación y validación de controles de seguridad de la información.
e. Decreto 2693 de 2012.

- Las aplicaciones web tienen estrecha relación con las bondades y limitaciones de la infraestructura critica, tanto así que su diseño interno obedece al lineamiento de:

a. Construcción de un sistema de información misional unificado.
b. Una arquitectura de las aplicaciones web basada en una defensa por capas, en cuanto a:

1. Comunicaciones WAN / LAN. (Corletti Estrada, 2017)
2. Seguridad perimetral: IDS / IPS, Balanceadores de tráfico, AntiSPAM, SANDBOX, Firewall de próxima generación, Firewall de Aplicaciones y Firewall de bases de datos.
3. Servidores: Plataformas de virtualización. Sistemas de almacenamiento.
4. Monitoreo de seguridad. Herramientas de correlación de eventos de seguridad.

- Información, la entidad genera información a todos los niveles organizacionales, pero se resalta la información necesaria para la investigación y el análisis criminal, y su relación con la toma de decisiones gerenciales y estratégicas de la entidad.

- La atención de los requisitos funcionales de las aplicaciones web con el control de la atención de los requisitos de seguridad y las metodologías de desarrollo SCRUM para el diseño de aplicaciones web.

En cuanto a los problemas identificados en la indagación se formula:

- Problemas de alcance: En cuanto al alcance de la ley de transparencia y del derecho de acceso, la entidad declara la clasificación de información pública reservada y publica clasificada que limita los servicios de publicación e intercambio de información, obligando a contar con una serie de procedimientos, guías e instructivos para el manejo de los datos personales.
- Problemas de entendimiento: Al abordar los requerimientos de intercambio de información entre los diferentes aplicaciones web en el estado, especialmente en el rol de policía judicial, se basa en la función que establece la constitución política de Colombia, que para el caso de la Entidad utiliza componentes de la arquitectura de servicios web que en primera medida requiere de la identificación de los datos que maneja cada uno de los sistemas y establecer un acuerdo de homologación y que información se debe auditar en su uso.
- Problemas de volatilidad: Se debe tener en cuenta para la publicación e intercambio de información los cambios en la legislación y los lineamientos establecidos en los acuerdos de intercambio de información con otras entidades del estado colombiano.
- En cuanto a la elaboración de los requerimientos de ciberseguridad y ciberdefensa, se deben tener en cuenta los siguientes aspectos:
- Las aplicaciones web deben intercambiar la totalidad de los datos acordados entre las entidades o actores del proceso judicial.
- En la publicación de información se debe mantener la disponibilidad, integridad y confidencialidad de acuerdo los lineamientos de la arquitectura empresarial.
- En el componente de la negociación, debe estar alineado con el componente de austeridad estratégica establecida en el direccionamiento 2016-2020 de la entidad, con lo que se ofrece servicios de intercambio en lo que le corresponde para publicar este tipo de servicios en la nube, y en este caso son las entidades las que deben contar con lo necesario para acceder a los servicios disponibles.

5.2. Proceso de definición de requisitos.

El inicio del proyecto se plantea con la concepción del mismo donde se establecen los eventos del sistema de información para la publicación de información de acuerdo con la legislación como es el caso de la ley 1581 de tratamiento de datos y la ley 1712 de transparencia y del derecho de acceso a la información pública. En el segundo paso propuesto por Pressman, (Pressman R. S., 2010), es la indagación que para el caso de la publicación de información consiste en los servicios de la información que se deben poner a disposición de la comunidad en la nube.

En este sentido, se da principal relevancia a la identificación de los requisitos funcionales a atender con el desarrollo de la aplicación web, los cuales parten de la buena definición de los procesos de negocio alineados con la norma vigente y su validación del impacto en las aplicaciones para obtener un nivel de seguridad adecuado para los procesos de negocio, sin embargo, no se aborda explícitamente lo relacionado con los requerimientos relacionados con la ciberseguridad y la ciberdefensa. Esto de acuerdo con el planteamiento de Pressman, (Pressman R. S., 2010), con la fase de planeación a partir del insumo producto de la fase anterior con la formulación de un plan de trabajo con la que se establece las tareas, fechas de entrega, asignación de recursos, mecanismos de seguimiento como son las reuniones con los usuarios funcionales para validar los prototipos desarrollados. En cuanto a la definición de requerimientos de las aplicaciones web, el aspecto de seguridad de ciberseguridad debe ser definida para la gestión de la información en el ciberespacio por parte de la entidad, es decir, deben identificarse parte de la definición de los requerimientos de las aplicaciones web y no en el momento de la publicación o el intercambio de información. De acuerdo con Pressman, (Pressman R. S., 2010) se plantea como una administración de los requerimientos para gestionar adecuadamente los requerimientos, esto a partir de la identificación de:

- Información necesarios para los procesos de la arquitectura de la entidad.
- Necesidades de intercambio de información entre procesos, usuarios y entidades del estado colombiano.
- Dueños y actores de los procesos de intercambio y publicación de información.
- Necesidades de integración de la arquitectura de la entidad.
- Escenarios de uso como herramienta de descripción de los requerimientos.

- Formulación de enunciados de necesidades, alcance, usuarios de ciberseguridad y ciberdefensa, así como la oportunidad de información.
- Estructura de ciberseguridad y ciberdefensa de la entidad.
- Una vez abordado los aspectos de la definición de los requerimientos del sistema de información, se aborda la necesidad de incorporar en la arquitectura empresarial de la entidad un modelo de desarrollo seguro para metodologías agiles como lo plantea la iniciativa de computación segura de Microsoft, en cuanto a:
    - Requerimientos de seguridad en el diseño.
    - Requerimientos de seguridad por omisión en la instalación.
    - Requerimientos de seguridad en la implantación del sistema de información.
    - Requerimientos de seguridad en las comunicaciones.
- Una metodología de desarrollo de software seguro de OWAS (Open Web Application Security Project), que plantea seguridad en cuanto a:
    - Disponibilidad.
    - Estabilidad.
    - Características de la plataforma

5.3.En cuanto al diseño de aplicaciones web.

Generalmente, para el desarrollo de aplicaciones web la arquitectura institucional se establece la reutilización de los desarrollos web existentes, es decir, el código ya construido y soportado por las capacidades de gobierno de la gestión de TI en la Entidad.

En la actualidad se desarrolla estas capacidades con los siguientes criterios:

- Ofrecer servicios que representen un valor agregado para los ciudadanos e instituciones.
- Establecer indicadores de medición de incidentes de seguridad de la información publicada en el ciberespacio.
- Proveer de mecanismos efectivos para el intercambio o publicación de información.
- Incorporar las políticas de seguridad, uso de aplicaciones web y tratamiento de datos que aplica la entidad.
- Identificar las necesidades de seguridad para el intercambio y publicación de información.

Lo anterior, en coherencia con lo planteado por Pressman, (Pressman R. S., 2010), donde se da inicio de la construcción con la comunicación del proyecto, la participación del área de tecnología de la entidad y el usuario funcional para establecer la necesidad y el requisito o requerimiento para que los equipos de desarrollo de aplicaciones web realicen la planeación correspondiente. En este sentido, y de acuerdo con la formulación de un modelo de negocio, (Osterwalder, 2010), se logra proyectar a la entidad en cuatro años en los aspectos estratégicos. (Nación F. G., Plan estratégico 2016-2020, 2018). Esto de acuerdo con el planteamiento de Pressman, (Pressman R. S., 2010), para la definición del modelamiento. En esta fase se realiza las actividades de análisis y diseño de la solución requerida, la cual generalmente se realiza por el empleado que efectúe las labores de arquitecto de software., el cual, no realiza el análisis de la seguridad en las aplicaciones web de la entidad y da mayor relevancia a identificar una solución que atienda características de calidad y entre ellas aspectos de seguridad del producto o la plataforma que permiten definir la arquitectura del sistema de información a utilizar.

5.4.En cuanto al desarrollo de las aplicaciones web.

A partir del decreto-ley No 016 de 2014, se establecen dentro de las funciones de la Subdirección de TIC, el liderar, coordinar y articular las diferentes aplicaciones web de la entidad, se formula la necesidad de gobernar el ciclo de vida del software, que para este caso se basa en la ISO 12207-1 y la norma colombiana NTC 4243, en la que se destaca:

- Desarrollar de manera integral las aplicaciones web, esto es bajo el principio de racionalización, satisfacer las necesidades de automatización de los procesos de la entidad a partir de las aplicaciones web disponibles.
- Mantener actualizadas las necesidades a satisfacer con aplicaciones web con la finalidad de ser priorizados.
- Actualizar los manuales de usuario según los cambios de los aplicativos.
- Capacitar a los usuarios funcionales del sistema de información.
- Realizar las pruebas funcionales a los desarrollos.
- Desarrollar en las aplicaciones, los perfiles y roles en la gestión de los usuarios.
- Desarrollar la funcionalidad para que no sea necesario el cambio directo en las bases de datos de las aplicaciones web.

- Validación de pruebas del software por parte del usuario funcional.
- Programar las ventanas de mantenimiento.
- Actualizar los procedimientos en el SGSI que tienen relación con las aplicaciones web.
- Cumplir con las políticas de seguridad de las aplicaciones web.
- Se cumplir los lineamientos del manual de identidad visual.
- Se debe cumplir con los lineamientos de gobierno en línea.
- Se debe desarrollar aplicaciones web con código libre de vulnerabilidades conocidas y codificación segura.

Por lo anterior y el grado de dinamismo del desarrollo obliga a utilizar una metodología de desarrollo de software en el Entidad basada en metodologías de desarrollo agiles, con la que se busca dinamizar la interacción con el usuario y detectar de manera temprana posibles fallos o bugs del sistema de información. Esto de acuerdo con el planteamiento de Pressman, (Pressman R. S., 2010), que se identifica con la construcción. El equipo de desarrollo asignados al proyecto construye el código y el equipo de pruebas efectúen las pruebas del caso. Para este último aspecto, se cuenta con una plataforma de análisis de calidad, para validar la funcionalidad requerida, usabilidad, portabilidad, integración con la arquitectura del sistema de información, disponibilidad, seguridad general de la aplicación, compatibilidad de los componentes, reutilización de componentes y personalización de componentes. No se evidencia análisis directos de costos, tolerancia ante fallas, resiliencia, facilidad de pruebas y de soporte frente a los requisitos de ciberseguridad y ciberdefensa.

Una vez analizados estos aspectos, se cuenta con la definición mediante un documento de formulación del requisito o requerimiento del sistema de información, el contempla aspectos básicos de:

- Autenticación.
- Datos de auditoria.

En cuanto a los requisitos de cifrado de los datos sensibles como contraseñas e información personal, no se le da especial tratamiento, solamente se gestión al ingreso del sistema y no la transmisión de datos entre los componentes de la arquitectura del sistema de

información o con otras aplicaciones web a través de un componente de orquestación de publicación de datos como es el caso de un bus de servicios.

En cuanto a la gestión de los riesgos en el desarrollo web, se identifica una estrategia reactiva dependiendo de las vulnerabilidades que se detecten en los componentes de la arquitectura del sistema los que se limita a la mitigación desde el punto de vista de la plataforma y no del código y de los siguientes aspectos:

- Autenticación y control de acceso de usuarios basados en contraseña.
- Calidad del software.

5.5. Pruebas de los desarrollos de aplicaciones web.

La validación del cumplimiento de los requisitos establecidos por los usuarios funcionales permite que los equipos de desarrollo asignado en el primer ciclo refinen la definición para de esta manera empezar a evolucionar la aplicación en un primer prototipo y realizar la planificación de la iteración y así mismo llevar el control de costos en tiempo y recursos.

Si bien es cierto que con ese modelo favorece la detección temprana de las desviaciones de la arquitectura, no permite el control de la proyección de costos iniciales, por lo que se toman decisiones en la fase planeación para viabilizar o posponer los nuevos requisitos detectados, para que posteriormente se modele la variación, se realice la construcción de acuerdo con la metodología de SCRUM, (Pressman R. S., 2010), adaptada para los desarrollos en los siguientes componentes:

- Priorización de las características del producto a desarrollar.
- Asignación de las características a desarrollar en el ciclo.
- Asignación de los ítems a desarrollar por equipo.
- Evolución y control diario de los desarrollos.
- Liberación del desarrollo.

5.6.En cuanto a la implementación de las aplicaciones web.

De acuerdo con Pressman, (Pressman R. S., 2010), en cuanto al despliegue, la liberación del aplicativo, se inicia con las tareas de soporte para estabilizar el servicio y en la

implementación de las aplicaciones web de la Entidad, se basa en la gestión de requerimientos soportados por la implementación de ITIL versión 3, en la que se establecen:

- De acuerdo con la resolución 01261 de 2014, se deben realizar implementaciones informáticas de manera integral de acuerdo con lo establecido en el decreto-ley 16 de 2014.
- Para la puesta en producción, es necesario contar con un concepto técnico de viabilidad de las diferentes alternativas que ofrece el mercado y de transferencia de conocimiento, sin describir aspectos concretos de seguridad.
- Mantener actualizados el inventario de aplicaciones web.
- Realzar el soporte de primer nivel concerniente a lo funcional y procedimental en la operación de las aplicaciones web.
- Programar las ventanas de despliegue de desarrollo, para lo cual se debe tener los informes de pruebas y documentación de casos a probar, resultado de pruebas, documentación de autorización de paso a producción del usuario líder funcional y documentación de los objetos de modificación, descripción del código fuente, y script de base de datos.
- Apoyar la migración de los datos de las aplicaciones web.
- Administrar los usuarios por medio de aplicaciones web.
- Realizar las acciones para lograr la gobernabilidad de las aplicaciones web.
- Las aplicaciones web a través de la red corporativa de la Entidad.
- Se debe gestionar los derechos de autor de las aplicaciones web construidos, ante la Dirección Nacional de Derechos de Autor.

5.7.En cuanto a la adquisición de las aplicaciones web.

En cuanto a la adquisición de aplicaciones web, aunque no es especifico en la resolución No 01261 de 2014, se puede identificar:

- Brindar el acompañamiento y asesoría en los procesos de mantenimiento de las aplicaciones web de la Entidad.
- Validar la garantía de protección de información de las bases de datos de las aplicaciones web.
- Validación de pruebas del software por parte del usuario funcional.

- Entrega del software ajustado
- Entregar la documentación de las fases, la cual debe incluir visión del proyecto, necesidades a satisfacer, casos de uso crítico, requerimientos funcionales detallados y validados por el usuario funcional, aspectos técnicos, cronograma de actividades del proyecto, arquitectura del sistema, script del modelo fisco y lógico, fuentes, objetos, manual de usuario, guías de ruta, despliegue del sistema, responsabilidad de transferencia de conocimiento, plan de capacitación, plan de manejo y control de cambios.
- Programar las ventanas de mantenimiento.
- Realizar las acciones para lograr la gobernabilidad de las aplicaciones web
- Para el soporte y mantenimiento, las solicitudes deben ser registradas y reportadas por el usuario a la Subdirección de TIC.

5.8. Operación de las aplicaciones web.

Los aspectos de gestión de riesgos en la entidad, establece que, de manera periódica al realizar los análisis de vulnerabilidad de los activos de información, que buscan identificar aspectos a solucionar producto de la acción de mecanismo de monitoreo de riesgos en los desarrollos efectuados o de la puesta en producción de un sistema en el ciberespacio, que basados en la experiencia se van fortaleciendo los conocimientos del equipo desarrollador y los arquitectos de la solución. Por lo que es necesario contar con una estrategia proactiva, es decir formular una estrategia de ciberseguridad y ciberdefensa en todas las fases del ciclo de vida de un sistema de información producto del lineamiento con la política de seguridad digital del estado colombiano, en donde como parte de la formulación se ejecuten las fases de identificación del riesgo con su respectivo análisis, valoración de impacto y la formulación del plan para la gestión de los riesgo del sistema de información que soportara los servicios de la entidad en la nube. A partir de la tipificación de riesgos en la desarrollo de software de pressman, (Pressman R. S., 2010), los riesgos del proyecto, técnicos y de negocio; se identifica la gestión de los riesgos en la arquitectura empresarial de la Entidad, sin embargo, no se ven formulados en la fase de identificación del requisito o requerimiento con una alineación en una de la directrices de la estrategia de la entidad como lo es la austeridad estratégica, (Nación F. G.,

Plan estrategico 2016-2020, 2018), con lo que se hace necesario tenerlo en cuenta en la formulación de la estrategia de ciberseguridad y ciberdefensa para el desarrollo, la implementación y uso de aplicaciones web en la Fiscalía General de la Nación.

- En los riesgos de negocio y en congruencia con la identificación temprana de las desviaciones de la arquitectura del sistema, los incrementos en costos ocasionados por los cambios en el alcance de los requisitos o requerimientos formulados son uno de los principales riesgos que afecta la planificación del proyecto, por lo que es necesario alinearse con lo establecido con la estrategia de la entidad en los aspectos de alcance del software, impacto en factores de calidad como desempeño, facilidad de mantenimiento o soporte, impacto en la gobernabilidad de la solución tecnológica por la inclusión de nuevas tecnologías en cuanto a la experiencia de implementación o la complejidad de la arquitectura del sistema para realizar el mantenimiento o la implementación correspondiente acorde con los cambios en los procesos de la entidad.
- No se identifica la formulación de una estrategia de ciberseguridad y ciberdefensa para las aplicaciones web de la entidad, desde el punto de vista del ciclo de vida del software como una manera de análisis integral del sistema de información.

5.9.En cuanto al uso de Aplicaciones web.

En la política de seguridad de la información de la Entidad, se establece en la responsabilidades y funciones aspectos de clasificación y documentación de la información de acuerdo con el grado de sensibilidad, clasificación, criticidad, permisos de acceso de acuerdo al perfil del usuario.

En cuanto a la identificación y gestión de riesgos de las aplicaciones web no se establece de manera explícita, se realiza de manera global en el sistema de gestión integral de la Entidad desde el punto de vista de la información, con lo que de manera indirecta influye en la arquitectura de las aplicaciones web como implementación de controles sin que se identifique los lineamientos de una estrategia de seguridad o específicamente de ciberseguridad o ciberdefensa.

6. CAPITULO III – PROPUESTA DE IMPLEMENTACIÓN DE LINEAMIENTOS ESTRATEGICOS DE CIBERSEGURIDAD Y CIBERDEFENSA PARA EL DESARROLLO DE APLICACIONES WEB DE LA FISCALIA GENERAL DE LA NACION Y GESTIÓN DE RIESGOS DE LA INFORMACIÓN DE LA FISCALIA GENERAL DE LA NACIÓN PUBLICADA EN EL CIBERESPACIO.

6.1. Lineamientos generales para el desarrollo seguro de aplicaciones web.

A partir del análisis efectuado se formulan los siguientes lineamientos generales:

Tabla 14
Lineamientos generales para el desarrollo de aplicaciones Web

Lineamiento	Descripción
Implementar un modelo de seguridad y privacidad de la información en el proceso de desarrollo de aplicaciones web de la Fiscalía General de la Nación a partir de las recomendaciones dadas en OWASP y la ISO/IEC 27001.	Establecer controles en el proceso de desarrollos de aplicaciones web para la protección de la información y aplicaciones en el marco de la confidencialidad, integridad y disponibilidad, es decir, establecer e implementar una metodología de análisis, evaluación y gestión de riesgos de activos informáticos que corresponde a: Sistema de gestión integral de la Entidad, pero no es especifica en la adquisición de adquisición, desarrollo y uso de aplicaciones web Políticas de desarrollo de aplicaciones Web para fortalecer la disponibilidad de la información publicada en el ciberespacio. Identificar qué información se encuentra a disposición de las aplicaciones, procesos o personas en el ciberespacio y establecer la posición de la entidad para determinar las reglas de negocio a implementar en los desarrollos de las aplicaciones Web. Controles y componentes que favorezcan la continuidad de los servicios de información publicados en el ciberespacio. Enfocar el proceso de construcción en un proceso de constante evolución, tal como se define en la ISO 12207, y en particular en lo relacionado con las aplicaciones, que dependen de su seguridad en un alto grado de la robustez de la arquitectura del sistema de información y de la arquitectura del software, tal como se evidencia en los Top de OWASP. Formular y fortalecer los procedimientos de la entidad para el cumplimiento de leyes y regulación en tiempos adecuados.
Diseñar e implementar controles de seguridad para el proceso de construcción de aplicaciones web que soporten los servicios de información en el ciberespacio.	Definir los criterios y componentes que permitan que las aplicaciones web puedan contar con: Características de resiliencia frente a riesgos de fallos de las aplicaciones web de la entidad. Monitoreo y evaluación de los cambios significativos de riesgos, que para el caso del uso de las aplicaciones web. Gestión de riesgos asociados a las vulnerabilidades las aplicaciones web que representan un alto riesgo en el ciberespacio, en cuanto a: A1 – Inyección A2 – Pérdida de autenticación y gestión de Sesiones A3 – Secuencia de comandos en sitios cruzados (XSS) A4 – Referencia Directa Insegura a Objetos A5 – Configuración de Seguridad Incorrecta A6 – Exposición de Datos Sensibles A7 – Ausencia de Control de Acceso a las Funciones A8 – Falsificación de peticiones en sitios Cruzados (CSRF) A9 – Uso de Componentes con Vulnerabilidades Conocidas A10 – Redirecciones y reenvíos no validados

	Desarrollo e implementación de controles de seguridad acordes con la gestión de servicios tecnológicos y usuarios en el ciberespacio para atender los lineamientos de gobierno digital del estado colombiano.
Identificar los datos como activos de información de la entidad disponibles en el ciberespacio para establecer los controles a implementar.	Identificar los datos a difundir en el ciberespacio y establecer los requerimientos de seguridad que deben cumplir los desarrollos de aplicaciones web y la gestión de los riesgos identificados, tal como lo enfoca Gasca. (Gasca-Hurtado, 2013), en cuanto a trazabilidad de datos y propiedad y seguridad de los datos.
Selección de plataformas y arquitecturas de software unificadas	La gestión de TIC de la Entidad debe coordinar los desarrollos o adquisición de aplicaciones web enmarcados en una arquitectura de seguridad para optimizar los recursos, capacidad de desarrollo y de integración para fortalecer la arquitectura de aplicaciones web basada en características de desarrollo de microservicios de seguridad para ofrecer soportar el desarrollo de todas las aplicaciones web. Adicionalmente se debe diseñar un plan de aseguramiento de las plataformas de desarrollo, pruebas, preproducción y producción mediante análisis de vulnerabilidades y acciones de remediación.
Fortalecimiento del proceso de selección de Talento Humano y proveedores especializado en desarrollo de software y seguridad	Con la implementación de la arquitectura institucional se requiere: Especializar el grupo seguridad de la información de la entidad para apoyar la construcción de las aplicaciones web. Seleccionar los proveedores de componentes de las aplicaciones web. Contar con un plan de entrenamientos con niveles básicos, intermedios y avanzados dependiendo de los roles en las diferentes fases de ciclo de vida del software en la Entidad.
Generación de conocimiento especializado para el desarrollo de aplicaciones web	En este sentido, a partir de los análisis de vulnerabilidades, pruebas y monitoreo de incidentes de seguridad de las aplicaciones web que soporten los servicios de información en el ciberespacio se debe generar una base de conocimiento especializado e implementar herramientas de análisis de datos para mantener un alto nivel de respuesta ante las amenazas y la mitigación de vulnerabilidades de las aplicaciones web. Pruebas integrales de las aplicaciones web a modificar o construir Para la revisión del código fuente y de los controles de desarrollo debe ser basado en las mejores prácticas como OWASP que permita una gestión de los riesgos de la construcción y uso de las tecnologías para maximizar las oportunidades y minimizar las amenazas, sin perjuicio de facilitar el desarrollo de los servicios formulados y brindados por la entidad en el ciberespacio. Para ampliar la cobertura en las pruebas, no solo las áreas funcionales deben realizar las pruebas para la aprobación de la puesta en funcionamiento de un servicio en el ciberespacio, sino que se debe contemplar planes de cooperación interdepartamental al interior de la entidad en la ejecución de análisis de vulnerabilidades, con la capacidad de control y acción del SOC de la Entidad para verificar el cumplimiento del direccionamiento estratégico de la entidad y la política nacional de seguridad digital.
Arquitectura de software integrada con una Arquitectura de Seguridad.	Para la atención de los requerimientos funcionales en el ciberespacio se debe enmarcar dentro de la arquitectura de seguridad de la entidad para permitir la integración con la arquitectura permite ofrecer a la comunidad el conocimiento de servicios de información.

Fuente: Aporte del autor.

Con la formulación de estos lineamientos, de igual manera se propone las siguientes actividades para su desarrollo en la Entidad:

- Con la participación del Grupo de Seguridad de la Información de la Subdirección de TIC y la Dirección de Planeación de la Entidad, se debe implementar en el sistema de gestión de la seguridad de la Entidad las

directrices definidas en el modelo de seguridad y privacidad de la información en el proceso de desarrollo de aplicaciones web de la Fiscalía General de la Nación a partir de las recomendaciones dadas en OWASP y la ISO/IEC 27001. En este sentido, para establecer un modelo de seguridad y privacidad en la Entidad se propone desarrollar las siguientes actividades:

- Incorporar los controles de gestión de riesgos enmarcados en OWASP y ISO/IEC 27001 relacionados en el Anexo 1 dentro del Sistema de Gestión Integral de la Entidad. Esto es la formulación de un componente de manual de seguridad de la información, el cual debe ser elaborado en coordinación con la Dirección de Planeación Estratégica de la FGN y la Subdirección de TIC con el fin de establecer el modelo de seguridad y privacidad de información a partir de los lineamientos formulados en este estudio.
- Con la formulación de los controles relacionados con el dominio de construcción, adquisición y mantenimiento de sistemas de información de la Política de seguridad de la información, se debe realizar la revisión y fortalecimiento de este dominio con la aplicación de las políticas específicas para el desarrollo seguro de aplicaciones Web de acuerdo con el análisis de riesgos y del DOFA propuesto en este estudio. Esta labor se debe validar por parte de la Dirección de Planeación de la Entidad como parte de proceso de fortalecimiento del modelo de gestión de riesgos implementado en la FGN.
- Al interior de la Subdirección de TIC, con el apoyo del grupo de seguridad de la información, se debe actualizar los procedimientos de gestión de TIC con la formulación y aplicación de la política de desarrollo seguro de aplicaciones Web. Esto enmarcado en el proceso de construcción de aplicaciones de la subdirección de TIC en cabeza del departamento de Sistemas de Información, con la finalidad de

implementar los controles y fortalecer la disponibilidad de la información publicada en el ciberespacio.

- Identificar qué información se requiere publicar en el ciberespacio y el tratamiento de los riesgos de seguridad asociados. En coordinación con la subdirección de Gestión Documental de la Entidad y la dirección de Asuntos Jurídicos de la FGN, se debe avalar los controles de ciberseguridad a implementar de acuerdo con lo establecido en las normas vigentes para el manejo de información pública y el fortalecimiento de la tablas de retención documental. Esto como insumo para el grupo de seguridad de la información y el departamento de arquitectura para ser aplicadas en el diseño e implementación de los servicios tecnológicos a publicar en el ciberespacio que soportan las aplicaciones y los procesos con lo que se permitirá establecer la posición de la entidad para determinar las reglas de negocio a implementar en los desarrollos de las aplicaciones Web.
- Establecer los controles y componentes que favorezcan la continuidad de los servicios de información publicados en el ciberespacio, para lo cual se debe estandarizar y establecer con el departamento de Arquitectura de la Subdirección de TIC y la Dirección de Planeación, una arquitectura base de aplicaciones que incluya controles de seguridad basados en OWASP los cuales deberán ser documentados y monitoreados para determinar su nivel de efectividad.
- Mantener una capacidad de medición de indicadores de compromiso de seguridad y de mejoramiento continuo en el proceso de desarrollo seguro de aplicaciones Web. Para esto, en coordinación con el Departamento de Arquitectura Institucional, el de Infraestructura y Comunicaciones, el departamento de Sistemas de Información, así como el Grupo de Seguridad de la Información de la Subdirección de TIC, deben establecer como marco de referencia las fases para el desarrollo de aplicaciones basado en la ISO 12207 e implementar la arquitectura institucional en

sus dominios de sistemas de información así como el de uso y apropiación para mejorar el proceso y la arquitectura del software implementada en la plataforma tecnológica de la Entidad y el tratamiento de riesgos identificados en este trabajo investigativo.

- Implementar el modelo de seguridad y privacidad de información para el desarrollo seguro de aplicaciones web articulado con la actualización de procedimientos de seguridad y de los procedimientos de gestión de TIC en la entidad para el cumplimiento de leyes y regulación en tiempos adecuados no solo desde el punto de vista funcional sino desde la normatividad aplicada al área de seguridad y privacidad de la información con la participación de la Dirección de Planeación y la Dirección de Asuntos Jurídicos de la Entidad.

- Diseñar e implementar controles de seguridad para el proceso de construcción de aplicaciones web que soporten los servicios de información en el ciberespacio. En este sentido se debe:
  - Definir los criterios y componentes que permitan aplicar los principios de ciberseguridad en la arquitectura institucional relacionada con las aplicaciones web, para lo cual se deben realizar:
    - Revisión con el Departamento de Arquitectura, Departamento de Infraestructura y Comunicaciones, y el Grupo de Seguridad de la Información de la Subdirección de TIC, de los requerimientos de seguridad de los servicios tecnológicos, controles propuestos por el tratamiento de riesgos en el desarrollo de aplicaciones Web y drivers tecnológicos establecidos en la arquitectura empresarial de la Entidad.
    - Implementar controles para dar tratamiento de los riegos de ciberseguridad asociados a la publicación de información en el ciberespacio por parte de la Subdirección de TIC y en articulación con la Dirección de Planeación y de Gestión

documental de la FGN, los cuales deben ser gestionados de acuerdo con el modelo de gestión de riesgos de la Entidad. Para esto, se deberá realizar en las fases de ciclo de vida del software establecido en la resolución No 1261 del 23 de julio de 2014, donde se establecen la directrices y buenas prácticas para el desarrollo de sistemas de información en la Fiscalía General de la Nación.

- Características de resiliencia frente a riesgos de fallos de las aplicaciones web de la entidad.
  - Establecer los puntos de control de seguridad formulados a implementar dentro de la formulación de los requisitos a satisfacer con el proceso de construcción de aplicaciones web en coordinación con el departamento de Sistemas de Información de la Subdirección TIC y el grupo de Seguridad de la Información, así como en el cumplimiento de mejores prácticas en la codificación y en las pruebas técnicas o funcionales, así como en la gestión de cambios en la puesta en producción y en la estabilización de la plataforma en producción.
  - Realizar pruebas de seguridad en las fases de pruebas en ambientes de preproducción para detectar posibles riesgos de ciberseguridad en la publicación de servicios tecnológicos en el ciberespacio.
- Monitoreo y evaluación de los cambios significativos de riesgos, que para el caso del uso de las aplicaciones web. Para la gestión de cambios, se debe establecer en el comité de cambios análisis de indicadores de compromiso asociados a OWASP para evaluar el impacto de los cambios solicitados y determinar las acciones a implementar con el fin de minimizar el efecto no deseado de los riesgos descritos. Para esto, se debe fortalecer el procedimiento de gestión de cambios en los siguientes aspectos:

- Efectuar por parte del grupo de seguridad de información de la Subdirección de TIC el análisis del tratamiento de riesgos asociados a la solicitud de cambio en los servicios tecnológicos asociados con la publicación de información en el ciberespacio.
- Incorporar el resultado de análisis de riesgos asociados como parte de los criterios a tener en cuenta en la aprobación del despliegue de la solución.
- Generar y registrar el conocimiento de los resultados de la implementación del cambio.

o Incluir los criterios de gestión de la ciberseguridad y ciberdefensa en los procedimientos de Gestión de TIC relacionados con la gestión de riesgos asociados con las vulnerabilidades las aplicaciones web que representan un alto riesgo en el ciberespacio, en cuanto a mínimo:

- A1 – Inyección. De acuerdo con los controles implementados en la arquitectura de software se deben realizar pruebas de inyección de código en las consulta a bases de datos o de servicios web para realizar las recomendaciones de ajuste en el desarrollo de la aplicación o en la arquitectura.
- A2 – Pérdida de autenticación y gestión de Sesiones. En las pruebas funcionales y unitarias se debe incluir pruebas de la trazabilidad de la información de auditoria propia de la plataforma y de la aplicación en cuanto a los procesos de autenticación y rastro de las sesiones utilizadas por la aplicación.
- A3 – Secuencia de comandos en sitios cruzados (XSS). En las pruebas de construcción, despliegue y estabilización de la aplicación, se debe contemplas ambientes controlados (SANDBOX) para determinar la presencia de comandos maliciosos en los navegadores asociados al uso de los servicios tecnológicos a publicar en el ciberespacio o si es el caso

determinar procedimientos de análisis forense en caso de requerirse.

- A4 – Referencia Directa Insegura a Objetos. Para controlar este tipo de riesgos, se debe revisar la arquitectura y la codificación por parte del grupo de seguridad de la información de la subdirección de TIC para determinar el nivel de riesgo que se presenta en cuanto al uso de los objetos de la solución.
- A5 – Configuración de Seguridad Incorrecta. En los procesos de pruebas de preproducción el grupo de seguridad de la información de la Subdirección de TIC, debe establecer los riesgos asociados a la configuración de la solución de acuerdo con la documentación presentada por el departamento de sistemas de información y recomendar los ajustes en el código o en la arquitectura utilizada o en la plataforma tecnológica que soporta el funcionamiento de la aplicación
- A6 – Exposición de Datos Sensibles. De acuerdo con los controles de seguridad para mantener la privacidad de información que no debe ser de conocimiento del publico en general el grupo de seguridad de la información deberá realizar el análisis de vulnerabilidades de los desarrollos efectuados en cuanto a su diseño y puesta en funcionamiento de la solución.
- A7 – Ausencia de Control de Acceso a las Funciones. En los desarrollos de la aplicaciones se debe establecer los requerimientos de gestión de perfiles y privilegios de acuerdo con los roles establecidos en el proceso de gestión asociado o que apoya la aplicación para realizar por parte del grupo de seguridad de información de la subdirección de TIC las pruebas de acceso a las funciones de la aplicación y la efectividad de los controles de restricción y trazabilidad.

- A8 – Falsificación de peticiones en sitios Cruzados (CSRF) . Para identificar los comandos enviados por usuario autorizado al servidor web, el grupo de seguridad debe realizar pruebas de análisis de vulnerabilidades en las cabeceras de las peticiones y determinar si existen elementos que ejecute código malicioso o comportamientos de redireccionamiento a sitios web externos, así como controles de validación adicionales a los implementados.
- A9 – Uso de Componentes con Vulnerabilidades Conocidas. El grupo de seguridad debe realizar pruebas de seguridad de los nuevos componentes a incorporar en la arquitectura de software y analizar en coordinación con el departamento de Sistemas de Información las alternativas a la funcionalidad soportada y requerida por componentes que presentan vulnerabilidades conocidas.
- A10 – Redirecciones y reenvíos no validados. Con el análisis de vulnerabilidades y herramientas de análisis forense o de seguridad perimetral como FW, IDS/IPS, modeladores de tráfico, el grupo de seguridad debe desarrollar capacidades para establecer el comportamiento normal de las aplicaciones y el sistema de alarmas para detectar eventos de redirecciones o reenvíos no autorizados en el funcionamiento normal de la aplicación.

- Desarrollo e implementación de controles de seguridad acordes con la gestión de servicios tecnológicos y usuarios en el ciberespacio para atender los lineamientos de gobierno digital del estado colombiano. Atendiendo las directrices del ministerio de TIC en cuanto a gobierno digital, a seguridad y privacidad de la información y en materia de arquitectura empresarial, los controles a implementar en la arquitectura

    - de la aplicación deben estar en coherencia con los drivers tecnológicos de la arquitectura empresarial de la entidad y fortalecer la arquitectura de seguridad de la información de la entidad para asegurar los servicios tecnológicos disponibles por parte de la Entidad en el ciberespacio.
- Identificar los datos como activos de información de la entidad disponibles en el ciberespacio para establecer los controles a implementar. Teniendo en cuenta que uno de los objetivos del direccionamiento estratégico de la entidad es la construcción de un sistema de información unificado para soportar el proceso misional de la entidad, la Subdirección de TIC en coordinación con la Dirección de planeación de la Entidad deben realizar una selección de plataformas y arquitecturas de software unificadas con miras a optimizar los costos de operación o mantenimiento, para lo cual los activos de información asociados se debe desarrollar de la siguiente manera:
    - Identificar los datos a difundir en el ciberespacio y establecer los requerimientos de seguridad que deben cumplir los desarrollos de aplicaciones web y la gestión de los riesgos identificados, tal como lo enfoca Gasca. (Gasca-Hurtado, 2013), en cuanto a trazabilidad de datos y propiedad y seguridad de los datos.
    - Coordinar los desarrollos o adquisición de aplicaciones web enmarcados tanto en la gestión de TIC de la Entidad como en una arquitectura de seguridad para optimizar los recursos, capacidad de desarrollo y de integración para fortalecer la arquitectura de aplicaciones web basada en características de desarrollo de microservicios de seguridad para ofrecer soportar el desarrollo de todas las aplicaciones web.
    - Diseñar un plan de aseguramiento de las plataformas de desarrollo, pruebas, preproducción y producción mediante análisis de vulnerabilidades y acciones de remediación.
- Fortalecimiento del proceso de selección de Talento Humano y proveedores especializado en desarrollo de software y seguridad.
    - Con la implementación de la arquitectura institucional se requiere:

- Especializar el grupo seguridad de la información de la entidad para apoyar la construcción de las aplicaciones web.
- Seleccionar los proveedores de componentes de las aplicaciones web.
- Contar con un plan de entrenamientos con niveles básicos, intermedios y avanzados dependiendo de los roles en las diferentes fases de ciclo de vida del software en la Entidad.

- Generación de conocimiento especializado para el desarrollo de aplicaciones web.
  - Registro de la información asociada a la gestión de eventos e incidentes de seguridad asociados a la ciberseguridad y ciberdefensa aplicados en el ámbito del desarrollo de aplicaciones web de la FGN y la gestión de los riesgos asociados. Teniendo en cuenta los análisis de vulnerabilidades, pruebas y monitoreo de incidentes de seguridad de las aplicaciones web que soporten los servicios de información en el ciberespacio se debe registrar en una base de datos de conocimiento especializado para implementar herramientas de BIG DATA y de analítica para generar conocimiento de utilidad para la gestión y toma de decisiones que apoye el desarrollo de capacidades de respuesta y mantener un alto nivel en el tratamiento de amenazas y la mitigación de vulnerabilidades de las aplicaciones web.
  - Realizar pruebas integrales de las aplicaciones web a modificar o construir. Para desarrollar una conciencia de la utilidad de pruebas integrales con los componentes de seguridad de las aplicaciones web que soportan los servicios tecnológicos en el ciberespacio, se debe revisar el código fuente y la efectividad de los controles de desarrollo debe ser basado en las mejores prácticas como OWASP.
  - Ampliar la cobertura en las pruebas. Con la participación de las áreas funcionales y del grupo de seguridad de la información de la subdirección de TIC deben realizar las pruebas para la aprobación de la

puesta en funcionamiento de un servicio en el ciberespacio. Y adicionalmente, formular planes de cooperación interdepartamental al interior de la entidad en la ejecución de análisis de vulnerabilidades, con la capacidad de control y acción del SOC de la Entidad.

- Generar conocimiento de ciberseguridad y ciberdefensa a la alta dirección. Con la implementación de indicadores de compromiso soportados por el desarrollo de capacidades de análisis de eventos e incidentes de seguridad ocurridos en el ciberespacio en los tableros de control e informes de gestión se propone como un medio no solo de apoyo de toma de decisiones sino de desarrollo de conocimiento en materia de ciberseguridad y ciberdefensa aplicado en el desarrollo seguro de las aplicaciones web en los niveles altos de la Entidad como instrumento de soporte a la toma de decisiones.

- Implementar una arquitectura de software integrada con una Arquitectura de Seguridad.
  - Enmarcar dentro de la arquitectura de seguridad de la entidad la atención de los requerimientos funcionales en el ciberespacio para permitir la integración con la arquitectura y ofrecer a la comunidad el conocimiento de servicios de información.
  - Desarrollar controles que minimice el impacto de los riesgos identificados antes de iniciar los procesos de construcción de las aplicaciones Web de la Entidad y optimizar los recursos de desarrollo para atender las recomendaciones y lineamientos de seguridad para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de la publicación de información en el ciberespacio.

6.2.Lineamientos para la gestión de aplicaciones web en la fiscalía general de la nación.

Teniendo en cuenta los requerimientos establecidos en el **Anexo No 5.** Requerimientos y Requisitos se formulan los siguientes lineamientos:

Tabla 15
Lineamientos para la gestión de aplicaciones Web

Lineamiento	Descripción

Medir el nivel de cumplimiento y formulación de los requisitos de seguridad a los datos para permitir que estos estén disponibles y accesibles.	Diseñar controles y mecanismos de medición para los siguientes criterios: - V1. Arquitectura, diseño y requerimientos de modelamiento de Amenazas - V2: Requisitos de verificación de autenticación - V9: Requisitos de verificación de comunicaciones - V10: Requisitos de verificación de código malicioso - V11: Requisitos de verificación de la lógica de negocios - V12: Requisitos de verificación de archivos y recursos - V13: Requisitos de verificación de servicios web y API. Comunicar y alinear los procesos de construcción de aplicaciones web en cuanto a: - V3: Requisitos de verificación de gestión de sesión - V4: Requisitos de verificación de control de acceso - V5: Requisitos de validación, desinfección y verificación de codificación - V6: Requisitos de verificación de criptografía almacenada - V8: Requisitos de verificación de protección de datos - V14: Requisitos de verificación de la configuración Formalizar los procedimientos con respecto a: V7: Gestión de errores y requisitos de verificación de registro.
Fortalecer el Sistema de Gestión de Seguridad de la información para ampliar la cobertura al proceso de desarrollo de aplicaciones web.	Fortalecer las políticas de seguridad de la información para el desarrollo de aplicaciones web en cuanto al dominio de: A5 Políticas de seguridad de la información. Formalizar los procedimientos con respecto a: - A6 Organización de la seguridad de la información. - A9 Control de acceso. - A10 Criptografía. - A12 Seguridad de las operaciones. - A16 Gestión de incidentes de seguridad de la información. - A14 Adquisición, desarrollo y mantenimiento de los sistemas de información. Definir procedimientos con respecto a: - A13 Seguridad de las comunicaciones. - A18 Cumplimiento.

Fuente: Aporte del autor basado en ISO 27002, (Carlos Ortiz de Zevallos, 2016) y OWASP, (Novillo Vicuña J. P., 2019)

De lo formulado y teniendo en cuenta que la política de seguridad de la información de la Entidad fue formulada tomando como marco de referencia la ISO/IEC 27001, se propone las siguientes actividades el establecimiento de estos lineamientos en la Entidad:

- Medir el nivel de cumplimiento y formulación de los requisitos de seguridad a los datos para permitir que estos estén disponibles y accesibles. En cuanto a la gestión del desarrollo de aplicaciones web en la entidad, uno de los factores primordiales es la medición para lo cual se propone en el marco de un sistema de gestión de seguridad de la información realizar las siguientes tareas para diseñar e implementar controles y mecanismos de medición:

- V1. Arquitectura, diseño y requerimientos de modelamiento de Amenazas. Para el control y monitoreo de la efectividad de la implementación de las arquitecturas empresariales, de plataforma tecnológica y de seguridad, se debe desarrollar:
  - Formulación de indicadores de compromiso en cada uno de los componentes de las arquitecturas en coordinación con el grupo de seguridad de la información como los departamentos de la Subdirección de TIC.
  - Dentro del modelo de gestión de riesgos de la entidad se debe realizar una validación en cuanto a los riesgos identificados en el Anexo No 1, con el fin de darles el tratamiento correspondiente enmarcado en el sistema de gestión integral de la entidad.
  - Coordinar con la subdirección de control interno para incluir dentro del plan anual de auditorias las concernientes al control de las amenazas relacionadas con el desarrollo de las aplicaciones web y con la gestión de riesgos en la publicación de información en el Ciberespacio.
- V2: Requisitos de verificación de autenticación. Con el establecimiento de los controles de autenticación enmarcados en el marco de referencia OWASP, de manera conjunta entre el Grupo de Seguridad y el departamento de sistemas de información de la Subdirección de TIC, se deben documentar y evaluar los controles de verificación de acceso utilizado por las aplicaciones web.
- V9: Requisitos de verificación de comunicaciones. Entre el departamento de Infraestructura y Comunicaciones, el departamento de Sistemas de

Información y el grupo de seguridad de la información se debe establecer los controles a implementar en las aplicaciones y en las plataformas tecnológicas asociadas para controlar las comunicaciones de los componentes de la aplicación y determinar los críticos a monitorear y controlar.

- V10: Requisitos de verificación de código malicioso. En coordinación entre el grupo de Seguridad de la Información y el Departamento de Sistemas de Información se debe establecer los puntos de control y lo criterios de desarrollo seguro de aplicaciones web. Posteriormente, se incluirán en los planes de pruebas los mecanismos de medición a realizar por el grupo de seguridad de la información.
- V11: Requisitos de verificación de la lógica de negocios. Teniendo en cuenta que existen requerimientos de seguridad funcionales y de auditoria en la fase de definición de requisitos, el grupo de seguridad y el departamento de Sistemas de Información deberá validar el registraro en la plataforma de gestión de requerimientos para realizar la trazabilidad del caso y validarlo dentro del proceso de construcción de la aplicación web y del uso de los servicios tecnológicos a publicar en el ciberespacio.
- V12: Requisitos de verificación de archivos y recursos. Se debe realizar una validación con el departamento de infraestructura, grupo de seguridad de la información y sistemas de información para identificar los mecanismos de uso de los controles de acceso a recursos de archivos que consumen las aplicaciones web y de las necesidades de ciframiento de la información en el

ciberespacio para aquellos servicios que están orientados a disponer en el ciberespacio de información pública reservada o pública clasificada, que se ve declarada en el índice de tratamiento de información de la Entidad, la cual debe ser actualizada por Gestión Documental, Subdirección de TIC y la Dirección de Asuntos Jurídicos en el campo especifico de información digital.

  - V13: Requisitos de verificación de servicios web y API. Con el fin de construir un anillo de seguridad en cuanto a los servicios o microservicios implementados en la arquitectura de las aplicaciones, se debe documentar los servicios construidos e incluir las buenas prácticas y controles de ciberseguridad implementados para que la aplicación este en capacidad de acceder y transmitir información entre diferentes sistemas de información del entorno en que se desenvuelve la Fiscalía.

- Comunicar y alinear los procesos de construcción de aplicaciones web en cuanto a:
  - V3: Requisitos de verificación de gestión de sesión. Para establecer los requerimientos de gestión de la sesiones, son el departamento de Sistemas de información y el Grupo de Seguridad de la información de la subdirección de TIC, que de acuerdo con los riesgos identificados en el Anexo No 1, que se deben monitorear la efectividad de los controles de acceso y mantenimiento de las sesiones utilizadas en las aplicaciones web con el fin de no perder la visibilidad y trazabilidad de la permanencia de la sesión y evitar los riesgos asociados a una posible suplantación o redirección.
  - V4: Requisitos de verificación de control de acceso. Una vez identificados los requisitos de control de acceso de la aplicación, las áreas funcionales y los

ingenieros que tienen como rol definir los requisitos de desarrollo deben registrar los cambios en los mecanismos de control de acceso de la arquitectura que ofrece la arquitectura para que conjuntamente con el Grupo de Seguridad de la Información determinen los riesgos asociados a los cambios efectuados y se determinen los ajustes a realizar en la arquitectura necesaria para atender los requerimientos identificados.

- V5: Requisitos de validación, desinfección y verificación de codificación. Teniendo en cuenta que el departamento de Sistemas de Información tiene la autonomía para implementar las metodologías de desarrollo ágil como es el caso de SCRUM, en coordinación con el grupo de Seguridad de la Información de la subdirección de TIC se deben realizar las siguientes actividades:
  - Establecer los puntos de control para realizar las tareas periódicas de desinfección de las plataformas de desarrollo.
  - Realizar el análisis de código desarrollado para determinar vulnerabilidades de la codificación realizada.
  - Realizar el análisis de la documentación para determinar el grado de actualización de acuerdo con los cambios realizados.
- V6: Requisitos de verificación de criptografía almacenada. Dada la sensibilidad de la implementación de controles de criptografía en las aplicaciones web, se debe realizar las siguientes actividades:

- Identificar los archivos o repositorios que requieren de servicios de criptografía, de acuerdo con los perfiles y procedimientos de gestión de usuarios establecido por parte de las áreas funcionales y los ingenieros de requerimientos de la Subdirección de TIC.
- Por parte del departamento de infraestructura en coordinación con el Grupo de Seguridad de la Información deben establecer los controles de gestión de llaves de los servicios de encripción para mitigar los riesgos de pérdida de información en los procesos de recuperación de llaves.

- V8: Requisitos de verificación de protección de datos. En la definición de los requisitos de la aplicación se debe establecer aquellos que son procedentes por la aplicación de la normatividad con la participación de las áreas funcionales y los ingenieros de definición de requerimientos acorde con la normatividad vigente.
- V14: Requisitos de verificación de la configuración. Teniendo en cuenta los requisitos de funcionamiento de los componentes de la arquitectura de software que hace uso las aplicaciones web, el departamento de Sistemas de Información debe:
  - Documentar los requisitos de funcionamiento de la aplicación.
  - Informar al Grupo de Seguridad de la Información de los nuevos componentes para su análisis y monitoreo.
  - Solicitar los accesos a internet de los componentes para ser valorados y viabilizados por el grupo de Seguridad de la Información.

- Formalizar los procedimientos con respecto a: V7: Gestión de errores y requisitos de verificación de registro. Para el control de errores y de registros a efectuar por parte de la aplicación se debe realizar las siguientes actividades por parte del departamento de sistemas de información y el grupo de seguridad de la información:
    - Identificar y documentar los controles de gestión de errores de la aplicación así como los mecanismo de registro del caso.
    - Definir los indicadores de compromiso asociados con los errores detectados en el funcionamiento de las aplicaciones web.
    - Monitorear el comportamiento de los indicadores de compromiso.
- Fortalecer el Sistema de Gestión de Seguridad de la información para ampliar la cobertura al proceso de desarrollo de aplicaciones web, con las siguientes actividades:
    - Determinar el alcance de la plataforma de seguridad para el monitoreo y tratamiento de los eventos e incidentes de seguridad ocurridos en el ciclo de vida del software asociado con la construcción de aplicaciones web.
    - Relacionar los eventos con los riesgos identificados en el funcionamiento de la aplicaciones web y los servicios tecnológicos que soportan la publicación de información de la Entidad en el ciberespacio.
- Fortalecer las políticas de seguridad de la información para el desarrollo de aplicaciones web en cuanto al dominio de:
    - A5 Políticas de seguridad de la información. Con respecto al desarrollo seguro de las aplicaciones web y la gestión de riesgos de ciberseguridad en la publicación de información en el ciberespacio se debe realizar la siguientes

tareas en cabeza del grupo de seguridad de la información de la Subdirección de TIC y el oficial de seguridad de la Dirección de Planeación:

- Incluir una política específica construida a partir de los lineamientos generales propuestos para establecer la posición de la Entidad.
- Realizar el seguimiento en el cumplimento de las políticas específicas establecidas.
- Valorar periódicamente la validez y efectividad de la política formulada.
- Gestionar los cambios en la política necesarios para la gestión de la seguridad en el desarrollo de aplicaciones web.

- Formalizar los procedimientos con respecto a:
  - A6 Organización de la seguridad de la información. A partir de la implementación de la arquitectura empresarial de la Entidad, (Nación F. G., RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES, 2018), se debe estructurar de manera interna el Grupo de Seguridad de la Información y el Departamento de Sistemas de Información para gestionar de manera conjunta incluyendo las siguientes actividades:
    - Identificación de los puntos de control a implementar en los procesos de construcción y seguridad de las aplicaciones web.

- Establecimiento de los controles a implementar con respecto al desarrollo seguro de las aplicaciones web y del tratamiento de los riesgos de la información disponible en el ciberespacio.
- Establecimiento de indicadores de compromiso para medir el grado de efectividad de los controles implementados.
- Mejoramiento de los procedimientos para la construcción de aplicaciones web.
- Mejoramiento de los procedimientos para la gestión de seguridad de la información.
- Evaluación periódica de los resultados.

▪ A9 Control de acceso. Para implementar este control se deben realizar las siguientes tareas de manera coordinada:

- Identificación y definición de perfiles, autorizaciones y roles de los usuarios de la aplicación web.
- Establecer los puntos de control de acceso de las aplicaciones de manera conjunta entre las diferentes áreas de la Subdirección de TIC.
- Formulación de un protocolo de implementación de controles de acceso por parte de los desarrolladores del departamento de Sistemas de Información.
- Definición y ejecución de un plan de pruebas a efectuar por el Grupo de Seguridad de la Subdirección de TIC.

- Formulación de acciones de mejora en la implementación y diseño a que haya lugar.

- A10 Criptografía. El Grupo de Seguridad de la Información en coordinación con el Oficial de Seguridad y la Subdirección de Gestión Documentar, deberán establecer:
  - La clasificación y Tablas de Retención Documental, a aplicar en la información a publicar en el ciberespacio y el grado de confidencialidad o reserva que deben controlar las aplicaciones Web.
  - Establecer una política de gestión de llaves y claves para determinar los criterios de asignación, recuperación y protección de llaves utilizadas para el ciframiento de información.
  - Definir las tablas de retención documental a implementar en la información cifrada.
- A12 Seguridad de las operaciones. Para la operación se propone realizar las siguientes tareas en coordinación con todas las áreas de la Subdirección de TIC y del oficial de seguridad de la información de planeación:
  - Valorar los aspectos a incluir en los procedimientos de operación de la Subdirección de TIC con respecto a la gestión de cambios de las aplicaciones web, y de las capacidades de

gestión para atender los requerimientos de publicación de información en el ciberespacio.

- Documentación de los controles implementados para proteger las aplicaciones web de código malicioso y determinar los indicadores de compromiso a aplicar.
- Documentar los controles implementados de la información de auditoria de las aplicaciones web como el registro de actividades realizadas y del manejo de la hora legal colombiana.
- Identificación de vulnerabilidades detectadas en la operación para establecer un plan de mejoramiento de la aplicación Web.

- A16 Gestión de incidentes de seguridad de la información. El grupo de Seguridad de la Información debe:
  - Fortalecer las capacidades de gestión de incidentes para incluir en el proceso de construcción de las aplicaciones Web puntos de control dentro del ciclo de vida, tal como identificar los requerimientos de Ciberseguridad y Ciberdefensa de la Aplicación Web.
  - Definir planes de pruebas de ciberseguridad ciberdefensa para establecer:
    - Calidad de la definición de los requisitos de ciberseguridad de la aplicación.

- Ejecución de planes de pruebas de ciberseguridad de los desarrollos efectuados acorde con los controles establecidos y la política de seguridad de la Entidad.
- Elaborar conceptos e informes de seguridad de las aplicaciones web en construcción, en proceso de puesta en funcionamiento o en producción.
- Realizar el seguimiento a los planes de mejoramiento formulados en lo relacionado con la ciberseguridad y la ciberdefensa.

- A14Adquisición, desarrollo y mantenimiento de los sistemas de información. El departamento de Sistemas de Información y el Grupo de Seguridad de la Información de la Subdirección de TIC debe establecer y ejecutar las siguientes tareas:
  - Evaluar el impacto de los cambios solicitados a realizar en la aplicación web de acuerdo con los procesos de control de cambios establecido.
  - Evaluar la seguridad en los entornos de desarrollo, calidad, preproducción y producción.
  - Evaluar el impacto y las restricciones en el desarrollo o de tercerización de las aplicaciones web.
  - Implementar controles de seguridad para proteger los datos de prueba y no exponer a la Entidad ante incidentes de pérdida de confidencialidad de la información sensible de la Entidad.

- Evaluar la efectividad de las pruebas realizadas en el ciclo de vida de las aplicaciones web y que soportan los servicios de publicación de información institucional en el ciberespacio.

- A13 Seguridad de las comunicaciones. El grupo de seguridad de la información y el departamento de Infraestructura y comunicaciones, debe adelantar las siguientes tareas:
  - Documentar los servicios de red asociados o utilizados por las aplicaciones Web para la publicación de servicios tecnológicos en el ciberespacio.
  - Evaluar la efectividad de los controles de red implementados para la publicación de información sensible en el ciberespacio.
  - Establecer los requisitos de seguridad de la infraestructura para el intercambio de información efectuados por las aplicaciones web de la Entidad.
  - Evaluar el uso de los acuerdos de seguridad utilizados en el intercambio de información realizada por las aplicaciones Web de la Entidad.
- A18 Cumplimiento. En coordinación con la alta dirección de la Subdirección de TIC, el área funcional que ha solicitado publicación de información en el ciberespacio y el grupo de seguridad debe:
  - Identificación del impacto normativo y contractual de la publicación de información.

- Evaluar los mecanismos de protección de seguridad y privacidad de la información, así como el cumplimiento de la norma en cuanto a la protección de datos personales.
- Establecer o coordinar los mecanismos de control de cumplimiento de la política de seguridad por parte de terceros.

6.3.Lineamientos estratégicos de competencia de negocio - CBS.

Para posicionar las aplicaciones web en la entidad y como plataforma tecnológica que soporta los servicios de información en el ciberespacio se debe realizar con una estrategia de diferenciación con características de calidad y seguros que apoyen la ejecución del plan de direccionamiento de la entidad, para esto se debe:

Lineamiento	Descripción
Desarrollo de aplicaciones web especializados en judicialización e investigación.	Con el conocimiento y fortalecimiento de los procesos de la entidad y de las capacidades de seguridad se debe satisfacer las necesidades de automatización y protección de seguridad de acuerdo con las leyes vigentes del estado, es decir, ofrecer servicios coordinados y de calidad que permita desarrollar capacidades de investigación y judicialización en el ciberespacio y permita optimizar las cargas de trabajo que tiene cada una de las entidades para detectar requerimientos duplicados por parte de los usuarios finales del servicio de investigación y judicialización en el ciberespacio.
Generar conocimiento institucional en la construcción de software seguro.	Para atender las necesidades de automatización de los procesos misionales que soportan los servicios en el ciberespacio, requiere de contar con una capacitación altamente especializada en cuanto al desarrollo seguro y el cumplimiento de la política de seguridad de la información de la Entidad. Para complementar las capacidades de control en la implementación de las aplicaciones web, se aprovecha la integración de la arquitectura de software con componentes de control como: Herramientas de gestión de perfiles y roles de usuarios. Herramientas de controles de acceso a bases de datos por roles. Herramientas de auditorías.

Fuente: Aporte del autor

De lo formulado, se propone las siguientes actividades para el establecimiento de estos lineamientos en la Entidad:

- Desarrollo de aplicaciones web especializados en judicialización e investigación.
    - Con el conocimiento y fortalecimiento de los procesos de la entidad y de las capacidades de seguridad se debe satisfacer las necesidades de automatización

y protección de seguridad de acuerdo con las leyes vigentes del estado como es el caso de:

- La ley 1581 del 2012 con la protección de datos personales, en particular con lo referente con el tratamiento de datos en el territorio colombiano, el cual debe ser ampliado en el ámbito del ciberespacio.
- La ley 1342 de 2009, con la que se establece los principios de la sociedad de la información.
- Decreto 2106 de 2019, con la finalidad de optimizar la gestión de la administración pública.
- Conpes 3975 de 2019, donde se establece la política de transformación digital.
- Conpes 3854 de 2016, donde se establece la política nacional de seguridad digital.
- Ley 1908 de 2018, donde se busca fortalecer la investigación y judicialización de organizaciones criminales.
- Ley 1928 de 2018, por medio de la cual se reconoce el convenio de ciberdelincuencia propuesto en Budapest, y establece lineamientos para el manejo de información y aspectos de cooperación internacional.
- Norma ISO/IEC 27002 en cuanto a los controles a implementar en un sistema de gestión de seguridad de la información.
- Norma ISO/IEC 27032, en cuanto a aspectos a tener en cuenta en ciberseguridad.

- Norma ISO/IEC 27035, en cuanto a la gestión de incidentes de seguridad.
- Norma ISO/IEC 27034, en cuanto a la seguridad de aplicaciones.
- Norma ISO/IEC 27037, 27038, 27041, 27042, 27043, en cuanto a la evidencia digital.
- Ley 489 de 1998, donde establece los principios de función pública.
- Ley 2693 de 2012, donde se define la estrategia de gobierno en línea.

Es decir, ofrecer servicios coordinados y de calidad que permita desarrollar capacidades de investigación y judicialización en el ciberespacio y permita optimizar las cargas de trabajo que tiene cada una de las entidades para detectar requerimientos duplicados por parte de los usuarios finales del servicio de investigación y judicialización en el ciberespacio.

- Generar conocimiento institucional en la construcción de software seguro. En coordinación con el departamento de altos estudios, y en la línea de generar conocimiento especializado, se propone realizar las siguientes tareas:
  - Diseñar y ejecutar un plan de capacitación orientada a la alta dirección para generar conciencia y cultura de la necesidad de gestionar la ciberseguridad de las aplicaciones web de la Entidad, y no realizar únicamente esfuerzos para atender las necesidades de automatización de los procesos misionales que soportan los servicios en el ciberespacio, y el cumplimiento de la política de seguridad de la información de la Entidad.

- Identificar los aspectos legales y normativos para consolidar programas de formación en aspectos normativos y legales aplicables en el control del ciberespacio.
- Para complementar las capacidades de control en la implementación de las aplicaciones web, se propone en el proceso de integración de la arquitectura de software incluir componentes de:
  - Herramientas de gestión de perfiles y roles de usuarios.
  - Herramientas de controles de acceso a bases de datos por roles.

6.4.Lineamientos estratégicos de compensación y beneficios ejecutivos – CEBD.

Con el desarrollo o adquisición de aplicaciones web que soportan los servicios tecnológicos de la entidad en el ciberespacio permite ofrecer un portafolio de consulta e intercambio de información con calidad y características de seguridad que permite apoyar el cumplimiento del direccionamiento estratégico referido al fortalecimiento del acceso a la justicia, la optimización de los procesos de divulgación o publicación de información con respecto a:

Tabla 16 6.4.
Lineamientos estratégicos de compensación y beneficios ejecutivos – CEBD.

Lineamiento	Descripción
Cooperación e intercambio de información entre entidades del estado de manera segura soportada por aplicaciones web.	Con el apoyo de la alta dirección para el desarrollo de las capacidades del equipo técnico y funcional para que participen de manera articulada en el ciclo de vida del software atendiendo las mejores prácticas de desarrollo seguro del entorno académico y comercial permite implementar servicios de información para atender las necesidades de intercambio y publicación de información en el ciberespacio que permiten la construcción de un portafolio de información a ofrecer al entorno.
Seguimiento a los costos asociados para el aseguramiento de las aplicaciones web.	Implementar indicadores de inversión y costos internos para el aseguramiento de las aplicaciones web.

Fuente: Aporte del autor

De lo formulado, se propone las siguientes actividades para el establecimiento de estos lineamientos en la Entidad:

- Cooperación e intercambio de información entre entidades del estado de manera segura soportada por aplicaciones web. Con el apoyo de la alta dirección y de las funciones de policía judicial que realiza la Entidad, se propone realizar:
    - El fortalecimiento de las capacidades de monitoreo de los servicios de intercambio de información mediante la implementación de controles de ciberseguridad en la infraestructura tecnológica.
    - Definición de protocolos de ciberseguridad como anexos a los convenios para asegurar la gestión de la información que se pone a disposición en el ciberespacio para su uso por los diferentes actores de la administración de justicia y la ciudadanía en general.
    - El acompañamiento de las áreas funcionales de la Entidad para que participen de manera articulada en el ciclo de vida del software atendiendo las mejores prácticas de desarrollo seguro del entorno académico y comercial.
    - Contemplar interfaces de intercambio de información lideradas por el grupo de seguridad de la información de la subdirección de TIC y el oficial de seguridad para:
        - Definir el plan de implementación de los servicios de información para atender las necesidades de intercambio y publicación de información en el ciberespacio que permiten la construcción de un portafolio de información a ofrecer al entorno.
        - Establecer los datos a intercambiar con ColCERT, el comando conjunto cibernético y el centro cibernético policial.

- Seguimiento a los costos asociados para el aseguramiento de las aplicaciones web. En coordinación con la Subdirección de TIC, la dirección de planeación y la subdirección contractual, se debe realizar la planificación y ejecución de los planes de aseguramiento de las aplicaciones de la siguiente manera:
    - Identificación y documentación de las necesidades, objetivos y parámetros de gestión del riesgo de la publicación de información institucional en el ciberespacio.
    - En caso de requerirse, adelantar los procesos de contratación de terceros para fortalecer las aplicaciones web de la Entidad.
    - Diseñar e implementar indicadores de inversión y costos internos para el aseguramiento de las aplicaciones web.

6.5. Lineamientos Gobernabilidad y coordinación efectiva.

En la estrategia de ciberseguridad y ciberdefensa se establecen como lineamientos de gobernabilidad y aseguramiento de los servicios de información disponibles en el ciberespacio con integración y coordinación de:

Tabla 17
Lineamientos Gobernabilidad y coordinación efectiva.

Lineamiento	Descripción
Procesos de gestión de TIC.	En este sentido es necesario fortalecer y ampliar las capacidades de seguridad de la plataforma de TIC de la Entidad.
Planeación y desarrollo.	En los programas de desarrollo de la entidad, se debe contar con la formulación de proyectos de fortalecimiento de las capacidades de gestión se debe incluir los componentes necesarios para asegurar los servicios de información de la entidad en el ciberespacio.
Innovación.	Con el desarrollo de grupos o roles para el desarrollo de soluciones tecnológicos la innovación en un marco de austeridad estratégica permite optimizar los procesos y desarrollo tecnologías que permitan fortalecer las aplicaciones web.
Normativo	Cumplimiento de las normas vigentes, así como los principios de administración y función pública.
Integración con el Sistema de Gestión Integral de la Entidad.	En este sentido, y tal como lo establece la resolución No 1165 de 2018, se incorpora funciones y capacidades para la gestión de la seguridad de la información.

Fuente: Aporte del autor

De lo formulado, se propone las siguientes actividades para el establecimiento de estos lineamientos en la Entidad:

- Implementar indicadores de inversión y costos internos para el aseguramiento de las aplicaciones web.
    - A partir de los indicadores de compromiso de seguridad se deben construir tableros de control para medir la capacidad de gestión de eventos e incidentes de seguridad.
    - Establecer con el departamento de arquitectura los indicadores de ejecución de proyectos de ciberseguridad y ciberdefensa para ampliar la cobertura de monitoreo de la plataforma de ciberseguridad de la Entidad.
- Planeación y desarrollo.
    - En coordinación con el departamento de arquitectura y el grupo de seguridad de la información de la subdirección de TIC, se debe establecer los programas de desarrollo de la ciberseguridad en la Entidad en materia de la construcción de aplicaciones Web.
    - En coordinación entre el Departamento de Altos Estudios de la Entidad y la Subdirección de TIC se debe establecer los programas de capacitación especializada en marcos de referencia de seguridad de aplicaciones.
- Innovación.
    - Con el respaldo de la alta dirección y en coordinación entre el Departamento de Altos Estudios de la Entidad se debe formular planes de capacitación para aumentar la capacidad de desarrollo seguro de aplicaciones web.
    - Para fomentar la investigación al interior de la Entidad en materia de ciberseguridad y ciberdefensa, se propone fomentar los convenios con universidades en donde participen funcionarios de todo nivel de la entidad para desarrollar la capacidad de innovación que requiere la Entidad.
    - Optimizar los procedimientos de gestión de ciberseguridad y ciberdefensa para que con los recursos con que cuenta la entidad se promueva la innovación en los procesos de la entidad.

- Incluir en los programas de formación del Departamento de Altos Estudios la difusión de conocimiento producto de la investigación hacia la comunidad de la Entidad.

- Normativo.
  - Definir y mantener un marco normativo con aplicación a la publicación de información en el ciberespacio para determinar los requisitos a atender en el desarrollo de aplicaciones Web. Esto en coordinación con la Dirección de Asuntos Jurídicos de la Entidad y la Dirección de planeación, y con el apoyo de la Subdirección de TIC.
  - Formular un plan de evaluación del cumplimiento de las normas vigentes en las aplicaciones Web, así como los principios de administración y función pública. Esta labor se debe adelantar por el grupo de Seguridad y el Departamento de Arquitectura de la Subdirección de TIC y la Subdirección de Control Interno.

- Integración con el Sistema de Gestión Integral de la Entidad. En este sentido, y tal como lo establece la resolución No 1165 de 2018, se incorpora funciones y capacidades para la gestión de la seguridad de la información, para lo cual se formulan las siguientes tareas a desarrollar:
  - En coordinación con el departamento de arquitectura y el grupo de seguridad de información de la Subdirección de TIC y la Dirección de Planeación, con su oficial de seguridad deben establecer la arquitectura de seguridad para definir los controles a diseñar e implementar en la arquitectura empresarial de la Entidad.
  - Construir los driver de arquitectura empresarial en cuanto a ciberseguridad y ciberdefensa.
  - Definir los programas y planes de ciberseguridad a desarrollar en un nuevo periodo de administración.

6.5. Alternativas de los lineamientos para la formulación de lineamientos estratégicos de ciberseguridad y ciberdefensa.

Para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio, se definen tres alternativas basadas en la implementación de:

- La ISO 27002, en el dominio No 10 para establecer los planes de implementación de los lineamientos estratégicos y la gestión de los riesgos.
- El marco de referencia OWASP, (Novillo Vicuña J. P., 2019).
- Complementar el planteamiento de ISO 27002 con OWASP, (Novillo Vicuña J. P., 2019).

De lo anterior, se estima como mejor alternativa de formulación de lineamientos la de complementar el planteamiento de ISO 27002 con OWASP, (Novillo Vicuña J. P., 2019), dado que se ajusta a las siguientes líneas de acción de la entidad:

- Efectividad de los servicios de justicia con el fortalecimiento de la capacidad de desarrollo seguro en las áreas de TIC de la Entidad.
- Adaptación al Entorno mediante el aseguramiento de las aplicaciones web existentes:
- Generación de innovación mediante el desarrollo de I+D+i en materia de seguridad de Aplicaciones web.

6.6. Objetivos de los lineamientos estratégicos de ciberseguridad y ciberdefensa.

Como objetivo global se formula la estandarización de características y procedimientos de seguridad para el diseño, implementación y uso de las aplicaciones web, así como las capacidades de detección, monitoreo y respuesta de en los ciberataques a las aplicaciones web de la entidad.

En este sentido, para a las aplicaciones web es coherente con los parámetros que requiere una estrategia de ciberseguridad y ciberdefensa en el sector justicia se propone:

- **Generar valor agregado con el desarrollo de las aplicaciones web de la entidad**. Con las funciones dinamizadoras se debe soportar los desarrollos para la prestación de los servicios de la entidad y facilitar el alinearse con la cultura organizacional y con los objetivos estratégicos de la Entidad.

- **Flexibilizar y adaptar los desarrollos de aplicaciones web al Entorno.** En el sector justicia se requiere un alto nivel de cambio en cuanto a normatividad que hace que los procesos sean constantemente revisados y en algunos casos ajustados que ocasiona que las aplicaciones web evolucionen de manera ágil y asertiva.
- **Apoyar la efectividad de los servicios de justicia**. La ciudadanía exige efectividad en los procesos que adelanta la entidad y por lo tanto, la Fiscalía debe soportar en la maduración de sus procesos una gestión efectiva de los servicios de información en el ciberespacio y desarrollar habilidades que tiene el talento humano en cuanto a lo misional y en los procesos de apoyo.
- **Generar conocimiento e innovación en el proceso de construcción y mantenimiento de aplicaciones web.** Desarrollar un plan de gestión del conocimiento en cabeza del departamento de altos estudios de la Fiscalía General de la Nación y generar proceso de innovación para el tratamiento de pruebas científicas en los procesos judiciales en la hace uso de la experiencia y conocimiento organizacional.
- **Crear cultura de ciberseguridad en el proceso de construcción de aplicaciones Web.** La entidad reconoce gran importancia en la credibilidad de la labor que cumple en el desarrollo de aplicaciones web seguras.
- **Formular proyectos de desarrollo de aplicaciones Web enmarcadas en una gestión integral de TI.** En el área de TIC gestionar la adquisición o desarrollo de aplicaciones web de acuerdo con las características de las plataformas de tecnologías de la entidad, seguridad informática, servidores, almacenamiento o redes LAN o WAN en un entorno de austeridad estratégica.
- **Coordinar con el área de planeación la gestión de TIC en cuanto a la priorización de desarrollos de funcionalidad de las aplicaciones web de la entidad.** Priorizar desarrollos en el marco de los lineamientos establecidos por la administración pública, normatividad vigente, intercambio de información entre entidades mediante la implementación de convenios para la administración de justicia y marcos de referencia de gestión, en el ámbito de ciberseguridad y ciberdefensa, se aborda como seguridad de la información.

- **Asegurar el ciclo de vida de las aplicaciones web de la Fiscalía General de Nación.** Mediante el aseguramiento de las diferentes fases de desarrollo, implementación y uso, incluyendo los procesos de adquisición, así como la formulación de una política de desarrollo o adquisición de aplicaciones web de la entidad para:
    - Identificar los diferentes actores en el desarrollo, adquisición, implementación y uso de las aplicaciones web, y asegurar los procesos y procedimientos del caso.
    - Lograr un adecuado nivel de resiliencia en las aplicaciones web de la Fiscalía General de la Nación.
    - Fortalecer las capacidades de detección temprana y de reacción en el ciclo de vida de las aplicaciones web.
    - Sensibilizar a los diferentes actores involucrados en el ciclo de vida de las aplicaciones web.
    - Consolidar y fortalecer el conocimiento de los actores involucrados en el ciclo de vida de las aplicaciones web.

6.7. Propuesta de implementación de los lineamientos estratégicos de ciberseguridad y ciberdefensa.

Se identifican las siguientes líneas de acción en la implementación de aplicaciones web:

- **Efectividad de los servicios de justicia** con el fortalecimiento de la capacidad de desarrollo seguro en las áreas de TIC de la Entidad.

Objetivo	Crear un proceso de desarrollo de aplicaciones web seguros en la prestación de servicios en la nube.					
Alcance	En término de una vigencia, se debe establecer el proceso mediante la declaración del proceso de desarrollo y del procedimiento en las diferentes etapas del ciclo de vida de software en la entidad, para lo cual, es la Subdirección de TIC la encargada de la formulación de lo correspondiente.					
Recursos:	Se contará con desarrolladores propios para atender las demandas de automatización de procesos para lo cual se cuenta con una plataforma virtualizada que provee los componentes de hardware y software necesarios para la configuración de las plataformas de desarrollo, pruebas, preproduccion y producción.					
Actividades	Tiempo	Lugar	Unidades	Recursos	Seguimiento	Logros

Capacitar a los desarrolladores o líderes de proyectos de aplicaciones web.	12 meses	Fiscalía	Reuniones de entendimiento con el equipo desarrollador.	4 desarrolladores senior 24 desarrolladores y tester	Mediciones en la calidad del código desarrollado	Establece una cultura de desarrollo seguro.
Implementar controles en las diferentes fases del ciclo de vida del sistema de información.	12 meses	Fiscalía	Número de procedimientos establecidos en el proceso de desarrollo de software.	1 coordinador de calidad. 4 profesionales de calidad	Evaluación de procedimientos y guías controladas	Estandarizar el proceso de desarrollo seguro.
Identificar y asegurar los componentes externos a incluir en la arquitectura del sistema de información.	12 meses	Fiscalía, entidades del estado	Número de componentes asegurados.	2 ingenieros de requerimientos. 24 desarrolladores y tester	Establecimiento de requisitos de intercambio de información con otras entidades	Implementar los componentes de la arquitectura institucional para el intercambio de información.
Lograr la cooperación de entidades afines a nivel regional o nacional.	12 meses	Fiscalía, entidades del estado	Número de convenios con anexos técnicos que incluyan requisitos de ciberseguridad y ciberdefensa	2 ingenieros de requerimientos	Establecimiento de requisitos de intercambio de información con otras entidades	Implementar los componentes de la arquitectura institucional para el intercambio de información.
Mantener actualizados y vigentes los procesos y directrices a utilizar en el	12 meses	Fiscalía	Número de procedimientos y guías actualizadas.	2 ingenieros de requerimientos	Actualización de la documentación de los proyectos de desarrollo de aplicaciones	Alinear el proceso de desarrollo, implementación y uso de las aplicaciones

ciclo de vida de las aplicaciones web en la Fiscalía General de la Nación					web de la Entidad	web con el entorno de la entidad,
Diseñar e implementar ambientes de pruebas de seguridad de software y dotarlas de herramientas de pruebas en ciberseguridad.	12 meses	Fiscalía	Número de pruebas de las aplicaciones web en requisitos de ciberseguridad y ciberdefensa	2 ingenieros de requerimientos	Registro y análisis de las pruebas realizadas.	Implementar controles de calidad, ciberseguridad y ciberdefensas en la entidad.
Incluir cooperación con los organismos de defensa e investigación del estado.	12 meses	Fiscalía, entidades del estado	Número de convenios de cooperación en materia de ciberseguridad y ciberdefensa	2 ingenieros de requerimientos	Establecimiento lineamientos y buenas prácticas en materia de ciberseguridad y ciberdefensa.	Implementar aplicaciones web que soporten servicios en el ciberespacio que estén alineados con la política de seguridad digital del estado colombiano.

- **Adaptación al Entorno mediante el** aseguramiento de las aplicaciones web existentes:

Objetivo	Construir, implementar y utilizar aplicaciones web que cuenten con controles ante los riesgos de ciberseguridad y ciberdefensa de la Fiscalía General de la Nación.					
Alcance	Diseñar arquitecturas que permitan un aseguramiento del sistema de información en el ciberespacio, de acuerdo con los lineamientos establecidos en el direccionamiento estratégico de la entidad.					
Recursos:	Para este plan de acción se contará con la plataforma tecnológica adquirida y la plataforma de seguridad perimetral que se encuentra en funcionamiento, así como la correspondiente al SOC.					
Actividades	Tiempo	Lugar	Unidades	Recursos	Seguimiento	Logros

Asegurar la arquitectura existente de aplicaciones web.	12 meses	Fiscalía	Número de vulnerabilidades detectadas en las plataformas actualizadas y aseguradas	4 ingenieros de infraestructura	Resultados de los estudios de hacking ético realizado a las plataformas.	Fortalecer las plataformas de TIC que soportan el funcionamiento de las aplicaciones web en la Entidad.
Desarrollar planes de aseguramiento de las aplicaciones web.	12 meses	Fiscalía	Número de controles implementados en el DRP.	2 ingenieros de requerimientos	Ejecución de DRP y evaluación de los resultados.	Fortalecer las capacidades de recuperación del servicio en las infraestructuras críticas de la entidad que soportan el desarrollo, implementación y uso de las aplicaciones web..
Optimizar los modelos de uso de las aplicaciones web.	12 meses	Fiscalía,	Numero de actualización de policitas de uso de las aplicaciones web de la Entidad,	2 ingenieros de requerimientos	Establecimiento lineamientos uso adecuado de las aplicaciones web en el ciberespacio.	Crear cultura de usos adecuado de las aplicaciones web que soporten servicios en el ciberespacio.
Diseñar servicios horizontales para optimizar el uso de las aplicaciones web.	12 meses	Fiscalía,	Numero de requerimientos atendidos sin necesidad de crear nuevos aplicaciones web	2 ingenieros de requerimientos	Atención de los requisitos con las capacidades de la plataforma actual de la Entidad.	Optimización de recursos necesarios para desarrollar, mantener y utilizar servicios en el

						ciberespacio que estén alineados con la política de seguridad digital del estado colombiano.
Crear campañas de sensibilización en materia de ciberseguridad y ciberdefensa para los actores que intervienen en el desarrollo, implementación y uso de las aplicaciones web	12 meses	Fiscalía,	Numero de campañas de sensibilización en amenazas en ciberseguridad y ciberdefensa.	2 ingenieros de requerimientos	Determinar el nivel de cumplimiento de los planes de sensibilización formulados.	Crear una cultura de uso seguro de las aplicaciones web en el ciberespacio.
Desarrollo de ética en el ciberespacio proyectos de desarrollo de aplicaciones web.	12 meses	Fiscalía,	Actualización el código de ética de la entidad.	2 ingenieros de requerimientos	Medición del nivel de asimilación del código de ética en aspectos de ciberseguridad y ciberdefensa.	Crear una cultura de uso seguro de las aplicaciones web en el ciberespacio.
Desarrollo de capacidad de gestión integral de TI en el ciberespacio.	12 meses	Fiscalía,	Requerimientos de ciberseguridad y ciberdefensa en las fichas.	2 ingenieros de requerimientos	Determinar los requerimientos de ciberseguridad .	Incluir en la gestión de TI las características de ciberseguridad y ciberdefensa a monitorear en la plataforma de TI de la Entidad.

Adhesión entre la planeación y la gestión de TIC	12 meses	Fiscalía,	Numero de planes de TI con el desarrollo de aplicaciones web formulados.	2 ingenieros de requerimientos	Determinar el nivel de cumplimiento de los planes de desarrollo de las aplicaciones web con mecanismos de control de ciberseguridad y ciberdefensa.	Construir aplicaciones web que soporten los servicios en el ciberespacio acorde con los lineamientos estratégicos de la Entidad.

- **Generación de valor agregado** mediante el fortalecimiento de la infraestructura tecnológica de la Entidad en materia de ciberseguridad y ciberdefensa.

Objetivo	Construir una conciencia de ciberseguridad para el desarrollo, implementación y uso de las aplicaciones web en la Entidad.					
Alcance	Concientizar en las áreas que gestionan las plataformas tecnológicas necesarias pare el uso de las aplicaciones web y que soportan los servicios que la Entidad dispone en el ciberespacio.					
Recursos:	El grupo de desarrollo de la Subdirección de TIC.					
Actividades	Tiempo	Lugar	Unidades	Recursos	Seguimiento	Logros
Determinar políticas de protección de uso de aplicaciones web.	12 meses	Fiscalía,	Numero de actualizaciones de las políticas de uso	2 ingenieros de requerimientos	Establecer y definir las policitas de uso de las aplicaciones web en la entidad.	Crear una cultura de uso seguro de las aplicaciones web en el ciberespacio.
Determinar herramientas y componentes de seguridad externos para fortalecer las aplicaciones web.	12 meses	Fiscalía,	Numero de actualizaciones de la plataforma del SOC de acuerdo con los requisitos identificados en este componente.	2 ingenieros de requerimientos	Establecer necesidades y fichas técnicas de actualización de la plataforma del SOC.	Contar con una plataforma de seguridad actualizada y acorde con el entorno de la Entidad.

- **Generación de innovación** mediante el desarrollo de I+D+i en materia de seguridad de Aplicaciones web.

Objetivo	Desarrollar las capacidades de innovación en el desarrollo, implementación y uso de las aplicaciones web que funcionan en el ciberespacio.					
Alcance	Para el desarrollo de nuevas arquitecturas de software que permita el crecimiento horizontal en funcionalidad, es necesario desarrollar y actualizar el conocimiento de aplicación de los mecanismos de implementación de los diseños propuestos de acuerdo con las vulnerabilidades identificas en las plataformas utilizadas en el ciclo de vida del sistema de información en la Entidad.					
Recursos:	Equipo desarrollador.					
Actividades	Tiempo	Lugar	Unidades	Recursos	Seguimiento	Logros
Implementación de metodologías de desarrollo ágil.	12 meses	Fiscalía,	Reuniones de seguimiento diario	24 ingenieros de desarrollo	Establecer y definir las incidencias de desarrollo a ser solucionadas.	Crear una base de conocimiento para el desarrollo, implementación y uso seguro de las aplicaciones web en el ciberespacio.

6.8. Controles de implementación de lineamientos.

En los lineamientos estratégicos de ciberseguridad y ciberdefensa de la entidad, las condiciones de publicación de la información clasificada y reservada desde las aplicaciones web se debe:

- Identificar el dueño y responsable de la información susceptible de publicar, consultar o compartir en el ciberespacio.
- Identificar los requerimientos de seguridad en las aplicaciones web para la publicación, consulta e intercambio de información en el ciberespacio.
- Formular de componentes de arquitectura de las aplicaciones web para lograr la continuidad de negocio en el DRP de la Entidad.
- Utilizar de medios de transmisión segura y cifrada entre los diferentes componentes de la arquitectura del sistema de información.
- Monitorear desde el SOC de los servicios de información disponibles en el ciberespacio.

- Análisis del impacto de negocio – BIA. De acuerdo con la identificación de las necesidades de servicios de información en el ciberespacio, se debe tener en cuenta los siguientes criterios:

Tabla 18
Controles de implementación de lineamientos.

Requerimientos de continuidad	Nivel requerido (aporte del autor).
Tiempos de recuperación de los servicios de información en el ciberespacio – Recovery Time Objective - RTO.	3 Horas
Recursos Tecnológicos	Aplicaciones web misionales
Recursos Humanos	Administradores de servidores, desarrolladores, administradores de la plataforma de seguridad y comunicaciones.
Tiempo máximo de caída tolerable Maximum Tolerable Downtime – MTD	24 horas.
Niveles mínimos de recuperación de los servicios de información – Revised Operating Level – ROL	95 % de los usuarios de los servicios de información.
Identificación de dependencias y de proveedores involucrados en los servicios de información	Áreas de gestión de TIC, planeación y misionales.
Grado de dependencia de la actualidad de los datos – Recovery Point Objetive – RPO	Proceso misional.

Fuente: Aplicado por el autor basado en modelos de análisis BIA.

- Estrategia de continuidad. Fortalecer e implementar mecanismos que disminuyan los tiempos de recuperación en tiempo inferiores al MTD de 24 horas para contar con la disponibilidad de procesos críticos y mitigación de riesgos de los servicios de información en el ciberespacio.
- Formulación de plan de crisis o de incidentes de seguridad de servicios de información en el ciberespacio para establecer como condición de alarma la indisponibilidad de los servicios de registro y publicación de las aplicaciones web misional, así como los flujos de toma de decisiones, medios de contingencia para el registro de información de las denuncias para evitar la pérdida de información.
- En cuanto al personal responsable, se involucra principalmente el área de TIC y misionales, mediante procedimientos donde se indique los diferentes pasos, identificación de contactos y datos. Para la priorización se tiene como partida las aplicaciones web de registro de noticias criminales, para lo cual como requisitos temporales se debe contar con canales de transmisión y plataformas de hardware y

software necesarios. Para este propósito, se cuenta con los procedimientos internos de los subprocesos de las áreas de TIC y misionales.

- Formulación de plan operativo de recuperación de entornos. Se debe recuperar las plataformas de servidores, comunicaciones y seguridad perimetral.
- Formulación de procedimientos técnicos de trabajo o de gestión de incidentes de seguridad de servicios de información en el ciberespacio, de acuerdo con los procedimientos, guías e instructivos establecidos para la administración de la plataforma de TIC.
- Formulación de plan de pruebas y mantenimiento. Se debe validar la información de contacto, procedimientos, guías e instructivos vigentes para la recuperación de los componentes del sistema de información. De igual manera debe está establecido el alcance, procedimientos, escenarios y resultados de las pruebas. Para el caso de mantenimiento se debe cumplir con los protocolos de acceso a áreas restringidas del ciberespacio.
- Formulación de plan de concienciación. Se debe diseñar y ejecutar pruebas del plan de contingencia con el apoyo de los recursos identificados que incluya el BIA y los planes formulados para el personal de TIC, planeación y misionales.

Una visión estratégica global para la ciberseguridad. Tomando como base la política de seguridad digital del estado colombiano, la Fiscalía General de la Nación debe cumplir un rol de responsable y parte interesada en la prestación de servicios de información de interés a los usuarios del ciberespacio para mitigar los riesgos del estado en lo que le compete como actor en la prestación del servicio de justicia, que de acuerdo con lineamientos establecidos por la arquitectura empresarial de la Entidad se contribuye a mantener la gobernabilidad de plataformas de TIC y servicios en el ciberespacio colombiano, el cumplimiento de los marcos legales y regulatorios, la implementación de un sistema de gestión de riesgos de seguridad digital nacional, crear y fortalecer una cultura de seguridad digital nacional en la ciudadanía y desarrollar capacidades que le competen a la Fiscalía General de la Nación.

Lo anterior para lograr la interacción para el logro de garantías en el buen uso de internet, generar y monitorear el cumplimiento de recomendaciones, formular y ejecutar

acciones preventivas o correctivas frente a ataques en el ciberespacio colombiano, detectar y reportar incidentes de ciberseguridad y ciberdefensa.

7. CAPITULO V. DISEÑO DE LA ARQUITECTURA DE CIBERSEGURIDAD DE LAS APLICACIONES WEB.

Para la definición de la arquitectura de aplicaciones web se debe incluirse en los componentes de la arquitectura:

Tabla 19
Criterios de diseño de arquitectura

Parámetro de diseño	Descripción (aplicado por el autor)
Modularidad y reutilización de código	Cada uno de los componentes debe ser cohesión débil para permitir la implementación de la evolución tecnológica y lograr la independencia de desarrollo o adquisición de software.
Estandarización de la construcción de código	Determinar una visión de la evolución tecnológica de la entidad para satisfacer las necesidades de automatización de manera segura y con criterios de calidad.
Interconexión de los diferentes componentes	La interconexión de los diferentes objetos de la arquitectura de software sino el intercambio de información.
Integración de los objetos de la arquitectura	deben ser diseñados para soportar la disponibilidad de las aplicaciones web y nuevos procesos de la Entidad.
Capas de la arquitectura, bloque de construcción (ABB),	Se deben definir requerimientos de seguridad de software y permitir la implementación de metodologías de desarrollo rápido. Debe incluirse componentes orientadas a la seguridad de la arquitectura de software
Riesgos del desarrollo de software	A partir de la definición de criterios de desarrollo de software se identifican las desviaciones de la arquitectura del sistema de información.
Arquitectura orientada a servicios.	Establecer criterios, directrices, principios orientados a servicios, para incluir componentes externos en la arquitectura de software.
Estándares de encripción avanzada (AES).	Se deben implementar las características de cifriamiento para la comunicación de los artefactos de la arquitectura del sistema de información.

Categorización de seguridad de información	Con la implementación del SOC se realiza la categorización de los diferentes incidentes de seguridad a los que se ve enfrentado el sistema de información.
Requerimientos de seguridad.	En la definición de los requisitos del sistema de información se identifican aquellos que deben minimizar las vulnerabilidades del sistema de información en el ciberespacio.
Plan de seguridad para aplicaciones web.	Con el diseño, implementación y uso de las aplicaciones web se establecen dentro de las metodologías de desarrollo las actividades necesarias para la implementación correspondiente.
Riesgos de información de aplicaciones web.	SP 800-30: Guía para la conducción de la valoración de riesgos de información federal y aplicaciones web.
Infraestructura de PKI.	SP 800-32: Introducción para la infraestructura de PKI federal y de tecnología de llave pública.
Planes de contingencia.	SP 800-34: Guía para planes de contingencia para información federal y aplicaciones web.
Marco de gestión de riesgos para aplicaciones web.	SP 800-37: Guía para la aplicación de un marco de gestión de riesgos para sistemas.
Riesgos de seguridad de información.	SP 800-39: Gestión de riesgos de seguridad de información.
Gestión de llaves criptográficas.	SP 800-52: Un perfil para los sistemas federales de U.S. de gestión de llaves criptográficas.
Seguridad y controles de privacidad.	SP 800-53: Seguridad y controles de privacidad para sistemas y organizaciones.
Valoración de seguridad y controles.	SP 800-53A: Valoración de seguridad y controles de privacidad en sistemas y organizaciones.
Gestión de llaves en aplicaciones.	SP 800-57 Parte 3: Recomendaciones para la gestión de llaves, parte 3 – Guía para la gestión de llaves especificas en aplicaciones.
Tipos de relaciones de información y aplicaciones web.	SP 800-60: Guía para tipos de relaciones de información y aplicaciones web para categorías de seguridad.
Manejo de incidentes de seguridad.	SP800-61: Guía para el manejo de incidentes de seguridad de computadores.
Seguridad de los sistemas de control industrial (ICS).	SP 800-82: Guía para la seguridad de los sistemas de control industrial (ICS).
Seguridad de servicios web.	SP 800-95: Guía para la seguridad de servicios web.
Protección de confidencialidad.	SP 800-122: Guía para la protección de confidencialidad para la información del personal identificable (PII).
Gestión de la configuración de las aplicaciones web.	SP 800-128: Guía para seguridad enfocada en la gestión de la configuración de las aplicaciones web.

Monitoreo continuo de seguridad.	SP 800-137: Monitoreo continuo de seguridad de la información para aplicaciones web y organización.
Perfil para sistemas de gestión de llaves criptográficas.	SP800-152: Un perfil para sistemas de gestión de llaves criptográficas federales en USA.
Ingeniería para la seguridad en sistemas.	SP 800-160: Ingeniería para la seguridad en sistemas, consideraciones en una aproximación multidisciplinaria en la ingeniería.
Acceso basado en atributos (ABAC).	SP800-162: Guía para la definición y consideraciones para el acceso basado en atributos (ABAC).
Gestión de riesgos en cadenas de suministros.	SP 800-161: Prácticas de gestión de riesgos en cadenas de suministros.
Estándares de criptografía.	SP 800-175A: Guía para el uso de estándares de criptografía en cuanto a directivas, mandatos y políticas.
Uso de estándares.	Para el uso de estándares en la implementación de aplicaciones web se tienen en cuenta: Criptografía. ISO/31000: gestión de riesgos ISO/22300: Gestión de la continuidad. ISO/15408. CNSS Microsoft SDL Quick security Rereference PCI DSS HIPAA CWE/SANS Top 25 Sarbanes - Oxley ISO/IEC 9126
Políticas de seguridad de la información	A.5. Políticas de seguridad de la información
Organización de la seguridad de la información.	A.6.Organización de la seguridad de la información.
Seguridad en los recursos humanos.	A.7. Seguridad en los recursos humanos.
Gestión de activos.	A.8. Gestión de activos.
Control de acceso.	A.9. Control de acceso.
Criptografía.	A.10. Criptografía.
Seguridad física y ambiental.	A.11. Seguridad física y ambiental.
Seguridad de las operaciones.	A-12. Seguridad de las operaciones.
Seguridad de las comunicaciones.	A.13. Seguridad de las comunicaciones.
Adquisición, desarrollo, mantenimiento de sistemas.	A.14. Adquisición, desarrollo, mantenimiento de sistemas.
Relaciones con proveedores.	A.15. Relaciones con proveedores.

Gestión de incidentes de seguridad de la información.	A.16. Gestión de incidentes de seguridad de la información.
Aspectos de seguridad de la información dentro de la continuidad del negocio	A.17.Aspectos de seguridad de la información dentro de la continuidad del negocio
Conformidad.	A.18. Conformidad.

Fuente: planteamiento basado en cervantes y Velazco (Cervantes, 2016)

En este sentido, a partir del planteamiento de cervantes y Velazco (Cervantes, 2016) en cuanto al ciclo de desarrollo se plantea de la siguiente manera:

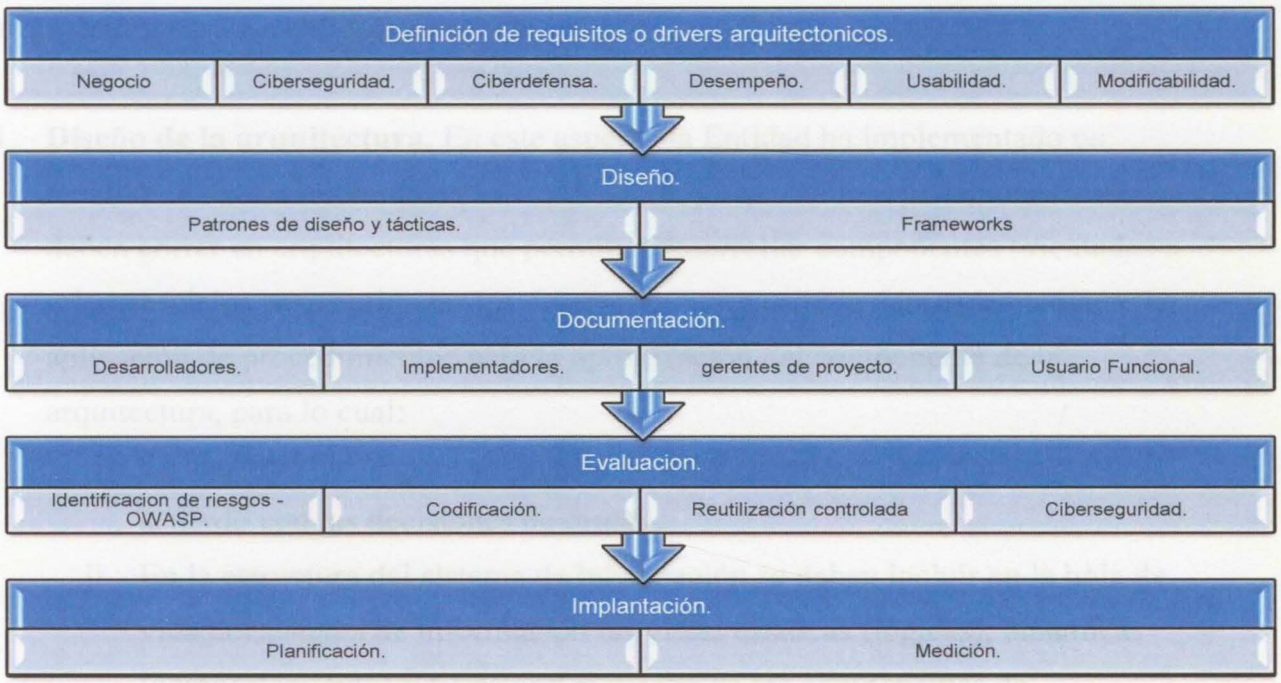

Grafico 16 Arquitectura de Software FISCALÍA GENERAL DE LA NACIÓN (aporte del autor).

Una vez definidos los objetivos del negocio e identificar la necesidad del usuario final (Wiegers, 2013), se debe establecer los siguientes procedimientos y guías dentro de la formulación de la estrategia:

1. Procedimiento de la definición de los requisitos o drivers arquitectónicos. Ver anexo No 1.
2. Instructivo para el Diseño de la arquitectura del sistema de información. Ver anexo No 3.
3. Documentación de la arquitectura del sistema de información. Ver anexo No 4.

4. Instructivo para la evaluación de la arquitectura del sistema de información. Ver anexo No 5.
5. Instructivo para la implementación de la arquitectura del sistema de información. Ver anexo No 6.
6. Instructivo para el diseño de pruebas del software. Ver anexo No 7.

En cuanto al diseño de la arquitectura (Cervantes, 2016) se propone la siguiente arquitectura para las aplicaciones web:

1. **Diseño de la arquitectura.** En este aspecto la Entidad ha implementado un método de diseño centrado en la arquitectura, ya que en las aplicaciones web deben correr en arquitecturas que permitan desarrollar componentes orientados a microservicios para optimizar los desarrollos y soportar la demanda mediante la aplicación de procedimientos para la optimización del componente de la arquitectura, para lo cual:
    i. Se declaran las responsabilidades de los elementos y las relaciones de acuerdo con las decisiones de diseño.
    ii. En la estructura del sistema de información se deben incluir en la hoja de vida del sistema de información las vistas estáticas (lógicas), dinámicas (comportamiento) y física con el detalle de los componentes de ciberseguridad y ciberdefensa implementados en la solución.
    iii. Definir el catálogo de elementos, en donde se detalle las condiciones de funcionamiento, propiedades y resultados.

    De lo anterior se destacan los siguientes componentes de la arquitectura:

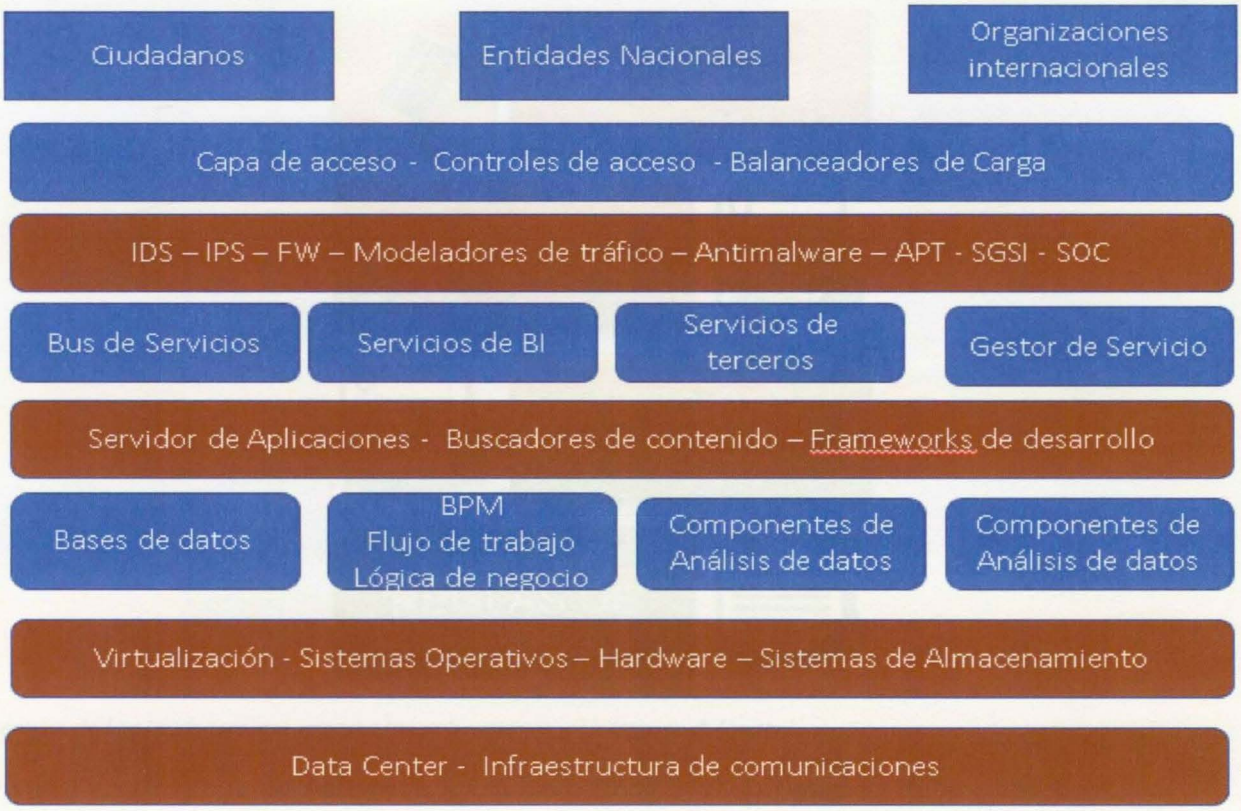

Grafico 17 Arquitectura de la plataforma que soporta las aplicaciones web (aporte del autor).

2. **Diseño de las interfaces.** Con el diseño de las interfaces con los diferentes componentes de la arquitectura se debe incluir componentes de inteligencia, (Óscar Fernando, 2007), como es el caso de Watson de IBM, que no solo permite descubrir patrones en la información no estructurada sino componentes de inteligencia a la arquitectura en cuanto a intercambio de información o inclusive en la misma captura de información del sistema.
3. **Diseño detallado de los módulos.** En el momento de la segmentación funcional de un sistema de información se establece como lenguaje de comunicación entre los diferentes artefactos para otras fases del proyecto.

4. **Diseño del Software.** En cuanto a la arquitectura de software, se propone la siguiente:

Grafico 18 Arquitectura de la plataforma que soporta las aplicaciones web (aporte del autor)

Diseño de pruebas de software. Para las pruebas del software se debe establecer el conjunto de entradas que debe procesar el sistema de información y la definición de los casos de prueba.

7.5. Arquitectura de ciberdefensa de las aplicaciones web.

Para la defensa de las aplicaciones web se propone la siguiente arquitectura:

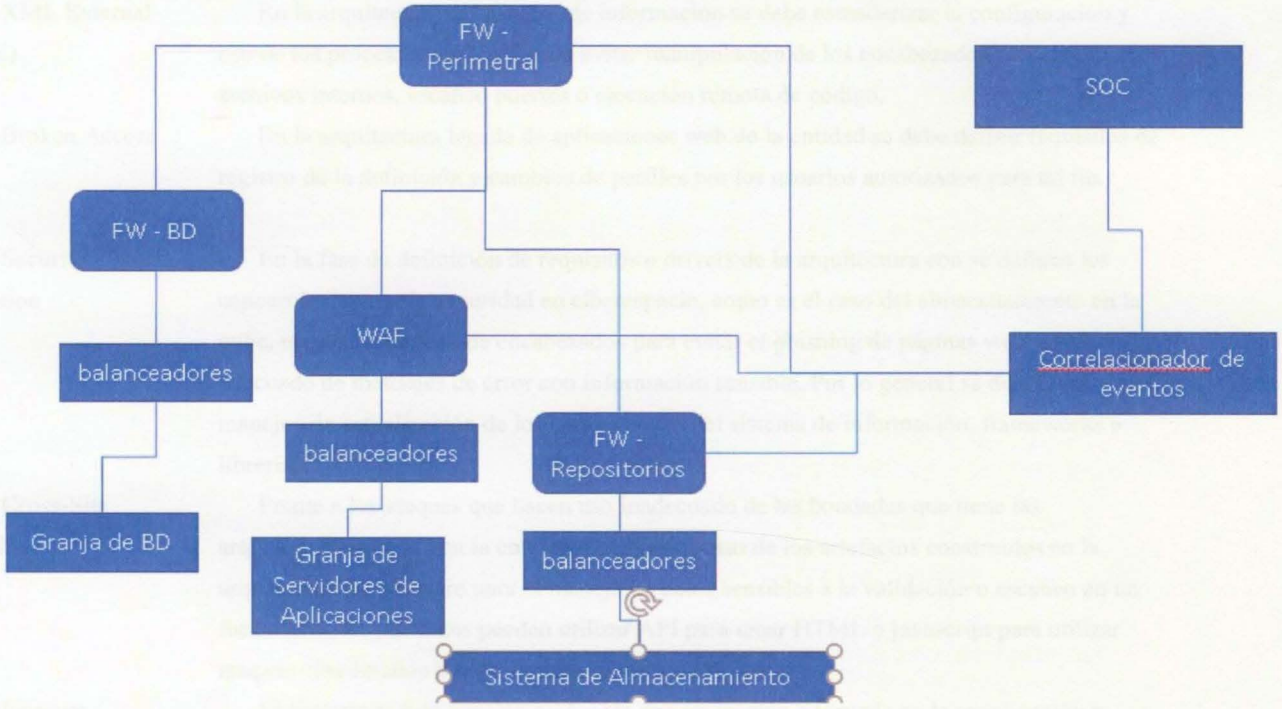

Grafico 19 Arquitectura de ciberdefensa. (aporte del autor)

Con esta estructura se permite implementar los siguientes controles que minimizan los riesgos identificados en basa en OWASP (OWASP-2017, 2017) de la siguiente manera:

Tabla 20
Controles en la arquitectura

Código	Descripción del control en la arquitectura
A1:2017-Injection	Con la modularización de los artefactos de la arquitectura de software del sistema de información, permite ocultar los componentes de consulta SLQ a las capas de persistencia y adicionalmente se debe cifrar estos componentes para que el atacante no pueda identificar las estructuras de datos utilizadas en la arquitectura.
A2:2017-Broken Authentication	Se debe desarrollar capas web para las aplicaciones web de 4GL, con los componentes adecuados para la gestión de la autenticación con la utilización de token para mantener el control durante la sesión y el flujo de transmisión de claves, llaves para la autenticación temporal o permanente.
A3:2017-Sensitive Data Exposure	Se debe definir requisitos de ciberseguridad y ciberdefensa para que en el sistema de información se desarrolle e implemente interfaces web con protecciones y monitoreo ante las modificaciones no autorizadas de los datos por lo que representa una vulnerabilidad a tener en cuenta en las nuevas arquitecturas de las aplicaciones web.

A4:2017-XML External Entities (XXE)	En la arquitectura del sistema de información se debe estandarizar la configuración y uso de los procesadores XML para evitar manipulación de los encabezados o el acceso a archivos internos, escaneo puertos o ejecución remota de código.
A5:2017-Broken Access Control	En la arquitectura legada de aplicaciones web de la entidad se debe definir requisitos de registro de la definición y cambios de perfiles por los usuarios autorizados para tal fin.
A6:2017-Security Misconfiguration	En la fase de definición de requisitos o drivers de la arquitectura con se definen los concernientes con la seguridad en ciberespacio, como es el caso del almacenamiento en la nube, manejo adecuado de encabezados para evitar el phishing de páginas web, manejo adecuado de mensajes de error con información sensible. Por lo general se deja estos manejos de actualización de los componentes del sistema de información, frameworks o librerias,
A7:2017-Cross-Site Scripting (XSS)	Frente a los ataques que hacen uso inadecuado de las bondades que tiene las arquitecturas que utiliza la entidad, como es el caso de los artefactos construidos en la arquitectura de software para el manejo de datos sensibles a la validación o escaneo en un formulario, los atacantes pueden utilizar API para crear HTML o javascript para utilizar ataques coordinados o redireccionar a sitios maliciosos.
A8:2017-Insecure Deserialization	El sistema de información no cuenta una protección adecuada en la serialización y deserialización de las tramas enviadas, con lo expone particularmente al sistema de información a la ejecución remota no autorizada de código para lograr inyección de código o escalamiento de privilegios.
A9:2017-Using Components with Known Vulnerabilities	Se debe establecer procedimientos y campañas de sensibilización el análisis de los componentes, librerías y frameworks en aspectos de ciberseguridad y ciberdefensa para ser utilizados en el desarrollo.
A10:2017-Insufficient Logging&Monitoring	Se debe especificar requisitos de auditoria y monitoreo de parámetros de calidad y desempeño para ser resueltos en el diseño de la arquitectura del sistema de información.

Fuente: Aplicado a partir de OWASP (OWASP-2017, 2017)

7.6. Manejadores arquitectónicos de seguridad en el ciclo de vida de las aplicaciones web.

Para el desarrollo de directrices en el ciclo de vida de las aplicaciones web se debe establecer roles específicos y capacidades para la evaluación y fortalecimientos de las aplicaciones web, como es el caso de la implementación de metodologías y herramientas de prueba para producir informes de aseguramiento y planes de fortalecimiento del proceso de desarrollo de las aplicaciones web.

7.6.1. Definición de requisitos.

Una vez viabilizado el conjunto de requisitos a atender, se debe tener en cuenta la siguiente estructura:

Tabla 21
Definición de requisitos de desarrollo de aplicaciones Web

Variable	Característica
Logro de los objetivos institucionales	Declaración de los requisitos se debe establecer los riesgos asociados de la implementación del sistema de información en el ciberespacio.
Tipificación del tipo de requisito.	Se debe establecer el tipo de requisito como funcional, técnico, de negocio, de calidad, de intercambio de información, de seguridad, de restricción o normativos, así como la calificación de priorización para tener en cuenta en el diseño e implementación correspondiente.
Identificación de desviaciones de la arquitectura	A partir del análisis de las historias de usuario se deben identificar y prever posibles desviaciones que puede tener la arquitectura del sistema de información.
Requisitos de usuario y funcionales.	Debe especificar los requisitos funcionales que requiere el usuario del sistema de información que según (Cervantes, 2016), corresponden a primarios o fundamentales y secundarios o de soporte. En cuanto a la funcionalidad se debe establecer los criterios de descomposición funcional de los componentes del sistema de información a partir de la relevancia, complejidad y priorización.
Requisitos de negocio.	Debe especificar los requisitos establecidos por la arquitectura institucional en lo referente a los procesos misionales, de apoyo y de control de la Entidad.
Requisitos de calidad.	Se establece los requisitos con respecto a la funcionalidad del sistema de información, su seguridad e interoperabilidad, usabilidad, desempeño, facilidad de mantenimiento y movilidad. Para esto se debe contar con criterios de priorización frente al logro de los objetivos estratégicos de la Entidad.
Requisitos de intercambio de información.	Se debe prever el intercambio de información con otros aplicaciones web tanto internos como externo a través del bus de servicio institucional.
Restricciones.	Se deben establecer las restricciones de índole técnico y administrativo para tener en cuenta en el diseño del sistema de información. El mas relevante es la relación que existe con el cumplimiento de los objetivos estratégicos de la Entidad.

Fuente: Aplicado a partir (42010, 2018)

7.6.2. Diseño de arquitectura.

Tabla 22
Criterios de diseño de arquitectura.

Variable	Característica
Información de los requisitos.	Define los criterios de diseño de la arquitectura del sistema de información como la asignación de funcionalidad a uno o varios componentes de la arquitectura.
Calidad.	El sistema de información debe construirse en esquemas de replicación y en crecimiento horizontal en el marco de la optimización de recursos necesarios para el diseño, implementación y uso del sistema de información, que permitan la disponibilidad, modularidad, cohesión,

	acoplamiento, patrones, tácticas, frameworks. Componentes a integrar en la arquitectura.
Tipo de usuarios.	De acuerdo a la visión y alcance del sistema de información se debe viabilizar el diseño a desarrollar en el sistema de información.
Socialización del diseño.	Se debe describir el contexto de funcionamiento del sistema de información, sus objetivos, las expectativas de calidad que debe tener, así como las restricciones de arquitectura detectadas.
Componentes arquitectónicos.	Se debe describir la estructura y funcionalidad de los componentes de la arquitectura del sistema de información, en cuanto a: diseño, interfaces y módulos.
Construcción y selección de escenarios.	Para la selección de los escenarios de requisitos a implementar que debe tener el sistema de información en el ciberespacio en cuanto a: funcionalidad, usabilidad, confiabilidad, desempeño, soporte, calidad y seguridad,
Diseño de interfaces.	Se deben construir con la ayuda de diagramas de secuencia, manejo de excepciones.

Fuente: Aplicado a partir (42010, 2018)

7.6.3. Documentación de la arquitectura.

Tabla 23
Documentación de la arquitectura.

Variable	Característica
Documentación de la arquitectura del software.	Conocimiento compartido, se debe preservar el conocimiento corporativo y establecer una base de conocimiento para la construcción y mantenimiento del sistema de información en la Entidad.
Guía de desarrollo.	Establecer los parámetros de diseño e implementación del sistema de información en cuanto a los alcances de las aplicaciones web, histórico de requisitos, diseños viabilizados, resultados y requisitos en la implementación, realización de pruebas, resultado de las implementaciones realizadas y requisitos de mantenimiento del sistema de información.
Homogeneidad de las estructuras,	La documentación permite contar con vistas lógicas, de comportamiento y físicas del sistema de información con lo que se logra la estandarización e integración de las aplicaciones web en la entidad.

Fuente: Aplicado a partir (42010, 2018)

7.6.4. Evaluación de la arquitectura.

Tabla 24
Evaluación de la Arquitectura

Variable	Característica
Fallas de la arquitectura.	Documentación de fallas de funcionamiento del sistema de información para la evaluación de costos y gestión del cambio asociado.
Errores en la funcionalidad del sistema de información.	Como parámetro de calidad del código es necesario registrar las incidencias en el desarrollo para evaluar la fortaleza de la arquitectura del sistema de información.

Desviaciones en la arquitectura del sistema de información.	Artefactos de la arquitectura, se debe evaluar los artefactos para detectar de manera tempana los requisitos de cambio de la arquitectura para satisfacer los requisitos mal formulados en cuanto falta de completitud o definiciones equivocadas.
Calidad del sistema de información.	La arquitectura del diseño del software, su implementación, pruebas y evaluación de las arquitecturas debe ser medible mediante parámetros de calidad y logro de los objetivos del sistema de información. Esto se efectúa mediante la revisión a partir de muestras o la revisión completa del sistema de información.
Talento humano.	Debe se medible en cuanto a la asignación de recursos y tiempo destinado para el diseño e implementación del sistema de información.

Fuente: Aplicado a partir (42010, 2018)

7.6.5. Implementación de la arquitectura.

Continuando con el proceso de desarrollo se aborda la fase de implementación se debe tener en cuenta las siguientes directrices, la cual exige contar con una estrategia de implementación basada en los lineamientos establecidos por cervantes, (Cervantes, 2016).:

Tabla 25
Criterios de implementación de la arquitectura.

Variable	Característica
Validación de la estructura general del sistema de información.	A partir de la arquitectura diseñada y la documentación establecida, se debe identificar y analizar tanto las estructuras como los componentes por cada uno de los módulos que conforman el sistema de información, Esto es definir o seleccionar las tecnologías a utilizar para el diseño de la arquitectura del sistema de información. En este proceso, es necesario identificar y documentar las diferentes vulnerabilidades que conlleva el diseño, implementación y uso del sistema de información.
Validación de los módulos del sistema de información	Se debe analizar la relación entre los módulos del sistema de información a partir de la arquitectura y los requisitos formulados.
Diseño de la aplicación.	Se debe diseñar la arquitectura del software para el desarrollo o adquisición de los módulos del sistema de información y atender los requisitos formulados. En este lineamiento se debe ejecutar las siguientes actividades: Implementación en la plataforma de desarrollo los diferentes componentes de la arquitectura. Diseñar los módulos acordes con la estructura del sistema de información. Asignación de recursos para desarrollo o ajustes en la aplicación.
Desarrollo o adquisición de la aplicación.	Se debe realizar las siguientes actividades: Adquirir el código existente para ser adecuado de acuerdo con la arquitectura definida. Desarrollo o ajustes del código. Integración de los componentes y módulos desarrollados. Ajustes del código.
Gestión de desviaciones en la implementación.	Para el aseguramiento del sistema de información es necesario tener registro, viabilidad y control de cambios en cuanto a: Valoración del cambio en la arquitectura. Gestión del riesgo de la viabilidad del cambio en la arquitectura.

Comprobación de código.	Rediseño de la arquitectura del sistema de información. Corrección de fallos o errores en el sistema de información. Cambios en la arquitectura por la falta de atención de requisitos o la ausencia de elementos necesarios para el funcionamiento del sistema de información. Para cada uno de los módulos funcionales se debe diseñar el plan de pruebas correspondiente, el cual debe incluir los diferentes requisitos formulados. Para este efecto se debe utilizar una herramienta para la gestión de los incidentes encontrados en las pruebas y de las soluciones aplicadas. En cuanto a las desviaciones de la arquitectura y en la codificación se debe verificar el diseño de los módulos y la calidad del código.

Fuente: Aplicado a partir (42010, 2018)

Para lograr la capacidad de desarrollo acorde con el entorno digital frente a las necesidades de información relacionada con los servicios de investigación y judicialización se debe implementar controles de seguridad de la información para el proceso de desarrollo ágil al que se ha visto obligada la entidad a implementar para atender los cambios funcionales que se presentan en la construcción del sistema de información que para el caso de la Entidad se identifica como SCRUM.

Por lo anterior, para la formulación de la estrategia para el desarrollo, implementación y uso de las aplicaciones web al interior de la entidad, se formula el ciclo de vida de un sistema de información basada en el planteamiento de métodos de desarrollo ágil, como es el caso de SCRUM dada las condiciones de desarrollo con equipos de desarrolladores de la Entidad asignados al apoyo durante todo el ciclo de vida de la aplicación producto de las iteraciones de corta duración.

8. CONCLUSIONES.

1. Con el análisis de los riegos de publicar servicios de información en el ciberespacio identificados en la investigación, se logró formular siete (7) lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web en la Entidad de la siguiente manera:

- Implementar un modelo de seguridad y privacidad de la información en el proceso de desarrollo de aplicaciones web de la Fiscalía General de la Nación a partir de las recomendaciones dadas en OWASP y la ISO/IEC 27001.
- Diseñar e implementar controles de seguridad para el proceso de construcción de aplicaciones web que soporten los servicios de información en el ciberespacio.
- Identificar los datos como activos de información de la entidad disponibles en el ciberespacio para establecer los controles a implementar.
- Selección de plataformas y arquitecturas de software unificadas
- Fortalecimiento del proceso de selección de Talento Humano y proveedores especializado en desarrollo de software y seguridad
- Generación de conocimiento especializado para el desarrollo de aplicaciones web
- Arquitectura de software integrada con una Arquitectura de Seguridad.

2. En esta investigación se establecieron criterios seis (6) criterios para el desarrollo seguro de aplicaciones web para ser utilizados por el equipo de desarrollo de la FGN, los cuales son:

- La definición de los requisitos de seguridad de los servicios de información en el ciberespacio en la entidad debe ser realizados a partir de las funciones establecidas por la ley orgánica No 16 de 2014 y la ley 898 de 2017, que rige la gestión de la Fiscalía General de la Nación.
- La identificación de los requisitos de seguridad de los servicios de información en el ciberespacio en la entidad debe realizarse en coherencia con las funciones establecidas por la implementación de la arquitectura empresarial de la entidad establecida en la resolución 1165 de 2018.
- Para la formulación y estandarización de los procesos de gestión de usuarios y accesos a los servicios de información en el ciberespacio se debe dar cumplimiento a las leyes de protección de datos y ley de transparencia del estado.
- En la identificación de los requerimientos de intercambio de información en el medio digital y en papel se debe realizar en la entidad como miembro de la policía judicial del estado colombiano.

- En la gestión documental producto de la implementación del sistema integral de gestión de la entidad se debe incluir el cumplimiento de la política de seguridad de la Entidad.
- La aplicación de los lineamientos estratégicos dados por cada administración en cabeza del fiscal general de la nación debe enfocarse en superar las fallas en la arquitectura, errores en la funcionalidad del sistema de información y calidad de las aplicaciones web.

3. Como resultado de la investigación, los criterios existentes en la FGN para el manejo de vulnerabilidades de las aplicaciones Web para la publicación de información en el ciberespacio se basan en la Arquitectura Empresarial del estado colombiano, que corresponde a los formulados para ser implementados en las Entidades del Sector Público Colombiano basados en los lineamientos del ministerio de las TIC, definidos de la siguiente manera:
   - Los establecidos en el artículo 209 de la constitución.
   - Artículo 3 de la ley 489 de 1998.
   - Ley 1437 de 2011.
   - Decreto 2693 de 2012.
   - Plan estratégico. (Nación F. G., Plan estratégico 2016-2020, 2018)
   - Objetivos estratégicos (Nación F. G., Plan estratégico 2016-2020, 2018).
   - Información que genera la Entidad a todos los niveles organizacionales.
   - Políticas de seguridad de la información.
4. Con el proceso de investigación se identificó la relación entre los lineamientos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio de la siguiente manera:
   - Se identifica la necesidad de relacionar los lineamientos estratégicos que integre las actividades de ciclo de vida del software definidas en la Fiscalía con la gestión de riesgos de ciberseguridad.
   - Se debe fortalecer la definición de requisitos de seguridad de la información y la correlación con la aplicación de los mecanismos de protección tanto de la información como de los activos asociados.

- En la relación no se incluye los mecanismos de control para evitar transmisión de información incompleta o de la modificación de información o de enrutamiento errado o de la alteración de mensajes entre los componentes de las aplicaciones web y la reproducción o copia de mensajes no autorizados con las vulnerabilidades a tratar en el proceso de disponer activos de información de la entidad en el ciberespacio.
- Existe la necesidad de control en la puesta en producción de la aplicación web y la detección de vulnerabilidades en su estabilización.
- Existe una dependencia de la identificación de vulnerabilidades a controlar con la protección de los ambientes de desarrollo, pruebas, preproducción y producción.
- La definición de los roles y acceso de los actores internos y externos en el proceso de construcción de las aplicaciones web de la entidad, con el papel que cumplen el ciclo de vida de la aplicación web.
- En la construcción de aplicaciones web deben incluir aspectos de operación de la plataforma crítica y en los procesos de continuidad de negocio.
- Los requerimientos de ciberseguridad que se deben atender en la arquitectura de las aplicaciones web de la entidad corresponden a la interacción con los requerimientos funcionales de las aplicaciones web analizados.
- Los servicios publicados en el ciberespacio, existe estrecha relación con los lineamientos establecidos en el índice de clasificación de información pública declarada por la entidad en su página web (Nación F. G., Declaración de índice de información clasificada y reservada, 2018)
- Se requiere en la entidad, dar cumplimiento con la arquitectura empresarial del estado colombiano (TIC M. d., Diseño y Especificación del Marco de Referencia. Diseño Detallado. Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información (TI), a Adoptar en las Entidades del Sector Público Colombiano., 2014), con los lineamientos dados por el ministerio de las TIC.

- Las aplicaciones web tienen estrecha relación con las bondades y limitaciones de la infraestructura critica, tanto así que su diseño interno obedece al lineamiento de:
- La atención de los requisitos funcionales de las aplicaciones web deben incluir el control de la atención de los requisitos de seguridad y las metodologías de desarrollo SCRUM para el diseño de aplicaciones web.

5. En el estudio se identifican los lineamientos para el análisis de contexto para la formulación de una estrategia de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio se plasman en el capítulo IV, numeral 4.1. se determina l.

6. En el desarrollo de la investigación se define como alternativa de la formulación de los lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web y de la gestión de riesgos de seguridad de la información publicada en el Ciberespacio, la implementación de la norma ISO 27001, específicamente en dominio No 10 para establecer los planes de implementación de los lineamientos estratégicos y complementado con la implementación del marco de referencia OWASP.

7. En el presente estudio se formulan los objetivos de los lineamientos estratégicos de ciberseguridad y ciberdefensa para el desarrollo seguro de aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio se centra en:

- Generar valor agregado con el desarrollo de las aplicaciones web de la entidad.
- Flexibilizar y adaptar los desarrollos de aplicaciones web al Entorno.
- Apoyar la efectividad de los servicios de justicia.
- Generar conocimiento e innovación en el proceso de construcción y mantenimiento de aplicaciones web.
- Crear cultura de ciberseguridad en el proceso de construcción de aplicaciones Web.
- Formular proyectos de desarrollo de aplicaciones Web enmarcadas en una gestión integral de TI.

- Coordinar con el área de planeación la gestión de TIC en cuanto a la priorización de desarrollos de funcionalidad de las aplicaciones web de la entidad.
- Asegurar el ciclo de vida de las aplicaciones web de la Fiscalía General de Nación. Proponer el plan de implementación de los lineamientos para la formulación de una estrategia de ciberseguridad y ciberdefensa para el desarrollo seguro e aplicaciones Web y la gestión de riesgos de seguridad de la información publicada en el Ciberespacio.

9. RECOMENDACIONES.

1. Incluir requerimientos de seguridad en las fases tempranas de desarrollo de las aplicaciones web.
2. Mantener un proceso continuo de valoración de riesgos en el ciclo de vida de las aplicaciones web de la Entidad.
3. Implementar una arquitectura de seguridad de las aplicaciones web de la entidad.
1. Identificar las amenazas y riesgos del desarrollo o adquisición, implementación y uso de las aplicaciones web en la Fiscalía General de la Nación.
2. Formular una estrategia de ciberseguridad y ciberdefensa para la gestión de Aplicaciones web en la Fiscalía General de la Nación.
3. Contar con una arquitectura de aplicaciones web que permita ofrecer servicios en el ciberespacio con los siguientes elementos:
    - Modularidad y reutilización de código.
    - Estandarización de la construcción de código.
    - Interconexión de los diferentes componentes.
    - Disponibilidad e integración de los objetos de la arquitectura.
    - En la arquitectura debe incluirse componentes orientadas a la seguridad de la arquitectura de software.
    - Disminuir los riesgos del desarrollo de software de manera temprana.
    - Establecer criterios, directrices, principios orientados a servicios, para incluir componentes externos en la arquitectura de software.

Referencias Bibliográficas.

(ITU), I. T. (2018). *guide to developing a national cybersecurity strategy.* Obtenido de strategic engagement in cybersecurity: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

42010, I. (31 de julio de 2018). *Defining architecture.* Obtenido de http://www.iso-architecture.org/42010/defining-architecture.html

Acosta, h. F. (2018). *Observatorio Tecnológico para el Desarrollo de Aplicaciones Web* . Obtenido de https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/20368/1/tg-andrade-martinez.pdf

Ballesteros, Á. (2016). *En busca de una Estrategia de Seguridad Nacional.* Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-62762013000200007

Batista-Canino, R. B.-C.-B. (2016). *Monitorización del proceso emprendedor a través del modelo de negocio.* Obtenido de Innovar, 26(61), 83-102.: https://www.researchgate.net/publication/305043225_Monitorizacion_del_proceso_emprendedor_a_traves_del_modelo_de_negocio

Bautista Peñaquishpe, A. C. (2019). *SISTEMAS COMPUTACIONALES Y ARQUITECTURAS TECNOLÓGICAS.* Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/9355/2/04%20ISC%20517%20TRABAJO%20GRADO.pdf

Bautista Peñaquishpe, A. C. (2019). *SISTEMAS COMPUTACIONALES;ARQUITECTURAS TECNOLÓGICAS;APPSHELL;RESPONSIVE DESIGN;SOA;WEB PROGRESIVA;GESTIÓN DE PEDIDOS;LOCALES MIPYMES;CAFÉ-RESTAURANT;OTAVALO.*

BID. (14 de 3 de 2016). *BID y OEA instan a América Latina y Caribe a mayores esfuerzos en ciberseguridad.* Obtenido de https://www.iadb.org/es/noticias/comunicados-de-prensa/2016-03-14/informe-sobre-ciberseguridad-en-america-latina%2C11420.html

Carlos Ortiz de Zevallos, X. M. (2016). *Mejores prácticas en la Implantación de ISO27001:2013 y PCI/DSS 3.1.* . Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/53507/9/cortizdTFC0616memoria.pdf

Cervantes, H. (enero de 2016). *Arquitectura de Software: Conceptos y Ciclo de Desarrollo.* Obtenido de https://www.researchgate.net/publication/291970001_Arquitectura_de_Software_Conceptos_y_Ciclo_de_Desarrollo

Chandra, P. (2009). *Software Assurance Maturity Model Una guía para integrar seguridad en el desarrollo de software Versión - 1.0.* . Obtenido de https://opensamm.org/downloads/SAMM-1.0-es_MX.pdf

Ciberseguridad., U. I. (2010). Obtenido de https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

Comunicaciones., M. d. (2019). *Ciberseguridad.* Obtenido de https://mintic.gov.co/portal/604/w3-article-18723.html?_noredirect=1

Conexionesan. (19 de 09 de 2018). *¿Cómo marcha la ciberseguridad en América Latina?* Obtenido de https://www.esan.edu.pe/apuntes-empresariales/2018/09/como-marcha-la-ciberseguridad-en-america-latina/

consolidada, L. (29 de 4 de 2011). *Ley 8 de 2011.* Obtenido de https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

Corletti Estrada, A. (09 de 2017). *Ciberseguridad, Una estrategia informático / militar.* Obtenido de http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

Cuzme Rodriguez, F. G. (2019). *ANALISIS Y PLANTEAMIENTO DE POLÍTICAS: ACUERDO AL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN; EGSI; EMPRESA PÚBLICA YACHAY.* Obtenido de - http://repositorio.utn.edu.ec/bitstream/123456789/9001/1/05%20FECYT%20213%20TRABAJO%20DE%20GRADO.pdf

dinero, r. (26 de 4 de 2016). *Los ciberdelincuentes se filtran en el corazón de las organizaciones*. Obtenido de https://www.dinero.com/empresas/articulo/los-ciberdelincuentes-que-operan-desde-el-interior-de-las-organizaciones-en-colombia/222883

Fernández Pérez, Y. (2018). *Modelo computacional para la evaluación y selección de productos de software.* . Obtenido de https://digibug.ugr.es/bitstream/handle/10481/51180/29022307.pdf?sequence=4&isAllowed=y

Fidalgo., L. V. (2019). *Aplicabilidad de la ingeniería concurrente colaborativa en proyectos de diseño tecnológicamente complejos con requerimientos no documentados.* Obtenido de https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

Foster., E. (2018). *Testing Web Application Security Scanners against a Web 2.0 Vulnerable Web Application.* Obtenido de https://www.sans.org/reading-room/whitepapers/tools/paper/38630

Gago, E. A. (s.f.). *El enfoque argentino sobre ciberseguridad y ciberdefensa (Doctoral dissertation, Escuela Superior de Guerra Tte Grl Luis María Campos).* Obtenido de 2017: http://cefadigital.edu.ar/bitstream/1847939/1097/1/TFL%20RRII%202017%20G1E3_214.pdf

Gary McGraw, P. S. (2014). *Building Security in Maturity Model.* . Obtenido de http://www.fundacionsadosky.org.ar/wp-content/uploads/2014/07/BSIMM-V-esp.pdf

Gasca-Hurtado, G. &. (2013). *Taxonomía de riesgos de outsourcing de software/Software outsourcing risk taxonomy.* Obtenido de Ingeniare: Revista Chilena De Ingenieria, 21(1), 41-53.: https://www.researchgate.net/publication/262664579_Taxonomia_de_riesgos_de_outsourcing_de_software

Guaman-Quinche, R. (2016). *Seguridad en Aplicaciones web para Sistemas de Gestión Académica.*

IEEE. (30 de julio de 2017). *C/S2ESC - Software & Systems Engineering Standards Committee.* Obtenido de http://ieeexplore.ieee.org/abstract/document/917550/

Jairo Andrés Becerra, M. E. (s.f.). *La Seguridad en el ciberespacio. Un desafío para Colombia.* Obtenido de https://esdeguelibros.edu.co/index.php/editorial/catalog/download/42/48/741-1?inline=1

Jangirala Srinivasa, A. K. (2019). *Government Regulations in Cyber Security: Framework, Standards and Recommendations.* Obtenido de https://www.researchgate.net/profile/Srinivas_Jangirala/publication/328183318_Government_regulations_in_cyber_security_Framework_standards_and_recommendations/links/5c1d53d892851c22a33d339e/Government-regulations-in-cyber-security-Framework-standards-and-

Karl Wiegers, J. B. (06 de 09 de 2013). Software Requirements.

Lascano Rivera, S. B. (2017). *Guía metodológica para el desarrollo de aplicaciones móviles enfocadas al M-Learning.* . Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/7439/1/PG%20542%20TRABAJO%20DE%20GRADO.pdf

Liliana González, S. A. (2015). *Campo de investigación en tecnologías de información y comunicación: Estrategia de gobernanza en la universidad de Medellin/Field research in information technologies: strategy at university Medellin.* Obtenido de /Field research in information and communication technologies: Governance strategy at universidad de medellín. Ingeniare: Revista Chilena De Ingenieria, 23(2), 301-311.: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-33052015000200015

Lopez, P. G. (14 de octubre de 2013). *Principales Novedades de la ISO 27001/ISO 27002.* Obtenido de http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf

Marquez Alayo, P. F. (2018). *Ciberseguridad y su Relación en la Seguridad de los Sistemas Informáticos del Ejercito del Perú Caso: DITELE 2013-2014.* Obtenido de http://repositorio.icte.ejercito.mil.pe/bitstream/ICTE/122/1/49%20TESIS%20Marquez%20Alayo%20Pedro%20Fernando%20%281%29.pdf

Martín Darío Arango, J. E.-B. (21 de Julio de 2015). *Solution architecture approach, mechanism to reduce the gap between enterprise architecture and implementation of technological solutions.* Obtenido de http://www.redalyc.org/pdf/496/49642141016.pdf

Members, I. D. (2019). Cybersecurity Best Practices Guide . https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf .

Michael Nieles, K. D. (junio de 2017). *An Introduction to Infomration Security.* Obtenido de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Miranda, E. C. (2010). *DINÂMICA DA ACUMULAÇÃO DE CAPACIDADES INOVADORAS: EVIDÊNCIAS DE EMPRESAS DE SOFTWARE NO RIO DE JANEIRO E EM SÃO PAULO/DYNAMICS OF ACCUMULATION OF CAPABILITY FOR INNOVATION : EVIDENCE FROM SOFTWARE FIRMS IN RIO DE JANEIRO AND SÃO PAULO.* Obtenido de DINÁMICA DE LA ACUMULACIÓN DE CAPACIDADES INOVADORAS: EVIDENCIAS DE EMPRESAS DE SOFTWARE EN RIO DE JANEIRO Y EN SÃO PAULO. Revista De Administração De Empresas, 50(1), 75-93.: https://www.academia.edu/4821537/Din%C3%A2mica_da_acumula%C3%A7%C3%A3o_de_capacidades_inovadoras_evid%C3%AAncias_de_empresas_de_software_no_Rio_de_janeiro_e_em_S%C3%A3o_Paulo

Mora Rodriguez, M. L. (2016). *ESTRATEGIAS PARA MEJORAR ATENCIÓN DEL IESS; INGENIERÍA COMERCIAL; DEPARTAMENTO DE PENSIONES IMBABURA; FONDO MORTUORIO.* Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/5485/1/02%20ICO%20493%20TRABAJO%20DE%20GRADO.pdf

Nación, F. G. (22 de 12 de 2017). *Índice de información clasificada y reservada.* Obtenido de https://www.fiscalia.gov.co/colombia/indice-de-informacion-clasificada-y-reservada/

Nación, F. G. (21 de 06 de 2017). *Mapa de Procesos*. Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Mapa-de-procesos-2017.jpg

Nación, F. G. (13 de 12 de 2018). *Declaración de índice de información clasificada y reservada* . Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/10_3-%C3%8Dndice-de-Informaci%C3%B3n-Clasificada-y-Reservada-%C3%8DICR-2018.xlsx

Nación, F. G. (22 de 10 de 2018). *Mapa de riesgos institucional - 2017*. Obtenido de https://www.fiscalia.gov.co/colombia/mapa-de-riesgos-institucional/

Nación, F. G. (15 de 07 de 2018). *Plan estrategico 2016-2020.* Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Plan-estrateigico-2016-2020-003-.pdf

Nación, F. G. (20 de 10 de 2018). *Plan estratégico 2016-2020.* Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Direccionamiento-estrate%CC%81gico-2016-2020-df-1.pdf

Nación, F. G. (20 de 02 de 2018). *Políticas de seguridad de la información del sitio web y protección de datos personales.* Obtenido de https://www.fiscalia.gov.co/colombia/politicas-de-seguridad-de-la-informacion-del-sitio-web-y-proteccion-de-datos-personales/

Nación, F. G. (24 de 09 de 2018). *RESOLUCIÓN NÚMERO 01165 DE 2018, POR MEDIO DE LA CUAL SE DEFINE EL ESQUEMA DE GOBIERNO DE LA ARQUITECTURA INSTITUCIONAL DE LA FISCALÍA GENERAL DE LA NACIÓN Y SE DICTAN OTRAS DISPOSICIONES.* Obtenido de https://app.vlex.com/#vid/740009173

Nación, F. G. (24 de 02 de 2019). *Manual Único de Policia Judicial*. Obtenido de https://www.fiscalia.gov.co/colombia/wp-content/uploads/Manual-de-Policia-Judicial-Actualizado.pdf

Narváez Pupiales, S. K. (2018). *MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN;INSTITUCIONES DE SALUD;BASADO EN LAS NORMAS ISO 27799:2008, ISO/IEC 27005:2008 E ISO/IEC 27002:2013; APLICADA A LA CLÍNICA MÉDICA FÉRTIL.* Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/8572/1/04%20RED%20201%20TRABAJO%20DE%20GRADO.pdf

Novillo Vicuña, J. P. (2019). *IMPLEMENTACIÓN DE CONTROLES QUE PERMITAN GARANTIZAR LA SEGURIDAD DE UN SITIO WEB A OWASP*. Obtenido de http://repositorio.utmachala.edu.ec/bitstream/48000/13606/1/ECUAIC-2019-SIS-DE00010.pdf

Novillo Vicuña, J. P. (2019). *OWASP.* Obtenido de http://repositorio.utmachala.edu.ec/bitstream/48000/13606/1/ECUAIC-2019-SIS-DE00010.pdf

Open Web Application Security Project, O. (19 de 4 de 2015). *SAMM - Security Requirements - 1*. Obtenido de https://www.owasp.org/index.php/SAMM_-_Security_Requirements_-_1

Óscar Fernando, C. D. (2007). *Basis for implementing a model of intelligence for strengthening the technological development of the software industry and its associated services in colombia.* Obtenido de Ingeniería e Investigación, 27(3), 182-192.: http://search.proquest.com/docview/1677615665?accountid=143348

Osterwalder, A. (2010). *Bussiness Model Generation a Handbook for visionaries, game changers and Callengers.* Obtenido de univerisad de los andes.: https://profesores.virtual.uniandes.edu.co/.../fetch.php?...business_model_generation.pdf

OWASP, T. O. (27 de agosto de 2017). *OWASP Top 10 -2013*. Obtenido de https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

OWASP-2017. (2017). *OWASP Top 10 -2017 Los diez riesgos más críticos en Aplicaciones Web.* Obtenido de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Owens. (2007). *STRATEGY AND THE STRATEGIC WAY OF THINKING. Naval War College Review, 60(4), 111-124.* Obtenido de https://apps.dtic.mil/dtic/tr/fulltext/u2/a520308.pdf

Peraza, A. (2012). *La estrategia gerencial y su aplicación en la gestión de los gobiernos locales.* Obtenido de https://www.redalyc.org/pdf/2190/219022812005.pdf

Pérez, A. P. (2016). *VENTAJAS DE APLICAR LA TRIANGULACIÓN EMPRESARIAL ENTRE ESPAÑA, CHINA Y AMÉRICA LATINA. UNA RELACIÓN WIN-WIN PARA TODOS LOS POLOS/.* Obtenido de Título en inglés: "the advantages of applying the business triangulation model between spain, china and latin america. A win-win relationship for all poles". UNISCI Discussion Papers, (41), 105-138.: https://www.ucm.es/data/cont/media/www/pag-83486/UNISCIDP41-5PARRA.pdf

Planeación, D. N. (16 de 04 de 2016). *Documento CONPES 3854 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.* Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Pressman, R. s. (2010). Software engineering a Practitioner's Approach. En R. s. Pressman. Bostom Burr Ridge: Mc Graw Hill.

Pressman, R. S. (2010). *Software enginierring A Practitioner´s Approach.* New York: Mc Graw Hill.

Procopiuck, M. &. (2009). *Redes de políticas públicas e de governança e sua análise a partir da websphere analysis. Revista De Sociologia e Política, 17(34), 63.* Obtenido de http://www.scielo.br/pdf/rsocp/v17n34/a06v17n34.pdf

Project, O. W. (1 de 3 de 2019). *Application Security Verification Standard 4.0.* Obtenido de https://github.com/OWASP/ASVS/raw/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0-en.pdf

Project, O. W. (3 de 2019). *Application Security Verification Standard 4.0.* Obtenido de https://www.owasp.org/images/8/88/OWASP_Application_Security_Verification_Standard_4.0-en.docx

Ramírez Quesada, A. (2018). *Modelos metaheurísticos para el soporte a la decisión en el proceso de construcción de software.* . Obtenido de https://helvia.uco.es/xmlui/bitstream/handle/10396/17194/2018000001823.pdf?sequence=1&isAllowed=y

Rivera Davila, A. O. (2019). *Riesgos de ciberseguridad y sus consecuencias en la prevención de fraudes en las empresas industriales del Distrito de Yanacancha – Pasco 2016.* . Obtenido de http://repositorio.undac.edu.pe/bitstream/undac/1372/1/T026_04066691_M.pdf

Robles Carrillo, M. (2015). *EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO*. Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-CIberseguridad_Margarita-Robles.pdf

Robles Carrillo, M. (2015). *EL CIBERESPACIO Y LA CIBERSEGURIDAD: CONSIDERACIONES SOBRE LA NECESIDAD DE UN MODELO JURÍDICO.* Obtenido de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-CIberseguridad_Margarita-Robles.pdf

Rubio Blanco, J. A. (2016). *Un Marco para el Análisis de Riesgos en Ciberseguridad.* . Obtenido de https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=gkX4iYQL2UE%3D

Ruiz Robles, R. A. (2017). *Valoración y gestión estratégica de activos de proceso intangibles en ingeniería del software.* . Obtenido de https://e-archivo.uc3m.es/bitstream/handle/10016/25144/tesis_ronald-alejandro_ruiz_robles_2017.pdf?sequence=1&isAllowed=y

Sanchez Blas, J. J. (2017). *Adopción de estrategias de Ciberseguridad en la protección de la Información en la Oficina de Economía del Ejército, San Borja- 2017.* . Obtenido de http://repositorio.icte.ejercito.mil.pe/bitstream/ICTE/26/1/Tesis%20John%20Sanchez%20Blas.pdf

Sánchez, J. M. (2016). *Control de proyectos de software: Actualidad y retos para la industria cubana/Control of software projects: Actuality and challenges for the cuban industry.* Obtenido de Ingeniare: Revista Chilena De Ingenieria, 24(1), 102-112.: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-33052016000100010

Sandra Cristina, R. E. (2008). *A model for assessing information technology effectiveness in the business environment. Ingeniería e Investigación, 28(2), 158-166.* Obtenido de https://revistas.unal.edu.co/index.php/ingeinv/article/view/14905/15710

Serna Patiño, A. M. (2018). *ANÁLISIS DE LA CAPACIDAD DE CIBERSEGURIDAD PARA LA DIMENSIÓN TECNOLÓGICA EN COLOMBIA: UNA MIRADA SISTÉMICA DESDE LA ORGANIZACIÓN.* Obtenido de https://repository.upb.edu.co/bitstream/handle/20.500.11912/4152/AN%C3%81LISIS%20DE%20LA

Services, A. W. (2019). *Marco de seguridad cibernética NIST (CSF, por sus siglas en inglés). Alineación con el NIST CSF en la nube de AWS.* Obtenido de https://d1.awsstatic.com/whitepapers/es_ES/compliance/NIST_Cybersecurity_Framework_CSF.pdf

Social, C. N. (2011). *LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA.* Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Social., C. N. (2011). *Lineamientos de política para la Ciberseguridad y Ciberdefensa. .* Obtenido de https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Stok, A. v. (27 de julio de 2005). *Una Guía para Construir Aplicaciones y Servicios Web Seguros.* Obtenido de https://www.owasp.org/images/b/b2/OWASP_Development_Guide_2.0.1_Spanish.pdf

Systems, O. (2016). Estadísticas de ciberataques empresas. págs. https://www.onasystems.net/estadisticas-ciberataques-empresas/.

Techonology, N. I. (febrero de 2005). *Recommended Security Controls for Federal Information Systems.* Obtenido de http://infohost.nmt.edu/~sfs/Regs/sp800-53.pdf

TIC, M. (23 de 10 de 2018). Estadísticas del sector. págs. http://colombiatic.mintic.gov.co/602/w3-propertyvalue-707.html.

TIC, M. d. (17 de 07 de 2014). *Diseño y Especificación del Marco de Referencia. Diseño Detallado. Marco de Referencia de Arquitectura Empresarial para la Gestión de Tecnologías de la Información (TI), a Adoptar en las Entidades del Sector Público Colombiano.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-4211_sumen_del_diseno_y_especificacion_del_Marco_de_Referencia_de_la_Arquitectura_Empresarial_para_la_Gestion_TI_del_Estado.pdf

TIC, M. d. (Julio de 2016). *Documento - Versión Actualizada del Modelo de Gestión IT4+.* Obtenido de https://www.mintic.gov.co/arquitecturati/630/propertyvalues-8170_documento_pdf.pdf

TIC, M. d. (16 de 02 de 2019). *Arquitectura TI Colombia.* Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8083.html

TIC, M. d. (2019). *INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD.* Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

tiempo, E. (16 de 05 de 2016). Una hora en el búnker que frena los ataques cibernéticos a la Fiscalía . págs. https://www.eltiempo.com/archivo/documento/CMS-16595102.

Valencia Maldonado, F. G. (2014). *MODELO DE GESTIÓN DE RIESGOS; GESTIÓN ADMINISTRATIVA; NORMA ISO 31.000:2009;ESTÁNDAR AS/NZS 4360;IBARRA;GOBIERNO AUTÓNOMO DESCENTRALIZADO.* . Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/2437/1/02%20ICA%2054

Varela Recalde, E. A. (2019). SISTEMAS COMPUTACIONALES; SEGURIDAD DE INFORMACIÓN; METODOLOGÍA MAGERIT; SEGURIDAD PERIMETRAL; FIREWALL. http://repositorio.utn.edu.ec/bitstream/123456789/7728/1/04%20ISC%20384%20TRABAJO%20GRADO.pdf.

Villalba Fernández, A. (2015). *La ciberseguridad en España 2011-2015 una propuesta de modelo de organización.* Obtenido de http://e-spacio.uned.es/fez/eserv/tesisuned:CiencPolSoc-Avillalba/VILLALBA_FERNANDEZ_Anibal_Tesis.pdf

Vive digital colombia. (31 de 5 de 2016). *G. GEN.3. Guia General de un proceso de Arquitectura Empresarial.* Obtenido de https://www.mintic.gov.co/arquitecturati/630/articles-9435_Guia_Proceso.pdf

Wiegers, K. E. (06 de 09 de 2013). *Software Requirements, 3rd Edition, Microsoft Press,*. Obtenido de https://www.academia.edu/12467370/Software_Requirements_3rd_Edition?auto=download

Y. H., &. G. (2019). *Lineamientos Estratégicos Para la Gestión Ambiental en las Universidades. LIMITACIONES Y OPORTUNIDADES PARA EL DESARROLLO DEL CARIBE COLOMBIANO.* Obtenido de https://repositorio.sena.edu.co/bitstream/11404/5786/1/limitaciones_oportunidad_desarrollo_caribe_colombiano.pdf

Anexo No 1. Detalle de riesgos identificados en el proceso de construcción de aplicaciones Web

Por la falta de una estrategia de ciberseguridad y ciberdefensa en el desarrollo, la implementación y uso de aplicaciones web en la Fiscalía General de la Nación se requiere como la falta de un modelo de seguridad para el diseño, desarrollo o adopción, pruebas, implementación y mantenimiento de aplicaciones de la Fiscalía General de la Nación por la carencia de una estrategia de ciberseguridad y ciberdefensa para las aplicaciones web misionales. En este sentido se identifican los siguientes aspectos en la valoración de los riesgos manejados por la Entidad:

Probabilidad	Nivel	Impacto	Nivel
Raro	1	Insignificante	1
Improbable	2	Menor	2
Posible	3	Moderado	3
Probable	4	Mayor	4
Casi seguro	5	Catastrófico	5

Tabla 10: Niveles de impacto y probabilidad para la valoración de riesgos.

En este sentido se realiza el análisis de riesgos de los desarrollos de las aplicaciones web para la publicación de los servicios de información en el ciberespacio basados en OWASP y NIST de la siguiente manera:

IDENTIFICACIÓN					**CALIFICACIÓN DEL RIESGO ANTES DE CONTROLES RIESGO INHERENTE**		
Formulación del riesgo	**Clasificación**	**Descripción**	**Causas**	**Consecuencias**	**PROBABILIDAD**	**IMPACTO**	**NIVEL DE RIESGO**
AD-01: Perder credibilidad en las aplicaciones web de la Entidad	Administrativo	Perdida de la credibilidad de los servicios de Información en el ciberestapacio por mal funcionamiento del sistema de información	Falta de oportunidad de información en el ciberespacio por indisponibilidad de las aplicaciones web.	No se cuenta con la viabilidad para el desarrollo de las aplicaciones web de la Entidad.	**3**	5	15

AD-02: Cambiar las prioridades establecidas por la alta dirección para el desarrollo de aplicaciones web de la entidad que soportan los servicios de información.	Administrativo	Cambios en los lineamientos políticos de la entidad para la publicación de los servicios de información en el ciberespacio.	falta de conocimiento del beneficio del proyecto para la publicación y divulgación de servicios de información	Desactualización tecnologica y funcional de las aplicaciones web	**2**	4	8
AD-03: Perder los recursos para la implementación de proyectos de fortalecimiento de las aplicaciones web que soportan los servicios de información en el ciberespacio	Administrativo	Indisponibilidad de los servicios de información en el ciberespcaio debido a conflictos en la priorización de recursos para la ejecución de los planes formulados por las diferentes áreas	Lineamientos de la alta dirección frente a las políticas de austeridad del estado	Desactualización tecnológica y funcional de las aplicaciones web	**2**	4	8
AD-04: Perder de gobernabilidad de las aplicaciones web por rotación o cambio de personal	Administrativo	Debido a la necesidad del negocio se implementan los cambios en personal	Necesidad de optimizar recursos y procesos	Falta de actualización funcional de las aplicaciones web.	**3**	5	15
AD-05: Cambiar los requerimientos funcionales en la construcción de las aplicaciones web debido a la reestructuración de las áreas misionales o cambios en los procesos de la entidad	Administrativo	Se reformulan funciones debido a la disponibilidad de personal de la Entidad	Cumplimiento de necesidad de cambiar la estructura frente a los cambios del comportamiento criminal	Falta de actualización funcional de las aplicaciones web.	**3**	5	15
AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación en los proyectos de desarrollo de aplicaciones web	Administrativo	Se considera la seguridad de la información como únicamente del dominio tecnológico.	Limitación de controles de seguridad a soluciones de índole tecnológico.	Incorporación de vulnerabilidades en la arquitectura de las aplicaciones web	**3**	4	12
AD - 07: Perder la documentación técnica actualizada en los desarrollos internos efectuados en la Subdirección de TIC	OPERATIVO	Se podría presentar dependencia de desarrolladores para modificaciones futuras en las aplicaciones web efectuados en la Subdirección de TIC	No se siguen las buenas prácticas para el desarrollo de Aplicaciones web Especialización de desarrolladores en proyectos específicos Retroalimentación al interior del equipo de trabajo	Imposibilidad de modificación o reproceso en las aplicaciones web afectando los cronogramas proyectados de desarrollo Dependencia de los desarrolladores Desconocimiento de los desarrollos	**3**	3	9

				realizados por parte del equipo de trabajo			
AD-08: Actulizar e Implementar de una arquitectura de gobierno flexible como producto de la arquitectura empresarial	Administrativo	**Se debe implementar la arquitectura empresarial en todos sus compontes para mejorar la efectividad de la Entidad**	Se contrata el diseño de la arquitectura empresarial	**Se cuenta con el soporte y lineamientos de la arquitectura empresarial de la entidad**	**3**	3	9
AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición	Alcance	Con el fin de atender las necesidades en una vigencia se sobrecarga el alcance del proyecto	Necesidad de dar resultados con los recursos disponibles	Indisponibilidad de los servicios por el sistema de información	**3**	3	9
AL-02: Perder la disponibilidad de las aplicaciones web por obsolescencia funcional y técnica.	Alcance	Dentro del ciclo de vida del sistema de información no se definen o se satisfacen nuevos requerimientos funcionales y técnicos limitando cada vez más su apoyo en la gestión de la entidad.	Necesidad de dar resultados con los recursos disponibles	Indisponibilidad de los servicios por el sistema de información	**3**	3	9
AL-02: Cambiar de manera no programada en el alcance del proyecto de publicación de servicios en el ciberepacio y el control de cambios en las aplicaciones web	Alcance	Durante la planeación se suscitan cambios en los requerimientos y actividades que impactan el alcance del proyecto	Necesidad de dar resultados con los recursos disponibles	retraso en la entrega de la funcionalidad convenida y generando la indisponibilidad de los servicios de información	**3**	4	12
AL-03: Publicar servicios de información con altos costos soportados por los sistemas legados u obsoletos.	Alcance	Se mantiene el funcionamiento del sistema de información sin considerar los costos de operación y mantenimiento	Necesidad de dar resultados con los recursos disponibles	Falta de alineación con los lineamientos de austeridad estratégica	**3**	4	12
AL-04: Cambiar el alcance de los requerimientos del sistema de información debido a que el equipo de trabajo define su propio alcance	Alcance	Por falla en el establecimiento o en el entendimiento del proyecto se redefine el alcance por parte del equipo de trabajo	Necesidad de dar resultados con los recursos disponibles	Desviación en la atención de los requerimientos de aplicaciones web.	**3**	4	12
AL-05: Formular y estimar requerimientos técnicos o funcionales equivocados	Alcance	Por necesidad de lograr la misión y visión de la entidad, se formula un alcance subestimado	Necesidad de dar resultados con los recursos disponibles	Desviación en la ateción de los requerimientos de aplicaciones web.	**3**	4	12

AL-06: No realizar las actividades programadas en cumplimiento de los planes de desarrollo de las aplicaciones web	Alcance	Debido al priorización de logro de la misión y visión no son viables actividades del proyecto	Necesidad de dar resultados con los recursos disponibles	retraso en la entrega de la funcionalidad convenida y generando la indisponibilidad de los servicios de información	**3**	3	9
AL-07: Definir de manera no adecuada los requerimientos de integración entre las aplicaciones web de la entidad	Alcance	Se presenta falta de integración entre las aplicaciones web fomentado la construcción de funcionalidad ya existente en las aplicaciones web	Necesidad de dar resultados con los recursos disponibles	Desviación en la atención de los requerimientos de aplicaciones web.	**3**	3	9
AL-08: Implementar requerimientos de seguridad no autorizados en la adquisición, desarrollo, implementación y uso de las aplicaciones web	Alcance	Por necesidad de lograr la misión y visión de la entidad, se formula un alcance subestimado	Necesidad de dar resultados con los recursos disponibles	Desarrollo de aplicaciones web con vulnerabilidades ya detectadas.	**3**	5	15
AL-09: Automatizar y fortalecer procesos de la entidad con el apoyo de la implementación de aplicaciones web misional.	Alcance	**Con la implementación de la legislación en la entidad se ha desarrollado un conocimiento para ser automatizado y apoyar los procesos misionales de la Entidad**	Se capitaliza el conocimiento en proyectos de SI	**Se ofrecen servicios de información para satisfacer las necesidades funcionales y técnicas de acuerdo con la arquitectura empresarial de la entidad**	**3**	3	9
ES-01: Perder la integración de los componentes de la estrategia con la arquitectura empresarial y el direccionamiento estratégico de la Entidad	Estratégicos	Se realiza el análisis teniendo en cuenta el plan de acción de una vigencia sin ser soportado dentro de la arquitectura de gobierno o del direccionamiento estratégico de la Entidad	Falta de estrategia de ciberseguridad y ciberdefensa para aplicaciones web de la entidad	Las aplicaciones web se desarrollan sin tener en cuenta la arquitectura empresarial de la entidad.	**3**	3	9
ES-02: Duplicar la funcionalidad de las aplicaciones web en los desarrollos.	Estratégicos	Debido a la especialización de las áreas de la Entidad se contemplan condiciones de especialización y confidencialidad del desarrollo	Falta de estrategia de ciberseguridad y ciberdefensa para aplicaciones web de la entidad	reprocesos en el desarrollo de aplicaciones web.	**3**	4	12
ES-03: Perder la integración de procesos o procedimientos de la Entidad	Estratégicos	Ante nuevas funciones de las áreas, se define procesos que no se detallan adecuadamente e impacta la integración	Falta de estrategia de ciberseguridad y ciberdefensa para aplicaciones web de la entidad	Falta de lineamientos Estratégicos de publicación de información en el ciberespacio	**3**	4	12
ES-04: Generar políticas de seguridad de la información no alineadas para la publicación e	Estratégicos	No se actualiza las políticas de seguridad a la realidad operativa de la Entidad	Falta de estrategia de ciberseguridad y ciberdefensa para aplicaciones web de la entidad	Falta de lineamientos Estratégicos de publicación de información en el ciberespacio	**3**	4	12

intercambio de información.							
ES-05: Perder la vigencia de gestión de riesgos de la publicación de servicios de información en el ciberespacio.	Estratégicos	Los funcionarios gestionan los riesgos de acuerdo con su interpretación o conocimiento	Falta de estrategia de ciberseguridad y ciberdefensa para aplicaciones web de la entidad	Falta de lineamientos Estratégicos de publicación de información en el ciberespacio	**3**	4	12
ES-06: Fortalecer el sistema de calidad implantado	Estratégicos	**Se cuenta con Sistema de Gestión de calidad institucional**	Se cuenta con sistema de calidad implementado	**Se cuenta con lineamientos de calidad de servicios de información**	**3**	4	12
PR-01: Retrasar la ejecución del cronograma del proyecto de desarrollo de aplicaciones web	Cumplimiento	Se genera retraso en lo programado debido a factores externos al proyecto	Limitación de presupuesto y ajuste en la formulación del proyecto	Sobrecostos en el desarrollo de aplicaciones web	**3**	3	9
PR-02: Priorizar de manera no planeada o equivocada de la atención de requerimientos de desarrollo de aplicaciones web.	Cumplimiento	Se cambia la ruta crítica en el plan del proyecto por razones no totalmente documentadas	Limitación de presupuesto y ajuste en la formulación del proyecto	Sobrecostos en el desarrollo de aplicaciones web	**3**	3	9
PR-03: Interrumpir o desviar las actividades del proyecto de desarrollo de aplicaciones web	Cumplimiento	Se interrumpen las actividades programadas por limitaciones externas	Limitación de presupuesto y ajuste en la formulación del proyecto	Sobrecostos en el desarrollo de aplicaciones web	**3**	3	9
PR-04: Generar reprocesos y sobrecostos en la ejecución del proyecto de desarrollo de aplicaciones web.	Cumplimiento	Se genera una subestimación de los costos de la ejecución debido a limitaciones en la planeación	Limitación de presupuesto y ajuste en la formulación del proyecto	Sobrecostos en el desarrollo de aplicaciones web	**3**	3	9
PR-05: Perder disponibilidad de los componentes de las aplicaciones web	Cumplimiento	Durante la ejecución se incluyen componentes en el proyecto que no son sostenibles.	Limitación de presupuesto y ajuste en la formulación del proyecto	Altos costos en el mantenimiento de las aplicaciones web para la publicación e intercanbio de información	**3**	3	9
PR-06: Contar con recursos propios para el desarrollo de aplicaciones web criticos para la entidad.	Cumplimiento	**Se realiza una adecuada estimación a partir de la defincón de los requerimientos enmarcados en los procesos y procedimientos documentados de la Entidad**	Se prioriza los proyectos de impacto	**Se satisface las necesidades de publicación e intercambio de información de la entidad**	**3**	3	9

A0: Perder funcionamiento de las aplicaciones web.	OPERATIVO	Se podría presentar mal funcionamiento de las aplicaciones web por fallas en el código fuente desarrollado.	Descripción insuficiente de los Requerimientos. No se aplican las buenas prácticas de desarrollo Se realizan modificaciones no validadas, no controladas y no autorizadas en el código fuente No se realiza un manejo adecuado de excepciones	Indisponibilidad en el servicio de las aplicaciones web Perdida de información Afectación de la integridad de la información	3	4	12
A0. Operar con una arquitectura de aplicaciones web desactualizada	OPERATIVO	Se podría presentar infraestructura informática desactualizada a nivel nacional, con el surgimiento de nuevas tecnologías y/o no ejecución del Plan Maestro de Tecnología. Lo anterior se pudo evidenciar de acuerdo a las necesidades contenidas en el Plan Maestro de Tecnología y al seguimiento de los contratos. Esta situación podría contravenir la visión de la FISCALÍA GENERAL DE LA NACIÓN en la aplicación de herramientas innovadoras de tecnología y comunicación, y el objetivo 5 "Investigar y evaluar las innovaciones y desarrollos de TIC, así como definir la posibilidad de incorporación de los mismos en la plataforma tecnológica de la Entidad".	No se cuenta con el presupuesto para cubrir las actividades tecnológicas acorde al Plan Maestro de Tecnología y así dar respuesta eficiente a las necesidades de la Entidad. Rezago tecnológico dentro de la FISCALÍA GENERAL DE LA NACIÓN	Atrasos en actividades propias de la gestión de la FISCALÍA GENERAL DE LA NACIÓN. Necesidades no solucionadas, debido a la falta de implementación de los proyectos del Plan Maestro de Tecnología.	3	4	12

A1: 2017: Perder integridad de los servicios de información en el ciberespacio.	Técnico	En la arquitectura se utiliza datos no confiables en consultas de SQL, NoSQL, LDAP, Xpath, comandos de SO, expresiones de lenguajes Object Graph Navigation Library – OGNL, analizadores de XML, encabezado SMTP, leguajes de expresión, parámetros y consultas OMR.	Uso de código heredado. Falta de filtros de los datos suministrados por el usuario. No se codifican los parámetros de acuerdo con el contexto. Se utiliza datos para extraer registros sensibles en las consultas Object-Relational Mapping – ORM. Uso de datos para generar en comandos o consultas SQL una serie de estructuras, comandos o procedimentos almacenados.	Pérdida de credibilidad en los servicios de información de la Entidad	**3**	3	9
A2: Perder confidencialidad en la autenticación de las aplicaciones web.	Técnico	Los atacantes cuentan con múltiples fuentes de contraseñas utilizadas por usuarios y hacer uso de herramientas para detectar autenticaciones defectuosas.	Reutilización de contraseñas conocidas. Permite ataques de fuerza bruta y automatizados. Permite contraseñas débiles. Procesos débiles de recuperación de contraseña. Almacenamiento de contraseñas en texto claro o con métodos de ciframiento débiles. Implementación débil de autenticación multifactor. Exposición de ID en las URL y validación débil o poca rotación de contraseñas en el cierre de las sesiones.	Accesos no autorizados a las aplicaciones web que soportan la publicación e intercambio de información.	**3**	4	12

A3: exponer datos sensibles.	Técnico	Se exponen datos en la infraestructura de TIC	Utilizan técnicas para robar datos. Falta o débil cifrамiento de datos sensibles en los diferentes niveles de procesamiento, almacenamiento y transmisión de información. Falta de identificación de datos sensibles – información personal sensible (PII), datos de denuncias, credenciales y tarjetas. Transmisión en texto claro. Uso de algoritmos de cifrамiento débiles. Uso de claves de cifrамiento predeterminadas. Falta de rotación de contraseñas. Falta de políticas de seguridad en la construcción de páginas y encabezados Web. Falta de verificación de certificados enviados por los servidores.	Incumplimiento de normas de protección de datos.	**3**	5	15
A4: explotar vulnerabilidades de procesadores XML por parte de entidades externas XML (XXE).	Técnico	Los procesadores XML permite configurar una entidad externa, referencias de URI en el procesamiento del XML.	La aplicación procesa documentos XML directamente. Habilidad del procesador de XML para trabajar definiciones de tipo de documentos – DTDs. Uso de SAML en el procesamiento de identidades. La aplicación utiliza SOAP menor a la 1.2 Ataques de denegación de servicio.	Obsolescencia de las aplicaciones web para la publicación e intercambio de información	**3**	3	9

A5: Perder el Control de Acceso como producto de los ataques de explotación de la falta de controles.	Técnico	Se presenta una pérdida de control de acceso o la imposibilidad de determinar si los controles funcionan correctamente.	Implementación de frameworks que no cuentan con controles de acceso. Falta de pruebas funcionales o unitarias de control de acceso en el desarrollo de la aplicación. Falta de comprobaciones de control de acceso modificando la URL, los estados de la aplicación, modificación del HTML desde API o herramientas de ataque. Cambios de contraseña de usuarios desde un usuario especifico. Cambios de privilegios durante la sesión de un usuario. Manipulación de metadatos, como es el caso de cookies, JSON web token – JWT o campos ocultos de privilegios. Mala configuración de CORS en el acceso de APIs. Navegación desde usuarios no autenticados en páginas autenticadas o privilegiadas. Uso discriminado de los comandos POST, PUT y DELETE soportados por API sin control de acceso.	Materialización de ataques a la disponibilidad, confidencialidad e integridad de los servicios de la información	**3**	4	12
A6: Configurar controles de Seguridad de manera incorrecta.	Técnico	Creación de vulnerabilidades conocimiento de reglas del negocio y aplicaciones sin parchar o que permiten el ingreso con cuentas por defecto, uso de páginas sin utilizar, archivos y directorios desprotegidos.	Configuración incorrecta o predeterminada de los componentes de un sistema de información. Configuración de servicios innecesarios o de opciones legadas. Falta de endurecimiento de las plataformas de TIC. Falta de configuración adecuada de permisos en la nube. Uso de cuentas predeterminadas y falta de rotación de contraseña.	Falta de concienciación en el tratamiento de los riesgos de ciberseguridad y ciberdefensa de la entidad	**3**	5	15

			Trazas de uso de la aplicación para el manejo de errores. Las nuevas funciones de seguridad del sistema de información se encuentran desactivadas o no configuradas correctamente. Falta de identificación y uso de valores seguros en las configuraciones de los componentes del sistema. El servidor no envía cabeceras de seguridad a usuarios.				
A7: Explotar comandos del navegador por medio de Cross – Site Scripting (XSS),.	Técnico	Permite ejecutar secuencia de comandos en el navegador para hurtar credenciales, secuestro de sesiones e instalación de software malicioso.	La aplicación utiliza datos sin validar o codificados, (XSS reflejado). No existe cabecera producto de una política de seguridad de contenido (CSP). La aplicación almacena datos sin verificar de los usuarios para ser utilizados por otros usuarios (XSS-Almacenado). La aplicación incluye datos dinámicos, paginas o APIs controlables por un atacante (XSS basado en DOM)	Perdida de confidencialidad en los servicios de información de la entidad en el ciberespacio	**3**	3	9
A8: Permitir la deserialización Insegura afectadon el comportamiento fucnional del sistema de información.	Técnico	Es la explotación de la deserialización de objetos controlables por un atacante para el cambio del comportamiento de la aplicación.	Ataque a los objetos y datos del sistema para la ejecución remota de código. Uso de comunicación remota e inter-procesos (RPC/IPC) Uso de protocolo de comunicaciones, web services y brokers de mensajes. Caching y persistencia. Uso de base de datos, servidores de cache y sistemas de archivos.	Perdida de integridad de los servicios de información de la entidad en el ciberespacio	**3**	3	9

A9: Usar componentes con vulnerabilidades conocidas.	Técnico	Uso de herramientas de exploits para utilizar las vulnerabilidades conocidas de los componentes de un sistema de información.	Uso indiscriminado de componentes de terceros que forman parte de las aplicaciones web. Falta de descripción de los ataques por parte de analistas de seguridad. Falta de soporte o actualización de los componentes de un sistema de información. Falta de análisis periódico de los componentes de un sistema de información. Falta de actualización de los componentes de acuerdo con un análisis de riesgos.	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	3	9
A10: Realizar registro y monitoreo insuficientes en el sistema de información.	Técnico	Utiliza el desconocimiento de las vulnerabilidades del sistema de información para realizar ataques.	Falta de eventos auditables en el sistema de información. Falta de claridad de los errores y advertencias del sistema de información Falta de monitoreo de registro de aplicaciones o APIs de las aplicaciones web. Almacenamiento de registros de manera local. Pruebas de penetración sin informe de alertas. Falta de reacción de incidentes de seguridad en las aplicaciones web.	Falta de auditabilidad del uso y publicación de los servicios de información en el ciberespacio.	**3**	4	12
TE-01: Perder la escalabilidad de los componentes de desarrollo de aplicaciones web	Técnicos	De la arquitectura de la solución se incluyen componentes que no son escalables o sostenibles por la extralimitación en las soluciones a los requerimientos establecidos.	Se implementan soluciones sin un claro beneficio para la entidad	Falta de flexibilidad en la publicación de servicios de información en el ciberespacio.	**3**	3	9
TE-02: Perdida de aplicabilidad del modelo de seguridad en el ciclo de vida de las aplicaciones web de la Entidad	Técnicos	El modelo de seguridad no asegura el proceso de desarrollo del software.	Se implementan soluciones sin un claro beneficio para la entidad	Utilización de procesos de desarrollo de aplicaciones web desalineados con la arquitectura empresarial de la entidad.	**3**	4	12

TE-03: Implementar componentes de las aplicaciones web con vulnerabilidades de seguridad	Técnicos	No se asegura en el modelo aplicado las vulnerabilidades del sistema de información	Se implementan soluciones sin un claro beneficio para la entidad	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	4	12
TE-04: Implementar aplicaciones web con controles innecesarios	Técnicos	Se extralimita en controles que no mitigan los riesgos	Se implementan soluciones sin un claro beneficio para la entidad	Afectación de la disponibilidad de los servicios de información	**3**	2	6
TE-05 – Permitir Inyección de código en las aplicaciones web que soportan los servicios de información en el ciberespacio	Técnicos	Se presentan eventos de inyección de código	No se realizan las pruebas necesarias	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	3	9
TE-06 – Perder la autenticación y gestión de Sesiones	Técnicos	No se requiere controles de sesión en los desarrollos	No se definen requerimientos de control de seguridad del software	Fuga de datos en la publicación de servicios de información en el ciberespacio.	**3**	4	12
TE-07 – Permitir la Secuencia de comandos en sitios cruzados (XSS)	Técnicos	No se requiere control de XSS	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	3	9
TE-08 – Permitir la Referencia Directa Insegura a Objetos de in sistema de información.	Técnicos	No se desarrolla funcionalidad de control de acceso a objetos de la arquitectura de software	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	3	9
TE-09 – Permitir la Configuración de Seguridad Incorrecta	Técnicos	No se tiene detalle de requerimientos de seguridad en el desarrollo de aplicaciones web.	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	3	9
TE-10 – Perder de información por exposición de Datos Sensibles	Técnicos	No se protegen datos como IP, usuarios, password	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	5	15
TE-11 – Implementar aplicaciones web con ausencia de Control de Acceso a las Funciones	Técnicos	No se requiere control en las funciones del software	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	5	15
TE-12 – Permitir la Falsificación de peticiones en sitios Cruzados (CSRF)	Técnicos	No se implementa controles de link desde el software	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	5	15
TE-13 – Usar de Componentes con	Técnicos	En el desarrollo no se evalúa los componentes a incluir en la arquitectura	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de	**3**	4	12

Vulnerabilidades Conocidas				información con vulnerabilidades.			
TE-14– Permitir las redirecciones y reenvíos no validados	Técnicos	No se controlan las redirecciones en el desarrollo	No se definen requerimientos de control de seguridad del software	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	4	12
TE-15: Implementar aplicaciones web con componentes que no tiene estabilidad	Técnicos	No se concibe una arquitectura adecuada a la demanda del servicio	Se implementan soluciones sin un claro beneficio para la entidad	Publicación en el ciberespacio de servicios de información con vulnerabilidades.	**3**	4	12
TE-16: Reutilizar componenentes de software estándar y seguros	Técnicos	**Con la plataforma de TIC de la entidad se dan soluciones a los requerimientos de desarrollo de la Entidad.**	Se cuenta con una infraestructura implementada	Fortalecimiento de los mecanismos de seguridad para la publicación de servicios de información en el ciberespacio.	**3**	3	9

De este análisis, se cuenta con la matriz de aceptabilidad de la siguiente manera

IDENTIFICACIÓN			**RIESGO RESIDUAL**								
Formulación del riesgo	**FORMULACIÓN DEL CONTROL**	**Tipo**	**PROBABILIDAD**	**IMPACTO**	**NIVEL DE RIESGO**	**Tratamiento**	**Acciones a implementar**	**Periodicidad de evaluación del control**	**Área responsable**	**Indicadores**	**Monitoreo**
AD-01: Perder credibilidad en las aplicaciones web de la Entidad	Establecimiento de plan de continuidad del servicio para mantener disponibles los servicios de información	Preventivo			0	Mitigar	Formulación del plan continuidad de servicios de información en el ciberespacio. Implementación del plan de continuidad para los servicios de	Anual	Dirección Administrativa	Numero de pruebas realizadas del plan de continuidad	TIC

							información de la entidad. Evaluación del plan				
AD-02: Cambiar las prioridades establecidas por la alta dirección para el desarrollo de aplicaciones web de la entidad que soportan los servicios de información.	Determinar el control de cambios para la publicación de servicios en el ciberespacio	Preventivo			4	Mitigar	Control en el proceso de control de cambios en las aplicaciones web que soportan los servicios de información de la entidad	Anual	Dirección Administrativa	Numero de cambios realizados / numero de requerimientos depublicación de servicios identificados	TIC
AD-03: Perder los recursos para la implementación de proyectos de fortalecimiento de las aplicaciones web que soportan los servicios de información en el ciberespacio	Integrar las arquitecturas de las aplicaciones web para atender los requerimientos de publicación de información en el ciberespacio	Preventivo			4	ASUMIR EL RIESGO	Identificar los requerimientos de integración en las aplicaciones web que soportan los servicios de información de la entidad	Anual	Dirección Administrativa	Numero de requerimientos de integración / numero de requerimientos de publicación de servicios identificados	TIC
AD-04: Perder de gobernabilidad de las aplicaciones web por rotación o cambio de personal	Fortalecer los procedimientos de documentación de las aplicaciones web en cuanto a su arquitectura y transferencia de conocimiento a diversos servidores de la entidad	Preventivo			0	Mitigar	Actualización de la documentación	Anual	Dirección Administrativa	Numero de actualizaciones realizadas	TIC
AD-05: Cambiar los requerimientos funcionales en la construcción de las aplicaciones web debido a	entregas tempranas de desarrollo soportado por metodologías de desarrollo ágil	Preventivo			0	Mitigar	Identificación de incidencias a los desarrollos efectuados	Anual	Dirección Administrativa	Numero de incidencias reportadas en los desarrollos	TIC

la reestructuración de las áreas misionales o cambios en los procesos de la entidad										efectuados	
AD-06: Incumplir las políticas de seguridad de la información en la Entidad por falta de concienciación de aplicación el los proyectos de desarrollo de aplicaciones web	Verificación en las diferentes fases del proceso de desarrollo del sistema de información de vulnerabilidades de ciberseguridad	Preventivo				Mitigar	Realizar análisis de vulnerabilidades en las diferentes etapas del procesos de desarrollo de las aplicaciones web.	Anual	Dirección Administrativa	Numero de vulnerabilidades reportadas en los desarrollos efectuados	TIC
AD - 07: Perder la documentación técnica actualizada en los desarrollos internos efectuados en la Subdirección de TIC	Realizar auditorías periódicas de la realización de la documentación.	Preventivo				ASUMIR EL RIESGO	Actualizar la documentación técnica de los SI en cuanto al diseño, implementación y cambios realizados	Anual	Dirección Administrativa	Generar reportes de documentación	TIC
AD-08: Actulizar e Implementar de una arquitectura de gobierno flexible como producto de la arquitectura empresarial	seguimiento al funcionamiento de la arquitectura empresarial de la entidad.	Preventivo				Mitigar	evaluación de indicadores de efectividad de la arquitectura empresarial de la entidad	Semestralmente	Área TIC	Niveles de los indicadores	TIC
AL-01: Sobredimensionar el alcance de los proyectos de adquisición, desarrollo, implementación y uso sin una definición	establecer mecanismos de valoración de esfuerzos para desarrollos o ajustes a las aplicaciones web que soportan la publicación de servicios de información en el ciberespacio.	Preventivo				Mitigar	Establecer niveles de carga de los desarrolladores	Semestralmente	Área TIC	Numero de requerimientos atendidos por desarrollador	TIC

AL-02: Perder la disponibilidad de las aplicaciones web por obsolecencia funcional y técnica.	Formular y ejecutar proyectos de fortalecimiento de las aplicaciones web que soportan los servicios de información de la entidad.	Preventivo				Mitigar	Establecer los proyectos que son atendidos por vigencia.	Semestralmente	Área TIC	Numero de requerimientos atendidos / Numero de requerimientos identificados	TIC
AL-02: Cambiar de manera no programada en el alcance del proyecto de publicación de servicios en el ciberepacio y el control de cambios en las aplicaciones web	Controlar la calidad en la formulación de los requerimientos de publicación de servicios de información de la entidad	Preventivo				Mitigar	establecer el nivel de calidad de la formulación de los requerimientos	Semestralmente	Área TIC	Numero de requerimientos reformulados	TIC
AL-03: Publicar servicios de información con altos costos soportados por los sistemas legados u obsoletos.	Fortalecer las aplicaciones web en cuanto a arquitectura y funcionalidad para la publicación de servicios de información	Preventivo				Mitigar	Establecer los requerimientos de cambio de la arquitectura de las aplicaciones web	Semestralmente	Área TIC	Numero de requerimientos técnicos reformulados	TIC
AL-04: Cambiar el alcance de los requerimientos del sistema de información debido a que el equipo de trabajo define su propio alcance	Seguimiento de los desarrollos y de la implementación de la arquitectura de las aplicaciones web enmarcado en metodologías de desarrollo rápido	Preventivo				Mitigar	Establecer el nivel de funcionalidades atendidas sin ajustes en la arquitectura del sistema de información	Semestralmente	Área TIC	Numero de requerimientos técnicos atendidos por funcionalidad requerida	TIC
AL-05: Formular y estimar requerimientos técnicos o funcionales equivocados	evaluar la calidad de la formulación de los requerimientos de publicación	Preventivo				Mitigar	establecer el nivel de calidad de la formulación de los	Semestralmente	Área TIC	Numero de requerimientos de servicios de información	TIC

	de servicios de información de la entidad						requerimientos			atendidos	
AL-06: No realizar las actividades programadas en cumplimiento de los planes de desarrollo de las aplicaciones web	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Reactivo				Mitigar	Establecer acciones de mejora en el proceso de desarrollo de los SI	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
AL-07: Definir de manera no adecuada los requerimientos de integración entre las aplicaciones web de la entidad	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Reactivo				Mitigar	Establecer acciones de mejora en el proceso de desarrollo de los SI	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
AL-08: Implementar requerimientos de seguridad no autorizados en la adquisición, desarrollo, implementación y uso de las aplicaciones web	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Reactivo			0	Mitigar	Establecer acciones de mejora en procesos de desarrollo de los SI	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
AL-09: Automatizar y fortalecer procesos de la entidad con el apoyo de la implementación de aplicaciones web misional.	Verificar el alcance de las aplicaciones web de acuerdo con los lieneamientos de la arquitectura institucional	Preventivo				Mitigar	Establecer acciones de mejora en procesos de desarrollo de los SI	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
ES-01: Perder la integración de los componentes de la estrategia con la arquitectura empresarial y el direccionamiento estratégico de la Entidad	Verificar el alcance de las aplicaciones web de acuerdo con los lineamientos de la arquitectura institucional	Preventivo				Mitigar	Identificar los requerimientos que amplían el alcance de las aplicaciones web	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC

ES-02: Duplicar la funcionalidad de las aplicaciones web en los desarrollos.	Verificar el alcance de las aplicaciones web de acuerdo con los lineamientos de la arquitectura institucional	Preventivo				Mitigar	Identificar los requerimientos que amplían el alcance de las aplicaciones web	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
ES-03: Perder la integración de procesos o procedimientos de la Entidad	Verificar el alcance de las aplicaciones web de acuerdo con los lineamientos de la arquitectura institucional	Preventivo				Mitigar	Identificar los requerimientos que amplían el alcance de las aplicaciones web	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
ES-04: Generar políticas de seguridad de la información no alineadas para la publicación e intercambio de información.	Verificar el alcance de las aplicaciones web de acuerdo con los lineamientos de la arquitectura institucional	Preventivo				Mitigar	Identificar los requerimientos que amplían el alcance de las aplicaciones web	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
ES-05: Perder la vigencia de gestión de riesgos de la publicación de servicios de información en el ciberespacio.	Verificar el alcance de las aplicaciones web de acuerdo con los lineamientos de la arquitectura institucional	Preventivo				Mitigar	Identificar los requerimientos que amplían el alcance de las aplicaciones web	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
ES-06: Fortalecer el sistema de calidad implantado	Verificar el alcance de las aplicaciones web de acuerdo con los lineamientos de la arquitectura institucional	Preventivo				Mitigar	Unificación de requerimientos que amplían el alcance de las aplicaciones web	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
PR-01: Retrasar la ejecución del cronograma del proyecto de desarrollo de aplicaciones web	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Preventivo				Mitigar	Auditoria en la formulación y ejecución de los planes de desarrollo de las	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC

							aplicaciones web que soportan solo servicios de información				
PR-02: Priorizar de manera no planeada o equivocada de la atención de requerimientos de desarrollo de aplicaciones web.	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Preventivo				Mitigar	Auditoria en la formulación y ejecución de los planes de desarrollo de las aplicaciones web que soportan solo servicios de información	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
PR-03: Interrumpir o desviar las actividades del proyecto de desarrollo de sistemas de infomación	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Preventivo				Mitigar	Auditoria en la formulación y ejecución de los planes de desarrollo de las aplicaciones web que soportan solo servicios de información	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
PR-04:Generar reprocesos y sobrecostos en la ejecución del proyecto de desarrollo de aplicaciones web.	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Preventivo				Mitigar	Auditoria en la formulación y ejecución de los planes de desarrollo de las aplicaciones web que soportan solo servicios de información	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
PR-05: Perder disponibilidad de los componentes de las aplicaciones web	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Preventivo				Mitigar	Auditoria en la formulación y ejecución de los planes de desarrollo de las	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC

							aplicaciones web que soportan solo servicios de información				
PR-06: Contar con recursos propios para el desarrollo de aplicaciones web críticos para la entidad.	Realizar auditorías periódicas al proceso de desarrollo e implementación de aplicaciones web	Preventivo				Mitigar	Auditoria en la formulación y ejecución de los planes de desarrollo de las aplicaciones web que soportan solo servicios de información	Semestralmente	Área TIC	Numero de hallazgos realizados por auditoria	TIC
A0: Perder funcionamiento de las aplicaciones web.	Generar reporte trimestral de la auditoria registrada en la herramienta control de versiones. Generar reporte trimestral de la gestión de requerimientos por cada uno de los sistema de información desarrollado en la Subtics Generar reporte de los pasos a producción por cada uno de los sistema de información desarrollados internamente en la Subtics	Preventivo				ASUMIR EL RIESGO	Actualizar el código fuente de las aplicaciones desarrolladas en la Subtics de la herramienta control de versiones. Registrar la gestión de desarrollo y pruebas en la herramienta de seguimiento de la atención de requerimientos Registrar los cambios de código fuente de las aplicaciones web desarrollad	trimestral	Área TIC	Reportes generados	TIC

							os en la en la Subtics en el momento del paso a producción en la herramienta de seguimiento de atención de requerimientos					
A0.Operar con una arquitectura de aplicaciones web desactualizada	1. Revisar la infraestructura informática que soportan los servicios a nivel nacional	Preventivo				REDUCIR EL RIESGO	Monitorear la capacidad de la infraestructura	Semestralmente	Área TIC	Informes generados	TIC
A1: 2017: Perder integridad de los servicios de información en el ciberespacio.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentar y realizar seguimiento de la implementación de nuevos servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC

A2: Perder confidencialidad en la autenticación de las aplicaciones web.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentar y realizar seguimiento de la implementación de nuevos servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
A3: exponer datos sensibles.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Auditorias de publicación de servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
A4: explotar vulnerabilidades de procesadores XML por parte de entidades externas XML (XXE).	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	evaluación de la calidad de los servicios de información publicados en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC

A5: Perder el Control de Acceso como producto de los ataques de explotación de la falta de controles.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Valoración de la efectividad de las incidencias de seguridad detectadas en los servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
A6: Configurar controles de Seguridad de manera incorrecta.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Valoración de la efectividad de las incidencias de seguridad detectadas en los servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
A7: Explotar comandos del navegador por medio de Cross – Site Scripting (XSS),.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Valoración de la efectividad de las incidencias de seguridad detectadas en los servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC

A8: Permitir la deserialización Insegura afectadon el comportamiento fucnional del sistema de información.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Valoración de la efectividad de las incidencias de seguridad detectadas en los servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
A9: Usar componentes con vulnerabilidades conocidas.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Valoración de la efectividad de las incidencias de seguridad detectadas en los servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
A10: Realizar registro y monitoreo insuficientes en el sistema de información.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Valoración de la efectividad de las incidencias de seguridad detectadas en los servicios de información en el ciberespacio	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-01: Perder la escalabilidad de los componentes de desarrollo de aplicaciones web	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-02: Perdida de aplicabilidad del modelo de seguridad en	realizar análisis de vulnerabilidades en las diferentes	Preventivo				Mitigar	Documentación de la gestión de incidencias	trimestral	Área TIC	resultado del análisis de	TIC

el ciclo de vida de las aplicaciones web de la Entidad	etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio						de seguridad detectadas en el SOC de la Entidad			vulnerabilidades		
TE-03: Implementar componentes de las aplicaciones web con vulnerabilidades de seguridad	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades		TIC
TE-04: Implementar aplicaciones web con controles innecesarios	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades		TIC
TE-05 – Permitir Inyección de código en las aplicaciones web que soportan los servicios de información en el ciberespacio	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades		TIC
TE-06 – Perder la autenticación y gestión de Sesiones	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades		TIC

	en el ciberespacio										
TE-07 – Pemitir la Secuencia de comandos en sitios cruzados (XSS)	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-08 – Permitir la Referencia Directa Insegura a Objetos de in sistema de información.	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-09 – Permitir la Configuración de Seguridad Incorrecta	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-10 – Perder de información por exposición de Datos Sensibles	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC

TE-11 – Implementar aplicaciones web con ausencia de Control de Acceso a las Funciones	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-12 – Permitir la Falsificación de peticiones en sitios Cruzados (CSRF)	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo			0	Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-13 – Usar de Componentes con Vulnerabilidades Conocidas	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-14– Permitir las redirecciones y reenvíos no validados	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC
TE-15: Implementar aplicaciones web con componentes que no tiene estabilidad	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC

	aplicaciones web que soportan los servicios de información en el ciberespacio						en el SOC de la Entidad					
TE-16: Reutilizar componenent es de software estándar y seguros	realizar análisis de vulnerabilidades en las diferentes etapas de desarrollo de las aplicaciones web que soportan los servicios de información en el ciberespacio	Preventivo				Mitigar	Documentación de la gestión de incidencias de seguridad detectadas en el SOC de la Entidad	trimestral	Área TIC	resultado del análisis de vulnerabilidades	TIC

Anexo 2. Aspectos normativos y legales.

En ámbito Internacional y conforme con lo expuesto en el CONPES 3701 de 2011, se señalan aspectos técnicos en materia de "Seguridad Cibernética", como lo son:

Convenio o tratado	Objetivo	Aplicabilidad en Aplicaciones web	Capacidad de implementar en el ámbito colombiano.
Ciberdelincuencia del Consejo de Europa – CCC (conocido como el convenio sobre Cibercriminalidad de Budapest)	Busca dotar de un marco legislativo internacional para la prevención de conductas delictivas en el ciberespacio	Dotar de los componentes que permita detectar, investigar y preservar pruebas de conductas delictivas.	Desarrollo de norma para prevenir la delincuencia en el diseño, construcción, implementación y uso de aplicaciones web con fines delictivos.
Resolución AG /RES 2004 (XXXIVO/04) de la Asamblea General de la Organización de los Estados Americanos.	Estrategia Integral para combatir las amenazas a la seguridad cibernética.	Interacción con Equipos Nacionales de Respuesta a Incidentes de Seguridad De Computadores – CSIRT. Aplicación de normas técnicas en materia de desarrollo de software. Implementación de arquitecturas de aplicaciones web seguras.	Creación de una cultura de la seguridad cibernética en el desarrollo de Aplicaciones web en la Entidades del Gobierno. Creación de instrumentos jurídicos para proteger los usuarios de las aplicaciones web.
Decisión 587 de la Comunidad Andina.	Establece los lineamientos de la Política de Seguridad Externa Común Andina	Contemplar los mecanismos para la prevención, enfrentamiento y reducción de las amenazas a la seguridad en las aplicaciones web en la Comunidad Andina.	Contar con leyes o normas comunitarias en materia de Aplicaciones web.
Unión Internacional de Telecomunicaciones - UIT, en las Naciones Unidas	Revisión de conceptos internacionales para el fortalecimiento de la seguridad de los sistemas mundiales de información y telecomunicaciones.	Cumplir con los lineamientos de se seguridad de Información.	Leyes 252/1995 y 873, 2005/2004 de sociedad de la información.
Resolución 64/25, Asamblea General de las Naciones Unidas (UNGA).	"Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional"	Contribuir y aplicar los resultados de análisis de amenazas reales y potenciales en el ámbito de la seguridad de la información.	Permitir el libre flujo de información de manera segura.
Resoluciones de la Asamblea General de la ONU	Lineamientos de aplicación financiera y de asuntos internos.	Ajustar la infraestructura de las aplicaciones web al entorno internacional.	Determinar lineamientos de diseño de aplicaciones web acorde con la realidad económica de la región.

Directiva 2006/24 de la Unión Europea	Conservación de datos en la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones	Incorporación de componentes de protección de datos en las aplicaciones web.	Dado que fue declarada invalida en cuanto a la privacidad, las aplicaciones web deben contemplar mecanismos de protección de datos para garantizar el cumplimiento de este derecho fundamental.
Resoluciones UNGA: 55/63 y 56/121	Prevenir el uso delictivo de las tecnologías de la información.	Aplicar criterios y lineamientos de protección de aplicaciones web en la Entidad.	Políticas de protección de infraestructuras criticas de información.
Cumbre Mundial sobre la Sociedad de la Información (CMSI).	Normas y reglas generales, como instrumentos jurídicos en el sistema de fuentes del Derecho Internacional.	Cumplimiento de recomendaciones a implementar en las aplicaciones web.	Políticas de protección de infraestructuras criticas de información.

En cuanto a la normatividad interna nacional.

Norma	*Objeto*	*Reformas*
Decreto 2573 de 2014	Se establecen los lineamientos generales de la Estrategia de Gobierno en línea.	
Ley 44 de 1993	Especifica penas entre dos y cinco años de cárcel, así como el pago de indemnizaciones por daños y perjuicios a quienes comentan el delito de piratería de software.	
Ley 11723:	"Ley de Propiedad Intelectual" o también como "Ley de Propiedad Científica, Literaria y Artística".	Noviembre de 1998, cuando por Ley 25036 se le introdujeron modificaciones referidas al software, para darle fin a las discusiones doctrinarias y jurisprudenciales sobre la cuestión de si el software estaba o no bajo el amparo de esta ley. Ahora establece expresamente en su Art. 1 que "... las obras científicas, literarias y artísticas comprenden los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales, ..." y en su art. 55 bis que "La explotación de la propiedad intelectual sobre los programas de computación incluirá entre otras formas los contratos de licencia para su uso o reproducción".
Artículo 15 de la Constitución Política	Derecho de todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.	
Artículo 74 de la Constitución	Garantiza que todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la	

Política	ley.	
Ley estatutaria 1581 de 2012	Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política. El derecho a la información consagrado en el artículo 20 de la misma. Artículo 2. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente ley aplicará al Tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del tratamiento o encargado del tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.	
Ley No 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.	
Constitución Política de Colombia	Artículos 209 de la Constitución Política. Artículo 3° de la Ley 489 de 1998. Artículo 3° de la Ley 1437 de 2011	
Decreto 2693 de 2012,	"por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia..."	El Estado garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones, y garantizar la libre y leal competencia y que su adopción sea armónica con el desarrollo ambiental sostenible.
Resolución CRC 3067 de 2011	Principios de confidencialidad, protección de los datos personales, inviolabilidad de las comunicaciones, seguridad de la información y prevención de fraudes	
CONPES 3701 de 2011	a estrategia del Gobierno Nacional y la Fuerza Pública, en materia de Ciberseguridad y Ciberdefensa	
Ley 1273 del 5 de Enero de 2009"	Ley de Delitos Informáticos, establece: Artículo 269A: Acceso abusivo a un sistema. Artículo 269B: Obstaculización	

	ilegítima de sistema informático o red de telecomunicación Artículo 269C: Interceptación de datos informáticos. Artículo 269D: Daño Informático. Artículo 269E: Uso de software malicioso. Artículo 269F: Violación de datos personales. Artículo 269G: Suplantación de sitios web para capturar datos personales. Artículo 269H: Circunstancias de agravación punitiva. Artículo 269I: Hurto por medios informáticos y semejantes. Artículo 269J: Transferencia no consentida de activos.	

Anexo No 3. Diseño de Cuestionarios.

Por otro lado, para la formulación de la estrategia se basa en los estándares de verificación de seguridad para aplicaciones 3.0 emitidas por (Open Web Application Security Project, 2015), para el software y aplicaciones críticas en cuatro niveles:

Nivel	Formulación	Detalle	Aplicabilidad
1	Oportunista.	Se cuenta con componentes identificados y tienen una razón para ser parte de la aplicación.	Para todo el software
2	Estándar.	La arquitectura está bien definida y el código está alineado con la arquitectura.	Para aplicaciones que contiene datos sensibles que requieren protección.
3	Avanzado.	La arquitectura y diseño está definida, en uso y es efectiva.	Para aplicaciones críticas que soportan un alto valor en las transacciones y la credibilidad.

Tabla 7: Niveles del estándar OWASP 3.0 para la seguridad de aplicaciones

- Arquitectura, diseño y modelamiento de amenazas:

Número	Descripción	1	2	3
1.1.	Verifique que todos los componentes de la aplicación estén identificados y se conoce que son necesarios.		X	
1.2.	Verifique la identificación de todos los componentes que no son parte de la aplicación pero que necesita para operar, tales como librerías, módulos y sistemas externos.		X	
1.3.	Verifique la definición y existencia de una arquitectura de alto nivel para la aplicación.		X	
1.4.	Verifique la definición y disponibilidad de todos los componentes de la aplicación en términos de las funciones de negocios y / o funciones de seguridad.	X		
1.5.	Verifique la disponibilidad de todos los componentes que no son parte de la aplicación, pero necesarios para su operación se definen en términos de funciones, y / o funcionalidad de seguridad.		X	
1.6.	Verifique que en el marco del objetivo de la aplicación se cuente con un modelo de amenazas para gestionar los riesgos asociados al Spoofing, manipulación, repudio, información, divulgación, denegación de servicio y elevación de privilegios (STRIDE).		X	
1.7.	Verifique la implementación de todos los controles de seguridad (incluidas las librerías que hacen llamados a servicios de seguridad externa).		X	
1.8.	Verificar que los componentes estén separados unos de otros a través de un control de seguridad definido, como la segmentación de red, reglas de firewall o en la nube basada en grupos de seguridad.		X	
1.9.	Verifique que la aplicación tenga una separación clara entre capas de datos, controlador y visualización (Modelo, Vista y Controlador), de modo que las decisiones de seguridad contribuyan a obtener sistemas confiables.		X	
1.10.	Verifique que no exista en el código de la cliente lógica empresarial sensible, claves secretas u otra información propietaria.		X	
1.11.	Verifique que todos los componentes de la aplicación estén libres		X	

	de vulnerabilidades como librerías, módulos, marcos de desarrollo, plataformas y sistemas operativos.			

- Requerimientos de verificación de autenticación.

Número	Descripción	1	2	3
2.1.	Verifique que todas las páginas y recursos cargados por defecto requieran autenticación, excepto aquellos específicamente destinados a ser públicos (Principio de mediación completa).		X	
2.2.	Verifique que los formularios que contienen credenciales no sean rellenados por la aplicación, esto implica que las credenciales se almacenan en texto plano o en formato reversible. Lo que está explícitamente prohibido.	X		
2.4.	Verifique que todos los controles de autenticación se apliquen en el lado del servidor.	X		
2.6.	Verifique que todos fallos de autenticación sean controlados de manera segura para garantizar que los atacantes no pueden iniciar sesión.	X		
2.7.	Verifique que los campos de entrada de contraseña permitan o fomenten el uso de frases de contraseña, y permitan a los administradores de contraseñas el ingreso de frases largas o contraseñas altamente complejas.	X		
2.8	Verifique que todas cuentas identificadas cuenten con funciones como la actualización de perfil, contraseña olvidada, token deshabilitado / perdido, mesa de ayuda o IVR).	X		
2.9.	Verifique que la funcionalidad de cambio de contraseña incluya control de la contraseña anterior, de la nueva contraseña y una contraseña confirmación.		X	
2.12.	Verifique que todas las decisiones de autenticación puedan ser registradas en log, sin almacenar identificadores de sesión sensibles o contraseñas, es decir, se debe incluir solicitudes con metadatos relevantes necesario para investigaciones de seguridad.		X	
2.13.	Verifique que las contraseñas de las cuentas cuenten con un hash para mitigar los ataques de fuerza bruta o ataques de recuperación de hash y contraseña.	X		
2.16.	Verifique que las credenciales sean transportadas por medio de enlaces cifrado y que todas las páginas o funciones que requieren credenciales de usuario se realicen por medio de enlaces cifrados.		X	
2.17.	Verifique que la funcionalidad de la contraseña olvidada y otros mecanismos de recuperación no revelan la contraseña actual y que la nueva contraseña no se envía en texto claro.		X	
2.18.	Verificar que la enumeración de la información no es posible realizarla a través de inicio de sesión, restablecimiento de contraseña, o de la funcionalidad de olvidó de la cuenta.	X		
2.19.	Verifique que no haya contraseñas predeterminadas en uso en la aplicación o en cualquier componente (como "admin / password").	X		
2.20.	Verifique que no haya automatización para prevenir ataques de violación de credenciales, ataques de fuerza bruta y bloqueo de cuentas.	X		
2.21.	Verifique que todas las credenciales de autenticación de acceso a servicios externos de la aplicación estén encriptados y almacenados en un lugar protegido.		X	
2.22.	Verifique que la funcionalidad de contraseña olvidada y otros medios de recuperación use un TOTP u otro token de software o mecanismos de recuperación fuera de línea por medio de dispositivo móvil. El uso de un valor aleatorio en un correo electrónico o SMS debe ser un último recurso.	X		
2.23.	Verifique que el bloqueo de la cuenta está dividido en estados de bloqueo suave y difícil, (no son mutuamente excluyentes). Si una cuenta es objeto de un ataque de fuerza bruta, está debe ser bloqueada temporalmente y no debería restablecerse con estado de bloqueo duro.		X	
2.24.	Verifique la obligatoriedad de las preguntas de seguridad basadas	X		

	en el conocimiento compartido (también conocidas como "preguntas secretas"), estas preguntas no deben violar las leyes de privacidad y deben ser lo suficientemente fuertes como para proteger las cuentas de un ataque de recuperación maliciosa.			
2.25.	Verifique que el sistema pueda configurarse para que controle un número de uso de contraseñas anteriores.		X	
2.26.	Verifique los controles de riesgo para las transacciones de alto valor frente a una re-autenticación, autenticación dos factores o la firma de transacción.		X	
2.27.	Verificar que existen medidas para bloquear el uso de contraseñas que son comúnmente elegidas y frases de paso débiles.		X	
2.28.	Verifique que, en la autenticación, ya sea exitosa o fallida, debe responder en el mismo promedio tiempo de respuesta.		X	
2.29.	Verifique que los secretos, claves de API y contraseñas no estén en el código fuente, o en repositorios en línea de código fuente.		X	
2.31.	Verifique que, si una aplicación permite a los usuarios autenticarse, se realice con autenticación de dos factores o mecanismos de autenticación fuerte, o cualquier esquema similar que proporciona protección contra la revelación de nombre de usuario y contraseña.		X	
2.32.	Verificar que las interfaces administrativas no sean accesibles para aspectos no confiables.		X	
2.33.	Permitir las opciones de autocompletar en el navegador, e integración con los gestores de contraseña a menos que estén prohibidos por la política de seguridad basada en riesgo.		X	

2.5.3. Requerimientos de verificación de administración de sesiones.

Número	Descripción	1	2	3
3.1.	Verifique que no haya un administrador de sesión personalizado, o que el administrador de sesiones personalizado sea el que resista todos los ataques comunes de gestión de sesión.	X		
3.2.	Verifique que las sesiones se invaliden cuando el usuario sale del sistema.		X	
3.3.	Verifique que las sesiones terminen después de un período específico de inactividad.	X		
3.4.	Verifique que las sesiones terminen después de un período de tiempo máximo el cual debe ser configurable administrativamente independientemente de actividad (un tiempo de espera absoluto).	X		
3.5.	Verifique que todas las páginas que requieren autenticación tengan acceso fácil y visible a la funcionalidad de cierre de sesión.	X		
3.6.	Verifique que el ID de sesión nunca se muestre en las URL, mensajes de error, o registros. Esto incluye verificar que la aplicación no permita la reescritura de URL de la sesión.	X		
3.7.	Verifique que toda autenticación exitosa y re-autenticación generen una nueva sesión y un ID de sesión.		X	
3.10	Verifique que solo los identificadores de sesión generados por la aplicación son reconocidos como activos.	X		
3.11.	Verifique que los ID de sesión sean suficientemente largos, aleatorios y que se basen en la sesión activa correcta.		X	
3.12.	Verifique que los ID de sesión almacenados en las cookies tengan su ruta establecida en un valor apropiadamente restrictivo para la aplicación y con tokens de sesiones de autenticación y aplicación. Además, establezca los atributos "HttpOnly" y "seguro"	X		
3.16.	Verifique que la aplicación limite el número de sesiones concurrentes activas.		X	
3.17.	Verifique que se muestre una lista de sesión activa en el perfil de cuenta o similar para cada usuario. El usuario debe ser capaz de	X		

	terminar cualquier sesión activa.			
3.18.	Verifique que se le solicite al usuario la opción de terminar todas las demás sesiones activas después de un proceso exitoso de cambio de contraseña		X	

2.5.4. Requerimientos de verificación de control de acceso.

Número	Descripción	1	2	3
4.1.	Verifique que exista el principio de privilegio mínimo de usuarios para solo acceder a funciones, archivos de datos, URL, controladores, servicios y otros recursos, para los cual debe contar con la autorización específica. Esto implica protección contra la falsificación y la elevación de privilegios.		X	
4.4.	Verifique que el acceso a registros confidenciales esté protegido para el acceso de los objetos o datos autorizados por cada usuario (por ejemplo, proteger contra usuarios que manipulan un parámetro para ver o alterar la cuenta de otro usuario).		X	
4.5.	Verifique que la navegación del directorio esté deshabilitada a menos que se requiera. Además, las aplicaciones no deben permitir el descubrimiento o divulgación de metadatos de archivos o directorios, como las carpetas Thumbs.db, .DS_Store, .git o .svn.	X		
4.8.	Verifique que las fallas de los controles de acceso sean administradas de manera segura.		X	
4.9.	Verificar el cumplimiento al lado del servidor de las mismas reglas de control de acceso implícitas en el capa de presentación.		X	
4.10.	Verifique que todos los usuarios, atributos de datos y políticas de la información aplicables en los controles de acceso no sean manipulados por usuarios finales a menos que esté específicamente autorizado.		X	
4.11.	Verificar que exista un mecanismo centralizado (incluyendo librerías que llaman a servicios de autorización externa) para proteger el acceso a cada tipo de recurso protegido.		X	
4.12.	Verifique que se registre en log todas las decisiones de control de acceso y todas las decisiones.		X	
4.13.	Verifique que la aplicación o framework use fuerte tokens anti-CSRF aleatorios o tiene otra transacción Mecanismo de protección.		X	
4.14.	Verifique que el sistema pueda proteger contra agregados o Acceso continuo de funciones seguras, recursos, o datos. Por ejemplo, considere el uso de un recurso gobernador para limitar el número de ediciones por hora o para evitar que toda la base de datos sea raspada por una Usuario individual.		X	
4.15.	Verifique que la aplicación tenga autorización adicional (tal como paso a paso o autenticación adaptativa) para menor valor Sistemas, y / o segregación de funciones por alto valor para aplicaciones con los controles antifraude según el riesgo de la aplicación y de fraude pasado.		XX	
4.16.	Verifique que la aplicación aplique correctamente la autorización sensible al contexto para no permitir la autorización no autorizada. Manipulación mediante manipulación de parámetros.		X	

2.5.5. Requerimientos de verificación de manejo de entradas maliciosas.

2.5.6. Codificación de salidas y escape.

Número	Descripción	1	2	3
5.1.	Verifique que el entorno de ejecución no sea susceptible a desbordamientos de búfer, o que los controles de seguridad evitan el búfer desbordes	X		
5.3.	Verificar que los errores de validación de entrada del lado del	X		

	servidor resulten Solicitar el rechazo y se registran.			
5.5.	Verifique que las rutinas de validación de entrada se apliquen en el lado del servidor.	X		
5.6.	Verifique que un control de validación de entrada único sea utilizado por la solicitud para cada tipo de datos que se acepte.		X	
5.10.	Verifique que todas las consultas SQL, HQL, OSQL, NOSQL y procedimientos almacenados sean la llamada de los procedimientos almacenados están protegidos por la uso de declaraciones preparadas o parametrización de consultas, y por lo tanto no es susceptible a la inyección de SQL		X	
5.11.	Verifique que la aplicación no sea susceptible a la inyección LDAP, o que los controles de seguridad impidan la inyección LDAP.		X	
5.12.	Verifique que la aplicación no sea susceptible al Comando OS Inyección, o que los controles de seguridad impiden el Comando OS. Inyección		X	
5.13.	Verifique que la aplicación no sea susceptible al archivo remoto. Inclusión (RFI) o inclusión de archivos locales (LFI) cuando se usa contenido eso es una ruta a un archivo.		X	
5.14.	Verifique que la aplicación no sea susceptible a XML común ataques, como la manipulación de consultas XPath, XML External Entity. Los ataques, y los ataques de inyección XML.		X	
5.15.	Asegúrese de que todas las variables de cadena colocadas en HTML u otra web el código del cliente se codifica adecuadamente de forma manual, o utilizar plantillas que automáticamente codifican contextualmente para asegurar que la aplicación no sea susceptible de reflejarse, almacenarse. y los ataques de secuencias de comandos de sitios cruzados (XSS) de DOM.	X		
5.16.	Si el marco de aplicación permite la masa automática. asignación de parámetros (también llamada vinculación automática de variables) desde la solicitud de entrada a un modelo, verifique que la seguridad campos sensibles como "balance de cuentas", "rol" o Las "contraseñas" están protegidas contra el enlace automático malicioso.		X	
5.17.	Verifica que la aplicación tenga defensas contra HTTP. Parámetros de ataques de contaminación, particularmente si la aplicación no hace distinción sobre la fuente de la solicitud. parámetros (GET, POST, cookies, encabezados, entorno, etc.)		X	
5.18	Verifique que la validación del lado del cliente se usa como una segunda línea de defensa, además de la validación del lado del servidor.	X		
5.19.	Verifique que todos los datos de entrada estén validados, no solo el formulario HTML campos, pero todas las fuentes de entrada, tales como llamadas REST, consulta parámetros, encabezados HTTP, cookies, archivos por lotes, fuentes RSS, etc; usando validación positiva (lista blanca), luego formas menores de validación como greylisting (eliminando las malas cadenas conocidas), o rechazar entradas erróneas (listas negras).		X	
5.20.	Verificar que los datos estructurados estén fuertemente tipados y validados contra un esquema definido que incluye caracteres permitidos, longitud y patrón (por ejemplo, números de tarjeta de crédito o teléfono, o validando que dos campos relacionados son razonables, tales como validación de suburbios y zip o códigos postales coinciden).		X	
5.21.	Verifique que los datos no estructurados estén desinfectados para aplicar genéricos medidas de seguridad tales como caracteres permitidos y longitud, y Los caracteres potencialmente dañinos en un contexto dado deben ser escapado (por ejemplo, nombres naturales con Unicode o apóstrofes,como ねこ o O'Hara)		X	
5.22.	Asegúrate de que no haya confianza en el HTML de los editores WYSIWYG o similar están correctamente desinfectados con un		X	

	desinfectante HTML y manejarlo apropiadamente de acuerdo con la tarea de validación de entrada y tarea de codificación.			
5.23.	Para la tecnología de plantillas de escape automático, si el escape de IU es deshabilitado, asegúrese de que el saneamiento de HTML está habilitado en su lugar.		X	
5.24.	Verifique que los datos transferidos desde un contexto DOM a otro, utiliza métodos de JavaScript seguros, como usar .innerText y .val.		X	
5.25.	Verifique cuando se analiza JSON en los navegadores, que se utiliza JSON.parse para analizar JSON en el cliente. No use eval () para analizar JSON en el cliente.		X	
5.26.	Verifique que los datos autenticados se borran del almacenamiento del cliente, tal como el navegador DOM, después de la sesión se termina.		X	

2.5.7. Requerimientos de verificación de criptografía.

Número	Descripción	1	2	3
7.2.	Verifique que todos los módulos criptográficos fallan de forma segura, y los errores se manejan de una manera que no habilitar el relleno oracle.	X		
7.6.	Verifique que todos los números aleatorios, archivo aleatorio Los nombres, GUID aleatorios y cadenas aleatorias son generado utilizando el módulo criptográfico generador de números aleatorios aprobado cuando esto pretende que los valores aleatorios no sean adivinables. por un atacante.		X	
7.7.	Verificar que los algoritmos criptográficos utilizados por la La aplicación ha sido validada contra FIPS 140-2 o un estándar equivalente.	X		
7.8.	Verificar que los módulos criptográficos operan en su Modalidad aprobada según su publicación. Políticas de seguridad.	X		
7.9.	Verifique que exista una política explícita sobre cómo Las claves criptográficas se administran (por ejemplo, generadas, distribuido, revocado, y vencido). Verificar que esto ciclo de vida de la clave se aplica correctamente.	X		
7.11.	Verificar que todos los consumidores de servicios criptográficos No tienen acceso directo a material clave. Aislar Procesos criptográficos, incluyendo secretos maestros y considerar el uso de un virtualizado o físico. bóveda de llave de hardware (HSM).	X		
7.12.	La información de identificación personal debe ser encriptados almacenados en reposo y garantizar que la comunicación se realiza a través de canales protegidos.	X		
7.13.	Verifique que las contraseñas sensibles o material clave mantenido en la memoria se sobrescribe con ceros como tan pronto como ya no sea necesario, para mitigar la memoria. ataques de dumping.	X		
7.14.	Verifique que todas las claves y contraseñas sean reemplazables, y son generados o reemplazados en el momento de la instalación.	X		
7.15.	Verifique que los números aleatorios se crean con entropía adecuada incluso cuando la aplicación está bajo Carga pesada, o que la aplicación degrada con gracia en tales circunstancias.	X		

3.5.8. Requerimientos de verificación de entrada y manejo de error.

Número	Descripción	1	2	3
8.1.	Verifique que la aplicación no genere error.		X	

	Mensajes o seguimientos de pila que contienen datos confidenciales que podría ayudar a un atacante, incluyendo ID de sesión, versiones de software / framework y personal. Información			
8.2.	Verificar que la lógica de manejo de errores en los controles de seguridad niega el acceso por defecto.		X	
8.3.	Verifique que los controles de registro de seguridad proporcionen la capacidad para registrar eventos exitosos y particularmente fallos que Se identifican como relevantes para la seguridad.		X	
8.4.	Verifique que cada evento de registro incluya necesaria información que permitiría una detallada investigación de la línea de tiempo cuando un evento pasa		X	
8.5.	Verifique que todos los eventos que incluyen datos no confiables no se ejecutarán como código en el registro previsto software de visualización.	X		
8.6.	Verifique que los registros de seguridad estén protegidos acceso y modificación no autorizados.		X	
8.7.	Verifique que la aplicación no registre datos confidenciales datos como se define en las leyes de privacidad locales o reglamentos, datos sensibles a la organización como definido por una evaluación de riesgos, o sensible Datos de autenticación que podrían ayudar a un atacante, incluyendo identificadores de sesión del usuario, contraseñas, hashes, o tokens API.	X		
8.8.	Verifique que todos los símbolos y campos no imprimibles separadores están correctamente codificados en las entradas de registro, para prevenir la inyección de troncos.		X	
8.9.	Verifique que los campos de registro sean confiables y no confiables Las fuentes son distinguibles en las entradas de registro.		X	
8.10.	Verifique que un registro de auditoría o similar permita no rechazar las transacciones clave.		X	
8.11.	Verifique que los registros de seguridad tengan alguna forma de controles de integridad o controles para prevenir modificación no autorizada.		X	
8.12.	Verifique que los registros estén almacenados en un lugar diferente partición que la aplicación se está ejecutando con Rotación de registro adecuada.		X	
8.13.	Las fuentes de tiempo deben estar sincronizadas para asegurar los registros tienen la hora correcta		X	

2.5.9. Requerimientos de verificación de protección de datos.

Número	Descripción	1	2	3
9.1.	Verifique que todos los formularios que contienen información sensible ha deshabilitado el almacenamiento en caché del lado del cliente, incluido el autocompletado características.		X	
9.2.	Verifique que la lista de datos confidenciales procesados por el Se identifica la aplicación, y que hay una explícita Política de cómo controlar el acceso a estos datos. Encriptado y aplicado bajo protección de datos relevantes Directivas		X	
9.3.	Verifique que todos los datos confidenciales se envíen al servidor en el cuerpo del mensaje HTTP o encabezados (es decir, los parámetros de URL son nunca utilizado para enviar datos sensibles).	X		
9.4	Verifique que la aplicación establezca un anti-caching apropiado encabezados según el riesgo de la aplicación, como el siguiendo: Fecha de vencimiento: martes, 03 de julio de 2001 06:00:00 GMT Última modificación: {ahora} GMT Control de caché: no-store, no-cache, mustrevalidate, max-age = 0 Control de caché: post-check = 0, pre-check = 0 Pragma: no-caché		X	
9.5	Verifique que en el servidor, todas las copias en caché o temporales		X	

	de datos confidenciales almacenados están protegidos de no autorizados Acceso o purgado / invalidado después del usuario autorizado. Accede a los datos sensibles.			
9.6	Verifique que exista un método para eliminar cada tipo de Los datos sensibles de la aplicación al final de la política de retención requerida.	X		
9.7	Verifique que la aplicación minimice el número de parámetros en una solicitud, como campos ocultos, Ajax Variables, cookies y valores de cabecera.		X	
9.8.	Verifica que la aplicación tenga la capacidad de detectar y alertar en números anormales de solicitudes de recolección de datos para Un ejemplo de pantalla de raspado.		X	
9.9.	Verifique que los datos almacenados en el almacenamiento del lado del cliente (como Almacenamiento local HTML5, almacenamiento de sesión, IndexedDB, regular cookies o Flash cookies) no contiene datos confidenciales o PII.		X	
9.10.	Verifique que el acceso a los datos confidenciales esté registrado, si los datos están recogidos bajo las directivas de protección de datos pertinentes o donde se requiere el registro de accesos.		X	
9.11.	Verifique que la información confidencial se mantenga en la memoria. se sobrescribe con ceros tan pronto como ya no sea necesario, para mitigar los ataques de volcado de memoria.		X	

2.5.10. Requerimientos de verificación de seguridad de las comunicaciones.

Número	Descripción	1	2	3
10.1	Verifique que se pueda construir una ruta desde una CA confiable a cada uno Certificado de servidor de Seguridad de la capa de transporte (TLS), y que Cada certificado de servidor es válido.		X	
10.3	Verifique que TLS se usa para todas las conexiones (incluyendo ambas Conexiones externas y backend) que son autenticadas. o que involucran datos o funciones sensibles, y no cae volver a los protocolos inseguros o no cifrados. Asegurar la La alternativa más fuerte es el algoritmo preferido.		X	
10.4	Verifique que las fallas de la conexión TLS del backend estén registradas.		X	
10.5	Verifique que las rutas de certificados estén construidas y verificadas para todos certificados de cliente utilizando anclajes de confianza configurados y información de revocación.		X	
10.6	Verifique que todas las conexiones a sistemas externos que involucren la información sensible o funciones son autenticadas.		X	
10.8.	Verifique que haya una sola implementación estándar de TLS que utiliza la aplicación que está configurada para operar En un modo de operación aprobado.		X	
10.10	Verifique que la fijación de la clave pública del certificado TLS (HPKP) sea implementado con claves públicas de producción y backup. Por más información, por favor, consulte las referencias a continuación.		X	
10.11.	Verifique que los encabezados de Seguridad de Transporte Estricto HTTP estén incluido en todas las solicitudes y para todos los subdominios, como Seguridad de transporte estricta: edad máxima = 15724800; incluirsubdominios		X	
10.12	Verifique que la URL del sitio web de producción se haya enviado a Lista precargada de dominios de seguridad de transporte estricto mantenido por los proveedores de navegadores web. Por favor vea el referencias a continuación.		X	
10.13.	Asegúrese de que los cifrados de secreto hacia adelante estén en uso para mitigar atacantes pasivos grabando el tráfico.		X	
10.14	Verifique que la revocación de certificación adecuada, como en		X	

	línea el protocolo de estado del certificado (OCSP), grapado, está habilitado Configurado			
10.15	Verifique que solo algoritmos, cifrados y protocolos sólidos Se utilizan, a través de toda la jerarquía de certificados, incluyendo certificados de raíz e intermediarios de sus seleccionados. autoridad certificadora		X	
10.16	Verifique que la configuración de TLS esté en línea con la dirección actual práctica, particularmente como configuraciones comunes, cifrados, y los algoritmos se vuelven inseguros.		X	

2.5.11. Requerimientos de verificación de configuración de seguridad http.

2.5.12. Requerimientos de verificación de configuración de seguridad.

Número	Descripción	1	2	3
11.1.	Verificar que la aplicación solo acepta un definido conjunto de métodos de solicitud HTTP requeridos, tales como se aceptan GET y POST, y métodos no utilizados (por ejemplo, TRACE, PUT y DELETE) están explícitamente obstruido.		X	
11.2	Verifique que cada respuesta HTTP contenga una encabezado de tipo de contenido que especifica un conjunto de caracteres seguro (por ejemplo, UTF-8, ISO 8859-1).		X	
11.3	Verifique que los encabezados HTTP agregados por un proxy de confianza o dispositivos SSO, como un token de portador, son Autenticado por la aplicación.		X	
11.4	Verifique que un encabezado X-FRAME-OPTIONS adecuado sea en uso para sitios donde el contenido no debe ser visto en un X-Frame de terceros.		X	
11.5	Verifique que los encabezados HTTP o cualquier parte de la respuesta HTTP no expone la versión detallada Información de componentes del sistema.		X	
11.6	Verifique que todas las respuestas de API contengan X-ContentType-Options: nosniff y Content-Disposition: adjunto archivo; filename = "api.json" (u otro nombre de archivo apropiado para el tipo de contenido).		X	
11.7.	Verifique que una política de seguridad de contenido (CSPv2) esté en lugar que ayuda a mitigar el DOM común, XSS, JSON, y las vulnerabilidades de inyección de JavaScript.		X	
11.8	Verifique que la protección X-XSS: 1; modo = bloque el encabezado está en su lugar para habilitar el navegador reflejado XSS filtros		X	

2.5.13. Requerimientos de verificación de control malicioso

2.5.14. Requerimientos de verificación seguridad interna.

Número	Descripción	1	2	3
13.1.	Verificar que toda actividad maliciosa sea adecuada. En caja de arena, en contenedores o aislados para retrasar y disuadir a los atacantes de atacar otras aplicaciones.	X		
13.2	Verifique que el código fuente de la aplicación, y como muchas bibliotecas de terceros como sea posible, no Contiene puertas traseras, huevos de Pascua, y fallas lógicas en Autenticación, control de acceso, validación de entrada, y la lógica de negocios de las transacciones de alto valor.		X	

2.5.15. Requerimientos de verificación de lógica de negocio.

Número	Descripción	1	2	3
15.1.	Verifica que la aplicación solo procese negocios. la lógica fluye en orden de pasos secuenciales, con todos los pasos siendo procesado en tiempo humano realista, y no proceso fuera de servicio, pasos omitidos, pasos de proceso de otro usuario, o enviado demasiado rápido actas.		X	
15.2	Verificar que la aplicación tiene límites de negocio y se aplica correctamente por usuario, con Alertas configurables y reacciones automatizadas a Ataque automatizado o inusual.		X	

2.5.16. Requerimientos de verificación de fuentes y archivos.

Número	Descripción	1	2	3
16.1.	Verifique que la URL redirecciona y reenvía solo lo que permite destinos en la lista blanca, o mostrar una advertencia cuando redirigir a contenido potencialmente no confiable.		X	
16.2	Verifique que los datos de archivos no confiables enviados a la aplicación no se usan directamente con el archivo I / O Comandos, particularmente para proteger contra el camino. Traversal, archivo local incluido, tipo de archivo mime y sistema operativo Vulnerabilidades de inyección de comando.		X	
16.3	Verificar que los archivos obtenidos de fuentes no confiables Se validan para ser del tipo esperado y se escanean por los antivirus para evitar la carga de conocidos contenido malicioso		X	
16.4	Verifique que los datos que no son de confianza no se utilizan dentro de Inclusión, cargador de clases, o capacidades de reflexión para evitar vulnerabilidades de inclusión de archivos remotos / locales.		X	
16.5	Verifique que los datos que no son de confianza no se usan dentro del intercambio de recursos entre dominios (CORS) para proteger contra Contenido remoto arbitrario.		X	
16.6	Verifique que los archivos obtenidos de fuentes no confiables Se almacenan fuera del webroot, con limitado Permisos, preferentemente con fuerte validación.		X	
16.7	Verifique que el servidor web o de aplicaciones sea configurado por defecto para denegar el acceso a remoto recursos o sistemas fuera de la web o servidor de aplicaciones.		X	
16.8	Verifique que el código de la aplicación no se ejecute datos cargados obtenidos de fuentes no confiables.		X	
16.9	No utilice Flash, Active-X, Silverlight, NACL, Java del lado del cliente u otras tecnologías del lado del cliente que no sean Compatible de forma nativa a través de los estándares del navegador W3C.		X	

2.5.17. Requerimientos de verificación de movilidad.

Número	Descripción	1	2	3
17.1.	Verifique que los valores de ID almacenados en el dispositivo y recuperable por otras aplicaciones, como el UDID o el número IMEI no se utiliza como autenticación tokens	X		
17.2	Verifique que la aplicación móvil no almacena datos confidenciales datos en potencialmente sin cifrar compartida recursos en el dispositivo (por ejemplo, tarjeta SD o compartida carpetas).	X		
.17.3	Verifique que los datos confidenciales no se almacenen sin protección en el dispositivo, incluso en áreas protegidas del sistema. como los llaveros.	X		

17.4	Verifique que las claves secretas, tokens de API o contraseñas se generan dinámicamente en aplicaciones móviles.	X		
17.5.	Verifique que la aplicación móvil evite fugas de información sensible (por ejemplo, capturas de pantalla Se guardan de la aplicación actual como el La aplicación está en segundo plano o sensible a la escritura información en la consola).	X		
17.6	Verificar que la aplicación está solicitando un mínimo permisos para la funcionalidad requerida y recursos	X		
17.7	Verifique que el código sensible a la aplicación esté puesto fuera de forma impredecible en la memoria (por ejemplo, ASLR).	X		
17.8	Verifique que existen técnicas anti-depuración. presentes que son suficientes para disuadir o retrasar a los posibles atacantes de inyectar depuradores en la aplicación móvil (por ejemplo, GDB).	X		
17.9	Verifique que la aplicación no exporte datos confidenciales actividades, intenciones, o proveedores de contenido para otras aplicaciones móviles en el mismo dispositivo para explotar.	X		
17.10	Verifique que la información confidencial se mantenga en la memoria se sobrescribe con ceros tan pronto como no más tiempo requerido, para mitigar el volcado de memoria los ataques.	X		
17.11	Verifique que la aplicación valide la entrada a exportada. Actividades, intenciones, o proveedores de contenido.	X		

2.5.18. Requerimientos de verificación de servicios web.

Número	Descripción	1	2	3
18.1.	Verifique que se usa el mismo estilo de codificación entre el cliente y el servidor.		X	
18.2	Verificar que el acceso a la administración y funciones de gestión dentro del servicio web y la aplicación está limitada al servicio web de administradores		X	
18.3	Verifique que el esquema XML o JSON esté en su lugar y Validados antes de aceptar la entrada.		X	
18.4	Verifique que todas las entradas estén limitadas a un límite de tamaño.		X	
18.5	Verifique que los servicios web basados en SOAP sean compatibles con servicios web-interoperabilidad (WS-I) básicos, TLS cifrado		X	
18.6	Verificar el uso de autenticación basada en sesión y autorización. Evita el uso de API estática teclas "y similares.		X	
18.7	Verifique que el servicio REST esté protegido de solicitudes de falsificación en sitios cruzados mediante tocken de origen, doble patrón de cookies, elementos de CSRF y token de referencia.		X	
18.8	Verifique que el servicio REST valide que el tipo de contenido entrante sea el esperado, como application / xml o application / json.		X	
18.9	Verifique que la carga útil del mensaje esté firmada para garantizar un transporte fiable entre el cliente y servidor, utilizando JSON Web Signing o WS-Security para Solicitudes de SOAP.		X	
18.10	Verificar la eliminación de rutas de acceso alternativas y menos seguras	X		

2.5.19. Configuración.

Número	Descripción	1	2	3
19.1.	Todos los componentes deben estar al día con la debida configuración de seguridad y de versión (es). Debe incluir la	X		

	eliminación de configuraciones innecesarias y carpetera. Aplicaciones, documentación de la plataforma, y por defecto. o usuarios de ejemplo.			
19.2	Comunicaciones entre componentes de manera encriptada, particularmente con componentes que están en diferentes contenedores o en diferentes sistemas	X		
19.3	Comunicaciones entre componentes de manera autenticada usando una cuenta con los privilegios menos necesarios.		X	
19.4	Verifique que los despliegues de aplicaciones sean adecuados y con la ayuda de sandbox para evaluarlos en contenedores o aislados para retrasar y disuadir a los atacantes de atacar otras aplicaciones.		X	
19.5	Verifique que la aplicación se compile y despliegue con procesos seguros.		X	
19.6	Verifique que los 11administradores autorizados tengan la capacidad para verificar la integridad de todas las configuraciones de seguridad relevantes para garantizar que tengan no ha sido manipulado.		X	
	19.7 Verifique que todos los componentes de la aplicación estén firmados.		X	
19.8	Verifique que los componentes de terceros provienen de repositorios de confianza.		X	
19.9	Verifique que los procesos de compilación para nivel de sistema, los indicadores de seguridad habilitados, como ASLR, DEP, y controles de seguridad.		X	
19.10	Verifique que todos los activos de la aplicación estén alojados en la aplicación, tales como librerías de JavaScript, CSS, hojas de estilo y las fuentes web estén alojadas en la aplicación y en un lugar de confiable como CDN o externo proveedor.		X	

Anexo No 4. Detalle de resultado de Análisis de OWASP

De lo anterior, se pueden clasificar las aplicaciones web de la siguiente manera:

Nivel	Tipos de aplicaciones web de la FGN.	Diagnóstico
1	Intranet y aplicaciones web para la consulta de los servidores de procesos de apoyo.	Nivel de aseguramiento bajo. En la Entidad se cuentan con sistemas de publicación de información de interés a los servidores como es el caso de la intranet las cuales son objeto de análisis de vulnerabilidades.
1	Aplicaciones web para procesos de Apoyo.	Aplicaciones con datos sensibles. Se cuenta con aplicaciones web de apoyo desarrollados internamente como son los que soportan los servicios de inventarios, nómina, viáticos, financieros y votaciones, las cuales son objeto de análisis de vulnerabilidades y fortalecimiento de la plataforma.
2	Aplicaciones web que soportan los procesos misionales de la Entidad.	Aplicaciones críticas. Se desarrollaron aplicaciones web para implementar la gestión misional de la Entidad como es el caso de la ley 600 de 2000 y ley 906 de 2004, las cuales son objeto de análisis de vulnerabilidades, la implementación de técnicas para asegurar las transferencias y fortalecimiento de la plataforma.

Tabla 3, Niveles ASVS - OWASP

De esta clasificación anterior, el ASVS v 4.0 plantea los siguientes objetivos de control:

V1. Arquitectura, diseño y requerimientos de modelamiento de amenazas. Con la implementación de la arquitectura empresarial de la Fiscalía General de la Nación se requiere de un componente de seguridad ágil durante el ciclo de vida del sistema de información para determinar el nivel de seguridad que requieren las aplicaciones y los servicios que pone la Entidad en el ciberespacio.

Otro aspecto importante es la optimización de recursos como lo es el reuso de la arquitectura de las soluciones implementadas, como es el caso de las funcionalidades comunes a todas las aplicaciones de la Entidad: AAA (autenticación, autorización y auditoria), persistencia, notificaciones, secuencia de datos, eventos y estructuras.

En esta fase, se aborda los requerimientos de disponibilidad, confidencialidad, procesamiento de la integridad, no repudio y privacidad, el desarrollador de la Fiscalía general de la nación debe contar con:

- Una lista de chequeo de buenas prácticas para la codificación
- Mentoría y entrenamiento para el uso de las capacidades de las arquitecturas existentes de las aplicaciones web en funcionamiento o por desarrollar.
- Control en la calidad de la codificación
- Planificación de pruebas.
- Control y documentación de desarrollo y configuración.
- Documentación de las operaciones del sistema de información.
- Ejecución y documentación de pruebas.

V1.1 Requerimientos del ciclo de vida de desarrollo de software seguro.

Como estrategia de ciberseguridad se requiere contar con la implementación de controles de seguridad para proteger su funcionalidad y los servicios esenciales que colocan en el ciberespacio ya que requieren funciones de control de acceso, trazabilidad, auditoria, servicios de notificación o de búsqueda. Para esto se toma como base los controles propuestos por OWASP (Open Web Application Security Project), (Project, Application Security Verification Standard 4.0, 2019), los cuales se adaptan a la entidad y se detallan a continuación:

Item	Descripción	L1	L2	L3
1.1.1.	Se declara un proceso de un ciclo de vida de desarrollo de software seguro basado en metodologías ágiles en la entidad adoptada por las áreas de desarrollo de la entidad.	X	X	X
1.1.2.	Con el uso de la metodología SCRUM se permite del proceso de la entidad la utilización de un modelamiento de amenazas para el cambio de las funcionalidades o la estructura de las aplicaciones web en el cambio de diseño o en la planificación de spring y permitir la planificación de mediciones, verificar las respuestas apropiadas frente para mitigar los riesgos y la guía de pruebas de seguridad.	X	X	X
1.1.3.	Para la definición de requerimientos se debe realizar y verificar todas las historias de usuarios y restricciones funcionales de seguridad.	X	X	X
1.1.4.	En la definición de los requerimientos se debe verificar la documentación y la justificación de aplicaciones con respecto a la arquitectura empresarial así como los limites de implementación normativa y funcional, de componentes y significado de flujo de datos dentro de los proceso de la entidad.		X	X
1.1.5.	Para los desarrollos de los servicios tecnológicos y de las aplicaciones web que lo soportan se debe verificar las definiciones de las arquitecturas de alto nivel como es el caso de la arquitectura empresarial de la entidad y realizar un análisis de seguridad de aplicaciones que permiten atender las necesidades funcionales y técnicos, así como los servicios remotos en el entorno digital.		X	X
1.1.6.	Teniendo en cuenta que la entidad cuenta con una única arquitectura empresaria se debe verificar la implementación centralizada y coordinada con los diferentes dominios que plantea la arquitectura así como la sencillez en el diseño incluir los planes de revisiones, de la arquitectura de seguridad y de controles en la reutilización de código, manejo de excepciones, y la evaluación de la infectividad o controles inseguros.		X	X
1.1.7.	Se debe contar con una lista de verificación de pruebas de código seguro, requerimientos de técnicas y de seguridad, y la aplicación de guías y de políticas de seguridad para los roles de desarrolladores y prueba de software.		X	X

V.1.2 Requerimientos arquitectónicos de autenticación.

En la gestión de la autenticación de las identidades para el acceso a las aplicaciones web se deben implementar mecanismos para proteger las vías de acceso no solo de los usuarios sino de los componentes.

Item	Descripción	L1	L2	L3
1.2.1	Las aplicaciones web deben incluir controles de verificación del uso de cuentas de sistema operativo que permitan determinar		X	X

	el cumplimiento de las políticas de seguridad como la responsabilidad única y el establecimiento de perfiles especiales para el acceso o modificación de todos los componentes de la aplicación, servicios y servidores.			
1.2.2	Dentro de la arquitectura se debe identificar y verificar las comunicaciones con la existencia de controles de autenticación entre los componentes de la aplicación como las API, el middleware y el acceso a las capas de datos con los privilegios de acuerdo con el índice de información clasificada y reservada de la entidad.		X	X
1.2.3	De acuerdo con las políticas de seguridad de la información de la entidad se debe verificar que la aplicación en desarrollo o mantenimiento utilice un único mecanismo de autenticación que permita una autenticación sólida y un registro y monitoreo para detectar intentos de abusos o de violaciones de la cuenta.		X	X
1.2.4	En la construcción del software se debe verificar las vías de autenticación dadas por la plataforma tecnológica de la entidad y del uso de API de administración de identidades para evitar la existencia de alternativas más débiles por el riesgo de la aplicación.		X	X

V1.3 Requisitos arquitectónicos de gestión de sesión.

En las arquitecturas de las aplicaciones web de la Entidad, se requiere el control de las sesiones para evitar la interceptación de las comunicaciones entre los componentes o los errores en la gestión de la sesión por medio de identificadores que le dan la posibilidad de mantener abiertas las sesiones.

Item	Descripción	L1	L2	L3
Por definir	En la arquitectura de las aplicaciones web integrados se contempla el control de sesión para generar hashen la verificación de publicación o transmisión de información.		X	X

V1.4 Requisitos arquitectónicos de control de acceso.

En el diseño de la arquitectura web se deben incluir componentes de control de acceso de manera estandarizada y controlada.

Item	Descripción	L1	L2	L3
1.4.1	Las aplicaciones web deben incluir puntos de control de acceso en el servidor y evitar el uso de puntos de control de acceso en el cliente.		X	X
1.4.2	Se debe establecer las necesidades de control de acceso a implementar en la aplicación.		X	X
1.4.3	El área de desarrollo de la entidad debe establecer los privilegios y roles a ser controlado por el sistema de información para minimizar los riesgos de suplantación de identidad o la elevación de privilegios de manera no autorizada o el acceso a funciones, archivos de datos, URL, controladores, servicios y otros recursos.		X	X
1.4.4	Para el desarrollo de servicios de información clasificada o reservada se deben utilizar mecanismos de control de acceso único y verificar los controles de acceso a datos y recursos		X	X

	protegidos para evitar fuga de información (copiar y pegar o utilizar rutas alternativas).			
1.4.5	Los componentes de control de acceso de las aplicaciones web deben hacer uso de controles de acceso basado en roles o en características o atributos que verifique las características de autorización requeridas o de los elementos de datos del usuario dentro de la arquitectura.		X	X

V1.5 Requisitos arquitectónicos de entrada y salida

Las capacidades de verificación de confianza en el servidor logran minimizar las vulnerabilidades del cliente con el uso de microservicios, API sin servidor, API asociadas o externas.

Item	Descripción	L1	L2	L3
1.5.1	Para establecer la viabilidad y el alcance del desarrollo o la implementación de un sistema de información se debe definir los requisitos de entrada y salida que requiere el procesamiento de datos según el entorno digital como contenido, tipo, leyes, regulaciones y normativas.		X	X
1.5.2	En los desarrollos no deben utilizar mecanismos de serialización para el envío de información a clientes no confiables o la implementación de controles de integridad o de cifrado cuando se requiera el acceso a datos confidenciales para evitar ataques de deserialización o de inyección de objetos.		X	X
1.5.3	En las fases de prueba se debe validar los controles de entrada de datos en la capa de servicio.		X	X
1.5.4	El sistema de información debe controlar la salida de datos que se produce cerca o por el intérprete para el que está destinada.			X

V1.6 Requisitos arquitectónicos criptográficos.

Se deben establecer que datos requieren componentes de criptografía a implementar en la arquitectura.

Item	Descripción	L1	L2	L3
1.6.1	La entidad debe contar con una política para la administración de claves criptográficas y establecer el ciclo de vida de una clave criptográfica que para este caso se indica el estándar de administración de claves NIST SP 800-57.		X	X
1.6.2	Para la información clasificada o reservada se debe verificar que los usuarios de servicios criptográficos del sistema de información permitan proteger la clave y datos secretos mediante el uso de almacenamiento controlado de clave o la implementación de las alternativas basadas en API.		X	X
1.6.3	Se debe establecer un proceso que permita controlar todas las claves y contraseñas y en el momento de generar nuevas se cifren los datos confidenciales.		X	X
1.6.4	Para el caso de la información clasificada o reservada se debe verificar la necesidad de uso de claves simétricas, las contraseñas, la protección de los secretos de la API, el cifrado de almacenamiento de dicha información de manera local o los usos temporales como es el caso de pruebas con datos reales con la implementación de mecanismos de ofuscación de parámetros.		X	X

V1.7 Errores, registro y auditoría de requisitos arquitectónicos.

Se debe implementar controles para incluir dentro del desarrollo web y su arquitectura destinados a llevar el registro de errores y de información de auditoria.

Item	Descripción	L1	L2	L3
1.7.1	Para atender los requerimientos de auditoria las aplicaciones web deben verificar el uso de mecanismo y un formato de registro común en todo el sistema.		X	X
1.7.2	En los módulos de auditoria se debe verificar que los registros se transmitan de manera segura y analizar los requerimientos de niveles de servicios para contemplar alternativas de procesamiento para soportar los servicios de análisis, detección, alerta y escalado.		X	X

V1.8 Protección de datos y requisitos arquitectónicos de privacidad.

Se debe identificar los datos que requieren servicios de privacidad de información que requiere el desarrollo web y los componentes a implementar en la arquitectura.

Item	Descripción	L1	L2	L3
1.8.1	En la definición de los requerimientos de información se debe identificar todos los datos confidenciales y clasificados para dar el tratamiento de los niveles de protección a implementar.		X	X
1.8.2	Se debe identificar todos los niveles de protección con sus correspondientes requisitos de cifrado, integridad, la retención, privacidad y confidencialidad, a implementar en la arquitectura del sistema de información.		X	X

V1.9 Requisitos arquitectónicos de comunicaciones.

Se debe controlar las comunicaciones entre contenedores y la interacción con otros sistemas de información.

Item	Descripción	L1	L2	L3
1.9.1	Se debe identificar los requerimientos de ciframiento de las comunicaciones entre componentes ubicados en diferentes contenedores, sistemas, sitios o proveedores de nube.		X	X
1.9.2	El sistema de información de verificar la autenticidad de cada lado del canal de comunicación para evitar ataques de persona en el medio.		X	X

V1.10 Requisitos arquitectónicos del software malicioso.

Se debe contar con un concepto y controles de construcción o modificación de código fuente.

Item	Descripción	L1	L2	L3
1.10.1	Para determinar la viabilidad de un desarrollo o modificación de un desarrollo de aplicación web se debe validar en un sistema de control de código fuente si la funcionalidad requerida está en producción y gestionar adecuadamente el cambio y que en el desarrollo se incluya un sistema de control de código fuente que permita el control de acceso y la trazabilidad de las actividades de los usuarios.		X	X

V1.11 Requisitos arquitectónicos de la lógica de negocios.

Se debe incluir controles de cumplimiento de la lógica de negocios en los desarrollos web.

Item	Descripción	L1	L2	L3
1.11.1	De acuerdo con el dominio de gobernabilidad de la arquitectura empresarial se debe definir y documentar todos los componentes de la aplicación en términos de las funciones de negocio o de seguridad que proporcionan.		X	X
1.11.2	Se debe verificar que no se comparta el estado de no sincronizado en los flujos de lógica de negocio de alto nivel, en los requerimientos de autenticación, administración de sesiones y el control de acceso.		X	
1.11.3	Se debe verificar la seguridad de los subprocesos en términos de funcionalidad, pruebas y uso del sistema de información en concordancia con todos los flujos de lógica de negocio de alto nivel, incluida la autenticación, la administración de sesión y el control de acceso.			X

V1.12 Requisitos arquitectónicos de carga segura de archivos.

En los desarrollos de las aplicaciones web deben incluir mecanismos de control de almacenamiento y consulta de archivos.

Item	Descripción	L1	L2	L3
1.12.1	Se debe verificar en los diseños que los archivos cargados en el sistema de información se almacenen fuera de la raíz web.		X	X
1.12.2	Identificar los requerimientos para que los archivos cargados por el usuario requieren de consulta o descarga desde la aplicación, reciban descargas de flujo de octetos o de un dominio no relacionado. Adicionalmente se debe implementar una política de seguridad de contenido para reducir el riesgo de los vectores XSS u otros ataques del archivo cargado.		X	

V1.13 Requisitos de arquitectura API.

Se cuenta con una arquitectura de API para los desarrollos web.

Item	Descripción	L1	L2	L3
1.13.1	Este es un marcador de posición para futuros requisitos arquitectónicos.			

V1.14 Requisitos arquitectónicos de configuración.

Se debe definir los requisitos de configuración de las aplicaciones web.

Item	Descripción	L1	L2	L3
1.14.1	En la arquitectura del sistema de información se debe implementar la segregación de componentes de diferentes niveles de confianza y controles de seguridad, reglas de firewall, puertas de enlace API, proxies inversos, grupos de seguridad basados en la nube o mecanismos relevantes para la seguridad del sistema.		X	X
1.14.2	Los desarrollos que incluyan el uso de binarios en dispositivos que no son de confianza deben utilizar firmas binarias, conexiones de confianza y puntos finales verificados.		X	
1.14.3	Para la compilación de los componentes de un sistema de información se debe identificar los obsoletos o inseguros para determinar las medidas a implementar.		X	
1.14.4	Se debe verificar el paso a paso de la compilación para verificar automáticamente si la implementación del sistema de información es segura y determinar si la infraestructura del sistema está definida por software.		X	

1.14.5	Se debe verificar que las plataformas de producción se encuentren en un entorno aislado para contener desde la red en términos de latencia para disuadir a los atacantes.		X	
1.14.6	Evitar en lo posible el uso de tecnologías del lado del cliente no autorizadas, que tengan una clasificación de inseguras o en desuso.		X	X

V2: Requisitos de verificación de autenticación

V2.1 Requisitos de seguridad de la contraseña.

Se debe contar con una política de contraseñas fuertes para ser controlada por los desarrollos web.

Item	Descripción	L1	L2	L3
2.1.1	En las aplicaciones web se debe implementar los lineamientos del procedimiento de creación de contraseñas de la entidad el cual contempla una longitud mínima de 12 caracteres.		X	X
2.1.2	Las aplicaciones web deben permitir funcionalidad para gestionar contraseñas de 64 caracteres.		X	X
2.1.3	Las aplicaciones web deben incluir en la funcionalidad el manejo de espacios en las contraseñas sin que se realice truncamientos.		X	X
2.1.4	Las aplicaciones web deben permitir el uso de caracteres Unicode para la gestión de contraseñas, por lo que un solo punto de código Unicode se considera un carácter.		X	X
2.1.5	Se debe establecer funcionalidades para que los usuarios puedan cambiar su contraseña.		X	X
2.1.6	En las aplicaciones web se debe evaluar y viabilizar la implementación funcionalidad que permita el cambio de contraseña a partir de la contraseña actual y la nueva.		X	X
2.1.7	En los controles de gestión de contraseñas a implementar en las aplicaciones web se debe verificar que el uso delas contraseñas cuenten con un registro de contraseñas violadas o con un estado de infracción para que los usuarios se vean obligados a cambiarla. En el caso de la utilización de una API externa se debe realizar una prueba de conocimiento cero u otro mecanismo para que no se envíe la contraseña de texto sin formato o con un estado de infracción de la contraseña.		X	X
2.1.8	Se debe evaluar e implementar controles para que se proporcione una clasificación de seguridad de contraseña y proveer mecanismos de construcción de contraseñas más segura.		X	X

V2.2 Requisitos generales de autenticación.

Se debe desarrollar las aplicaciones web teniendo en cuenta un control de los incidentes de autenticación.

Item	Descripción	L1	L2	L3
2.2.1	Verificar los controles para mitigar las pruebas de credenciales violadas, la fuerza bruta y los ataques de bloqueo de cuenta.		X	
2.2.2	Verificar el uso de autenticadores débiles se utilicen únicamente en la verificación secundaria y la aprobación de transacciones, así como el uso de métodos más sólidos antes que los débiles, que los usuarios conozcan los riesgos o que se tomen las medidas adecuadas para limitar los riesgos del compromiso de la cuenta.		X	
2.2.3	Verifique que las notificaciones seguras se envíen a los usuarios después de las actualizaciones de los detalles de autenticación, como restablecimientos de credenciales, cambios		X	

	de dirección o correo electrónico, inicio de sesión desde ubicaciones desconocidas o riesgosas. Se prefiere el uso de notificaciones push, en lugar de SMS o correo electrónico, pero en ausencia de notificaciones push, SMS o correo electrónico son aceptables siempre y cuando no se divulgue información confidencial en la notificación.			
2.2.4	Verifique la resistencia a la suplantación de identidad contra el phishing, como el uso de la autenticación de múltiples factores, los dispositivos criptográficos con intención (como las claves conectadas con un empuje para autenticar) o, en los niveles más altos de AAL, los certificados del lado del cliente.		X	
2.2.5	Verifique que cuando un proveedor de servicios de credenciales (CSP) y la autenticación de verificación de la aplicación están separados, se establece un TLS mutuamente autenticado entre los dos puntos finales.		X	
2.2.6	Verifique la resistencia de reproducción mediante el uso obligatorio de dispositivos OTP, autenticadores criptográficos o códigos de búsqueda.		X	
2.2.7	Verifique la intención de autenticarse mediante la entrada de un token OTP o una acción iniciada por el usuario, como presionar un botón en una llave de hardware FIDO.		X	

V2.3 Requisitos del ciclo de vida del autenticador.

Se debe controlar la generación de contraseñas o códigos de activación iniciales.

Item	Descripción	L1	L2	L3
2.3.1	Las contraseñas iniciales o los códigos de activación deben ser temporales y generados por el sistema de manera segura y aleatoria, tener una longitud mínima de caracteres, y contener letras y números, y controlar un tiempo de expiración después de un corto período de tiempo.		X	
2.3.2	Verifique que la inscripción y el uso de los dispositivos de autenticación provistos por el suscriptor sean compatibles, como los tokens U2F o FIDO.		X	
2.3.3	Verifique que las instrucciones de renovación se envíen con tiempo suficiente para renovar los autenticadores de límite de tiempo.		X	

V2.4 Requisitos de almacenamiento de credenciales.

Se debe contar con controles de acceso en los desarrollos web concernientes al almacenamiento de credenciales.

Item	Descripción	L1	L2	L3
2.4.1	Verifique que las contraseñas se almacenen en una forma que sea resistente a los ataques sin conexión. Las contraseñas DEBEN ser tratadas con sal mediante una derivación de clave unidireccional aprobada o una función de hashing de contraseña. Las funciones de derivación de claves y hash de contraseñas toman una contraseña, un salt y un factor de costo como entradas cuando se genera un hash de contraseña.		X	
2.4.2	Verifique que la sal tenga al menos 32 bits de longitud y se elija arbitrariamente para minimizar las colisiones de valores de sal entre los hashes almacenados. Para cada credencial, se DEBE almacenar un valor de sal único y el hash resultante.		X	
2.4.3	Verifique que si se usa PBKDF2, el recuento de iteraciones DEBERÍA ser tan grande como lo permita el rendimiento del servidor de verificación, típicamente al menos 100,000 iteraciones.		X	
2.4.4	Verifique que si se usa bcrypt, el factor de trabajo DEBE ser		X	

	tan grande como lo permita el rendimiento del servidor de verificación, generalmente al menos 13			
2.4.5	Verifique que se realice una iteración adicional de una función de derivación de claves, utilizando un valor de sal que sea secreto y que solo conozca el verificador. Genere el valor de sal utilizando un generador de bits aleatorio aprobado [SP 800-90Ar1] y proporcione al menos la fuerza de seguridad mínima especificada en la última revisión de SP 800-131A. El valor de sal secreto SE DEBE almacenar por separado de las contraseñas con hash (por ejemplo, en un dispositivo especializado como un módulo de seguridad de hardware).		X	

V2.5 Requisitos de recuperación de credenciales.

El desarrollo web debe contemplar funcionalidad de recuperación de credenciales.

Item	Descripción	L1	L2	L3
2.5.1	Verifique que la activación inicial generada por el sistema o el secreto de recuperación no se envíe en texto claro al usuario		X	
2.5.2	Verifique que las sugerencias de contraseña o la autenticación basada en el conocimiento (las llamadas "preguntas secretas") no estén presentes.		X	
2.5.3	Verifique que la recuperación de la credencial de la contraseña no revele la contraseña actual de ninguna manera.		X	
2.5.4	Verificación que las cuentas compartidas o predeterminadas no están presentes (por ejemplo, "root", "admin" o "sa").		X	
2.5.5	Verifique que si se cambia o reemplaza un factor de autenticación, se notifica al usuario sobre este evento.		X	
2.5.6	Verifique la contraseña olvidada, y otras rutas de recuperación usan un mecanismo de recuperación seguro, como TOTP u otro token de software, dispositivo móvil u otro mecanismo de recuperación sin conexión.		X	

V2.6 Requisitos del verificador secreto de búsqueda.

Se debe incluir controles en el resultado y presentación de las búsquedas de información efectuada por las aplicaciones web.

Item	Descripción	L1	L2	L3
2.6.1	Verifique que los secretos de búsqueda se pueden usar solo una vez.		X	X
2.6.2	Verifique que los secretos de búsqueda tengan suficiente aleatoriedad (112 bits de entropía), o si son menos de 112 bits de entropía, salados con una sal de 32 bits única y aleatoria y hash con un hash unidireccional aprobado.		X	X
2.6.3	Verifique que los secretos de búsqueda sean resistentes a los ataques sin conexión, como los valores predecibles.		X	X

V2.7. Requisitos del verificador fuera de banda

Se deben identificar la necesidad de implementar controles para la autenticación sin conexión a la red.

Item	Descripción	L1	L2	L3
2.7.1	Verifique la autenticación de texto claro fuera de banda como es el caso del uso de SMS o PSTN y no se ofrezcan el servicio directo y sin notificaciones.		X	
2.7.2	Verifique que el verificador fuera de banda caduque las solicitudes, códigos o tokens de autenticación fuera de banda después de 10 minutos.		X	
2.7.3	Verifique que las solicitudes, códigos o tokens de autenticación del verificador fuera de banda solo se puedan		X	

	utilizar una vez, y solo para la solicitud de autenticación original.			
2.7.4	Verifique que el autenticador y el verificador fuera de banda se comuniquen a través de un canal independiente seguro.		X	
2.7.5	Verifique que el verificador fuera de banda solo retenga una versión con hash del código de autenticación.		X	
2.7.6	Verifique que el código de autenticación inicial sea generado por un generador seguro de números aleatorios, que contenga al menos 20 bits de entropía (por lo general, un número aleatorio digital de seis es suficiente).		X	

V2.8 Requisitos del verificador único o multifactorial

Los desarrollos web cuentan con controles para la protección y gestión de claves.

Item	Descripción	L1	L2	L3
2.8.1	Verifique que las OTP basadas en el tiempo tengan un tiempo de vida definido antes de que caduque.		X	
2.8.2	Verifique que las claves simétricas utilizadas para verificar las OTP enviadas estén altamente protegidas, por ejemplo, mediante el uso de un módulo de seguridad de hardware o un almacenamiento de claves basado en un sistema operativo seguro.		X	
2.8.3	Verifique que los algoritmos criptográficos aprobados se utilizan en la generación, la inicialización y la verificación.		X	
2.8.4	Verifique que la OTP basada en el tiempo se pueda usar solo una vez dentro del período de validez.		X	
2.8.5	Verifique si un token OTP multifactorial basado en el tiempo se reutiliza durante el período de validez, se registra y rechaza con notificaciones seguras que se envían al titular del dispositivo.		X	
2.8.6	Verifique que el generador de OTP de factor único físico pueda ser revocado en caso de robo u otra pérdida. Asegúrese de que la revocación sea efectiva de inmediato en las sesiones iniciadas, independientemente de la ubicación.		X	
2.8.7	Verifique que los autenticadores biométricos se limiten a usar solo como factores secundarios junto con algo que tenga y algo que sepa.		X	

V2.9 Requisitos del verificador de dispositivos y dispositivos criptográficos.

Se deben incluir controles para la generación y almacenamiento de claves criptográficas para los desarrollos web.

Item	Descripción	L1	L2	L3
2.9.1	Verifique que las claves criptográficas utilizadas en la verificación se almacenen de forma segura y estén protegidas contra la divulgación.		X	
2.9.2	Verifique las semillas de generación de claves sea de al menos 64 bits de longitud, y estadísticamente único o único durante la vida útil del dispositivo criptográfico.		X	
2.9.3	Verificación que los algoritmos criptográficos aprobados se utilizan en la generación, la inicialización y la verificación.		X	

V2.10 Requisitos de autenticación del servicio.

Se debe incluir controles para no exponer información de claves, llaves y datos propios del funcionamiento de la aplicación en la publicación de servicios en el ciberespacio.

Item	Descripción	L1	L2	L3
2.10.1	Verifique los secretos de integración no se basen en contraseñas invariables, como claves de API o cuentas con privilegios compartidos.		X	
2.10.2	Verifique si se requieren contraseñas, las credenciales no son una cuenta predeterminada.		X	
2.10.3	Verifique el almacenamiento de las contraseñas con suficiente protección para evitar ataques de recuperación fuera de línea, incluido el acceso al sistema local.		X	
2.10.4	Verifique que las contraseñas, las integraciones con bases de datos y sistemas de terceros, las semillas y los secretos internos, y las claves de API se administren de manera segura y no se incluyan en el código fuente o se almacenen en los repositorios de código fuente. Dicho almacenamiento DEBE resistir los ataques sin conexión. Se recomienda el uso de un almacén de claves de software seguro (L1), un módulo de plataforma confiable de hardware (TPM) o un módulo de seguridad de hardware (L3) para el almacenamiento de contraseñas.		X	

V3: Requisitos de verificación de gestión de sesión

V3.1 Requisitos de Gestión de Sesiones Fundamentales.

Se debe incluir controles para no exponer información de tocken en la publicación mediante URL o en los mensajes del sistema.

Item	Descripción	L1	L2	L3
3.1.1	Verifique que la aplicación nunca revela tokens de sesión en parámetros de URL o mensajes de error.		X	

V3.2 Requisitos de vinculación de sesión.

La aplicación web debe incluir controles para el manejo de la autenticación de sesiones.

Item	Descripción	L1	L2	L3
3.2.1	Verifique que la aplicación genere un nuevo token de sesión en la autenticación del usuario.	X	X	X
3.2.2	Verifique que los tokens de sesión posean al menos 64 bits de entropía.	X	X	X
3.2.3	Verifique que la aplicación solo almacene tokens de sesión en el navegador utilizando métodos seguros, como cookies protegidas adecuadamente (consulte la sección 3.4) o el almacenamiento de sesión HTML 5.		X	X

V3.3 Requisitos de sesión y de tiempos de espera.

Las aplicaciones web deben contar con controles de tiempo de vida y cierre de las sesiones.

Item	Descripción	L1	L2	L3
3.3.1	Verifique que el cierre de sesión y la caducidad invaliden el token de la sesión, de modo que el botón de retroceso o una parte dependiente descendente no reanude una sesión autenticada, incluso entre las partes confiables.		X	
3.3.2	Si los autenticadores permiten que los usuarios permanezcan conectados, verifique que la autentificación ocurra periódicamente tanto cuando se usan activamente como después		X	

	de un período de inactividad.			
3.3.3	Verifique que la aplicación termine todas las demás sesiones activas después de un cambio exitoso de la contraseña, y que esto sea efectivo en toda la aplicación, el inicio de sesión federado (si está presente) y cualquier otra parte que confíe.		X	
3.3.4	Verifique que los usuarios puedan ver y cerrar sesión en cualquiera o todas las sesiones y dispositivos activos actualmente.		X	

V3.4 Gestión de sesiones basada en cookies.

Se deben activar los atributos que permitan proteger el uso de cookies en la gestión de sesiones.

Item	Descripción	L1	L2	L3
3.4.1	Verifique que los tokens de sesión basados en cookies tengan el atributo "Seguro" establecido.		X	
3.4.2	Verifique que los tokens de sesión basados en cookies tengan el atributo 'HttpOnly' establecido.		X	
3.4.3	Verifique que los tokens de sesión basados en cookies utilicen el atributo 'SameSite' para limitar la exposición a ataques de falsificación de solicitudes entre sitios.		X	
3.4.4	Verifique que los tokens de sesión basados en cookies utilicen el prefijo "__Host-" para proporcionar la confidencialidad de las cookies de sesión.		X	
3.4.5	Verifique que si la aplicación se publica bajo un nombre de dominio con otras aplicaciones que configuran o usan cookies de sesión que podrían invalidar o revelar las cookies de sesión, establezca el atributo de ruta en tokens de sesión basados en cookies utilizando la ruta más precisa posible.		X	

V3.5 Gestión de sesión basada en token

Las aplicaciones web deben actualizar los tokens en caso de terminar las vinculaciones con otros sistemas de información.

Item	Descripción	L1	L2	L3
3.5.1	La aplicación no debe tratar OAuth y actualizar los tokens en cuanto a la presencia del suscriptor y permisos para que los usuarios terminen las relaciones de confianza con las aplicaciones vinculadas.		X	
3.5.2	Verifique que la aplicación use tokens de sesión en lugar de claves y secretos de API estática, excepto con implementaciones heredadas.		X	
3.5.3	Verifique que los tokens de sesión sin estado utilicen firmas digitales, cifrado y otras contramedidas para protegerse contra la manipulación indebida, la envolvente, la reproducción, el cifrado nulo y los ataques de sustitución de claves.		X	

V3.6 Re-autenticación de una Federación o Afirmación.

Se debe incluir controles de autenticación contemplando los tiempos de asignación y trazabilidad.

Item	Descripción	L1	L2	L3
3.6.1	Verifique que las partes confiables especifiquen el tiempo máximo de autenticación para los CSP y que los CSP vuelvan a autenticar al suscriptor si no han utilizado una sesión dentro de ese período.		X	
3.6.2	Verifique que los CSP informen a las partes confidentes del último evento de autenticación, para permitir que los RP determinen si necesitan volver a autenticar al usuario.		X	

V3.7 Defensas contra explotaciones de gestión de sesión.

El desarrollo web debe incluir controles de inicio de sesión para determinar su validez y permitir las transacciones contempladas.

Item	Descripción	L1	L2	L3
3.7.1	Verifique que la aplicación garantice una sesión de inicio de sesión válida o que requiera una nueva autenticación o verificación secundaria antes de permitir cualquier transacción confidencial o modificación de la cuenta.		X	

V4: Requisitos de verificación de control de acceso

V4.1 Diseño general de control de acceso.

El desarrollo web incluye reglas de control de acceso en capas de servicio o controles de acceso de usuarios a recursos.

Item	Descripción	L1	L2	L3
4.1.1	Verifique que la aplicación aplique las reglas de control de acceso en una capa de servicio confiable, especialmente si el control de acceso del lado del cliente está presente y podría ser anulado.		X	
4.1.2	Verifique que los usuarios finales no puedan manipular todos los atributos de usuario y datos, así como la información de política utilizada por los controles de acceso, a menos que esté específicamente autorizado.			
4.1.3	Verifique que exista el principio de privilegio mínimo: los usuarios solo deben poder acceder a funciones, archivos de datos, URL, controladores, servicios y otros recursos, para los cuales poseen autorización específica. Esto implica protección contra la suplantación de identidad y la elevación de privilegios.		X	
4.1.4	Verifique que exista el principio de denegar de forma predeterminada, por lo que los nuevos usuarios / roles comienzan con permisos mínimos o nulos y los usuarios / roles no reciben acceso a nuevas funciones hasta que el acceso se asigna explícitamente.		X	

V4.2 Control de acceso a nivel de operación

En los desarrollos web se deben proteger los datos confidenciales y API ante ataques de falsificación de peticiones en sitios cruzados mediante el uso de token.

Item	Descripción	L1	L2	L3
4.2.1	Verifique que los datos confidenciales y las API estén protegidos contra los ataques directos de objetos dirigidos a la creación, lectura, actualización y eliminación de registros, como crear o actualizar el registro de otra persona, ver los registros de todos o eliminar todos los registros.		X	
4.2.2	Verifique que la aplicación o el marco de trabajo aplique un fuerte mecanismo anti-CSRF para proteger la funcionalidad autenticada, y la efectiva anti-CSRF o anti-CSRF protege la funcionalidad no autenticada.		X	

V4.3 Otras consideraciones de control de acceso.

Las aplicaciones web deben incluir controles de navegación de directorio o descubrimiento de metadatos.

Item	Descripción	L1	L2	L3
4.3.1	Verifique que las interfaces administrativas usen la autenticación multifactor apropiada para evitar el uso no autorizado.		X	
4.3.2	Verifique que la navegación del directorio esté deshabilitada a menos que se desee deliberadamente. Además, las aplicaciones no deben permitir el descubrimiento o la divulgación de metadatos de archivos o directorios, como las carpetas Thumbs.db, .DS_Store, .git o .svn.		X	
4.3.3	Verifique que la aplicación tenga autorización adicional (como la autenticación avanzada o adaptativa) para los sistemas de menor valor y / o la separación de tareas para que las aplicaciones de alto valor apliquen controles antifraude según el riesgo de la aplicación y el fraude anterior.		X	

V5: Requisitos de validación, desinfección y verificación de codificación.

V5.1. Requisitos de validación de entradas.

Las aplicaciones web deben incluir controles ante ataques de contaminación asignación masiva de parámetros o de HTTP.

Item	Descripción	L1	L2	L3
5.1.1	Verifique que la aplicación tenga defensas contra los ataques de contaminación de parámetros HTTP, especialmente si el marco de la aplicación no hace distinciones sobre la fuente de los parámetros de solicitud (GET, POST, cookies, encabezados o variables de entorno).		X	
5.1.2	Verifique que los marcos protejan contra los ataques masivos de asignación de parámetros, o que la aplicación tenga contramedidas para proteger contra la asignación insegura de parámetros, como marcar campos privados o similares.		X	
5.1.3	Verifique que todas las entradas (campos de formulario HTML, solicitudes REST, parámetros de URL, encabezados HTTP, cookies, archivos por lotes, fuentes RSS, etc.) se validen utilizando una validación positiva (lista blanca).		X	
5.1.4	Verifique que los datos estructurados estén tipificados y validados con fuerza contra un esquema definido, incluidos los caracteres permitidos, la longitud y el patrón (por ejemplo, números de tarjeta de crédito o teléfono, o validar que dos campos relacionados sean razonables, como verificar que coincida el suburbio y código postal).		X	
5.1.5	Verifique que la URL redirecciona y reenvía solo a destinos incluidos en una lista blanca, o muestra una advertencia cuando se redirige a contenido potencialmente no confiable.		X	

V5.2 Requisitos de saneamiento y sandboxing.

Los desarrollos web deben incluir controles de validación de presencia de virus en los datos como control de caracteres y longitud.

Item	Descripción	L1	L2	L3
5.2.1	Verifique que todas las entradas de HTML no confiables de editores WYSIWYG o similares estén correctamente desinfectadas con una biblioteca de desinfectante HTML o una función de marco.		X	
5.2.2	Verifique que los datos no estructurados se desinfecten para aplicar medidas de seguridad, como caracteres y longitud permitidos.		X	
5.2.3	Verifique que la aplicación desinfecte la entrada del usuario antes de pasar a los sistemas de correo para protegerse contra la inyección de SMTP o IMAP.		X	
5.2.4	Verifique que la aplicación evite el uso de eval () u otras funciones de ejecución de código dinámico. Donde no haya alternativa, cualquier entrada del usuario que se incluya debe ser desinfectada o en un espacio aislado antes de ser ejecutada.		X	
5.2.5	Verifique que la aplicación proteja contra los ataques de inyección de plantillas asegurándose de que cualquier entrada del usuario que se incluya esté desinfectada o en un espacio aislado.			
5.2.6	Verifique que la aplicación proteja contra los ataques de la SSRF, al validar o limpiar datos no confiables o metadatos de archivos HTTP, como los nombres de los archivos y los campos de ingreso de URL, use la lista blanca de protocolos, dominios, rutas y puertos.		X	
5.2.7	Verifique que la aplicación desinfecte, deshabilite o genetine el contenido de las secuencias de comandos SVG proporcionadas por el usuario, especialmente en lo que se refiere a XSS que resultan de los scripts en línea y foreignObject.		X	
5.2.8	Verifique que la aplicación desinfecte, deshabilite o incluya en la arena el contenido del lenguaje de la plantilla de expresión o de script provisto por el usuario, como Markdown, CSS o XSL hojas de estilo, BBCode, o similar.		X	

V5.3 Codificación de salida y requisitos de prevención de inyección.

El desarrollo web debe incluir controles de codificación de salida o inyección a base de datos o repositorios mediante la validación del conjunto de caracteres configurado y parámetros de consulta.

Item	Descripción	L1	L2	L3
5.3.1	Verifique que la codificación de salida sea relevante para el intérprete y el contexto requerido. Por ejemplo, use codificadores específicamente para valores HTML, atributos HTML, JavaScript, parámetros de URL, encabezados HTTP, SMTP y otros según lo requiera el contexto, especialmente de entradas no confiables (por ejemplo, nombres con Unicode o apóstrofes, como ㄴ o O'Hara) .		X	
5.3.2	Verifique que la codificación de salida conserve el conjunto de caracteres y la configuración regional elegidos por el usuario, de modo que cualquier punto de carácter Unicode sea válido y se maneje de manera segura.		X	
5.3.3	Verifique que el escape de salida consciente del contexto, preferiblemente automatizado o, en el peor de los casos, manual, protege contra XSS reflejados, almacenados y basados		X	

	en DOM.			
5.3.4	Verifique que la selección de datos o las consultas de base de datos (por ejemplo, SQL, HQL, ORM, NoSQL) utilicen consultas parametrizadas, ORM, marcos de entidades o estén protegidos de los ataques de inyección de base de datos.		X	
5.3.5	Verifique que cuando no existan mecanismos parametrizados o más seguros, se utilice la codificación de salida específica del contexto para proteger contra ataques de inyección, como el uso de escape de SQL para protegerse contra la inyección de SQL.		X	
5.3.6	Verifique que la aplicación se proyecte contra los ataques de inyección de JavaScript o JSON, incluidos los ataques eval, los controles remotos de JavaScript, los desvíos de CSP, DOM XSS y la evaluación de expresiones de JavaScript.		X	
5.3.7	Verifique que la aplicación proteja contra las vulnerabilidades de Inyección LDAP, o que se hayan implementado controles de seguridad específicos para evitar la Inyección LDAP.		X	
5.3.8	Verifique que la aplicación proteja contra la inyección de comandos del sistema operativo y que las llamadas al sistema operativo utilicen consultas de sistema operativo parametrizadas o utilicen la codificación de salida de la línea de comandos contextual.		X	
5.3.9	Verifique que la aplicación proteja contra ataques de inclusión de archivos locales (LFI) o inclusión de archivos remotos (RFI).		X	
5.3.10	Verifique que la aplicación proteja contra la inyección de XPath o los ataques de inyección de XML.		X	

V5.4 Requisitos de memoria, cadena y código no administrado de

El desarrollo web debe utilizar controles de cadena de memoria segura y formato de entrada.

Item	Descripción	L1	L2	L3
5.4.1	Verifique que la aplicación utilice una cadena de memoria segura, una copia de memoria más segura y una aritmética de punteros para detectar o evitar el desbordamiento de la pila, el búfer o el montón.		X	
5.4.2	Verifique que las cadenas de formato no tomen entradas potencialmente hostiles y sean constantes.		X	
5.4.3	Verifique que las técnicas de validación de signos, rangos y entradas se utilizan para evitar desbordamientos de enteros.		X	

V5.5 Requisitos de prevención de deserialización.

El desarrollo web debe controlar la integridad de los objetos serializado y sus requerimientos de encripción

Item	Descripción	L1	L2	L3
5.5.1	Verifique que los objetos serializados utilicen controles de integridad o estén encriptados para evitar la creación de objetos hostiles o la manipulación de datos.		X	X
5.5.2	Verifique que la aplicación restrinja correctamente los analizadores XML para que solo usen la configuración más restrictiva posible y para asegurarse de que las funciones no seguras, como la resolución de entidades externas, estén deshabilitadas para evitar la XXE		X	X
5.5.3	Verifique que se evite la deserialización de datos no confiables o que esté protegido tanto en el código personalizado como en las bibliotecas de terceros (como los analizadores		X	X

	JSON, XML y YAML).			
5.5.4	Verifique que al analizar JSON en navegadores o en backends basados en JavaScript, JSON.parse se utiliza para analizar el documento JSON. No utilice eval () para analizar JSON.		X	X

V6: Requisitos de verificación de criptografía almacenada

V6.1 Clasificación de datos.

Los desarrollos web deben incluir controles de almacenamiento de datos privados que lo requieran.

Item	Descripción	L1	L2	L3
6.1.1	Verifique que los datos privados regulados se almacenen encriptados mientras se encuentran en reposo, como información de identificación personal (PII), información personal confidencial o datos que se consideran sujetos a GDPR de la UE.		X	X
6.1.2	Verifique que los datos de salud regulados se almacenen encriptados mientras se encuentran en reposo, como registros médicos, detalles de dispositivos médicos o registros de investigación anónimos.		X	X
6.1.3	Verifique que los datos financieros regulados se almacenen encriptados mientras están en reposo, como cuentas financieras, incumplimientos o historial de crédito, registros de impuestos, historial de pagos, beneficiarios o registros de anonimización del mercado o de investigación.		X	X

V6.2 Algoritmos.

Las aplicaciones web deben incluir controles de los errores de los componentes o servicios de encripción.

Item	Descripción	L1	L2	L3
6.2.1	Verifique que todos los módulos criptográficos fallen de manera segura y que los errores se manejen de una manera que no habilite los ataques de Oracle Padding.		X	
6.2.2	Verifique que se utilicen los algoritmos, modos y bibliotecas criptográficos probados en la industria o aprobados por el gobierno, en lugar de la criptografía codificada personalizada.		X	
6.2.3	Verifique que el vector de inicialización de encriptación, la configuración de cifrado y los modos de bloqueo estén configurados de manera segura utilizando el último consejo.		X	
6.2.4	Verifique que los números aleatorios, algoritmos de cifrado o hash, longitudes de clave, rondas, cifrados o modos puedan reconfigurarse, actualizarse o intercambiarse en cualquier momento, para protegerlos contra roturas criptográficas.		X	
6.2.5	Verifique que los modos de bloque inseguros conocidos (es decir, el BCE, etc.), los modos de relleno (es decir, PKCS # 1 v1.5, etc.), los cifrados con tamaños de bloque pequeños (es decir, Triple-DES, Blowfish, etc.), y los algoritmos de hashing débil (es decir, MD5, SHA1, etc.) no se utilizan a menos que sean necesarios para la compatibilidad con versiones anteriores.		X	
6.2.6	Verifique que los nonces, los vectores de inicialización y otros números de uso único no se deben usar más de una vez con una clave de cifrado determinada. El método de generación debe ser apropiado para el algoritmo utilizado.		X	
6.2.7	Verifique que los datos cifrados se autentiquen mediante firmas, modos de cifrado autenticados o HMAC para garantizar que el texto cifrado no sea alterado por una parte no autorizada.		X	

6.2.8	Verifique que todas las operaciones criptográficas son de tiempo constante, sin operaciones de "cortocircuito" en las comparaciones, cálculos o devoluciones, para evitar la pérdida de información.		X	

V6.3 Valores aleatorios.

Los desarrollos web deben incluir en su funcionamiento de generador de números aleatorios o pseudoaleatorios seguros.

Item	Descripción	L1	L2	L3
6.3.1	Verifique que todos los números aleatorios, los nombres de archivos aleatorios, los GUID aleatorios y las cadenas aleatorias se generen utilizando el generador de números aleatorios criptográficos seguros aprobados por el módulo criptográfico cuando un atacante no debe poder adivinar estos valores aleatorios.		X	
6.3.2	Verifique que los GUID aleatorios se crean utilizando el algoritmo GUID v4 y un generador de números pseudoaleatorios criptográficamente seguros (CSPRNG). Los GUID creados con otros generadores de números pseudoaleatorios pueden ser predecibles.		X	
6.3.3	Verifique que los números aleatorios se crean con la entropía adecuada incluso cuando la aplicación está bajo una gran carga, o que la aplicación se degrada con gracia en tales circunstancias.		X	

V6.4 Gestión secreta.

Los desarrollos web deben contemplar controles de acceso y almacenamiento o de destrucción de la información clasificada como secreta.

Item	Descripción	L1	L2	L3
6.4.1	Verifique que se utilice una solución de administración de secretos, como una bóveda de claves, para crear, almacenar, controlar el acceso y destruir de forma segura los secretos.		X	X
6.4.2	Verifique que el material clave no esté expuesto a la aplicación, sino que utilice un módulo de seguridad aislado como una bóveda para operaciones criptográficas.		X	X

V7: Gestión de errores y requisitos de verificación de registro

V7.1 Requisitos de contenido de registro

Las aplicaciones web deben controlar el registro de credenciales, token asignados o datos confidenciales de los usuarios.

Item	Descripción	L1	L2	L3
7.1.1	Verifique que la aplicación no registre credenciales o detalles de pago. Los tokens de sesión solo deben almacenarse en los registros de forma irreversible y hash.		X	X
7.1.2	Verifique que la aplicación no registre otros datos confidenciales como se define en las leyes de privacidad locales o la política de seguridad relevante.		X	X
7.1.3	Verifique que la aplicación registre eventos relevantes de seguridad que incluyan eventos de autenticación exitosos y fallidos, fallas de control de acceso, fallas de deserialización y		X	X

	fallas de validación de entrada.			
7.1.4	Verifique que cada evento de registro incluya la información necesaria que permitiría una investigación detallada de la línea de tiempo cuando ocurre un evento.		X	X

V7.2 Requisitos de procesamiento de registro.

El desarrollo web debe registrar las decisiones de autenticación sin almacenar identificadores de sesión o contraseñas.

Item	Descripción	L1	L2	L3
7.2.1	Verifique que todas las decisiones de autenticación estén registradas, sin almacenar identificadores de sesión o contraseñas confidenciales. Esto debe incluir solicitudes con metadatos relevantes necesarios para las investigaciones de seguridad.		X	X
7.2.2	Verifique que todas las decisiones de control de acceso se puedan registrar y todas las decisiones fallidas se registren. Esto debe incluir solicitudes con metadatos relevantes necesarios para las investigaciones de seguridad.		X	X

V7.3 Requisitos de protección de registro

La aplicación web debe codificar los datos proporcionados por el usuario y controlar la visualización de datos de registro.

Item	Descripción	L1	L2	L3
7.3.1	Verifique que la aplicación codifique adecuadamente los datos proporcionados por el usuario para evitar la inyección de registros.		X	X
7.3.2	Verifique que todos los eventos estén protegidos de la inyección cuando se visualicen en el software de visualización de registros.		X	X
7.3.3	Verifique que los registros de seguridad estén protegidos contra accesos y modificaciones no autorizados.		X	X
7.3.4	Verifique que las fuentes de tiempo estén sincronizadas con la hora y la zona horaria correctas. Considere seriamente el registro solo en UTC si los sistemas son globales para ayudar con el análisis forense posterior al incidente.		X	X

V7.4 Manejo de errores.

La aplicación web debe controlar los mensajes genéricos de un error o de manejo de excepciones.

Item	Descripción	L1	L2	L3
7.4.1	Verifique que se muestre un mensaje genérico cuando ocurra un error inesperado o sensible a la seguridad, potencialmente con una identificación única que el personal de soporte puede usar para investigar.		X	
7.4.2	Verifique que el manejo de excepciones (o un equivalente funcional) se use en la base de código para tener en cuenta las condiciones de error esperadas e inesperadas.		X	
7.4.3	Verifique que se haya definido un controlador de errores de "último recurso" que detectará todas las excepciones no manejadas.		X	

V8: Requisitos de verificación de protección de datos

V8.1 Protección general de datos.

La aplicación web debe controlar los datos o parámetros almacenados en cache o en memoria temporal y de su eliminación.

Item	Descripción	L1	L2	L3
8.1.1	Verifique que la aplicación evite que los datos confidenciales se almacenen en caché en los componentes del servidor, como balanceadores de carga y cachés de aplicaciones.		X	X
8.1.2	Verifique que todas las copias en caché o temporales de los datos confidenciales almacenados en el servidor estén protegidos contra el acceso no autorizado o que se purguen / invaliden después de que el usuario autorizado acceda a los datos confidenciales.		X	X
8.1.3	Verifique que la aplicación minimice el número de parámetros en una solicitud, como campos ocultos, variables Ajax, cookies y valores de encabezado.		X	X
8.1.4	Verifique que la aplicación pueda detectar y alertar sobre un número anormal de solicitudes, como por IP, usuario, total por hora o día, o lo que tenga sentido para la aplicación.		X	X
8.1.5	Verifique que se realicen copias de seguridad periódicas de datos importantes y que se realice una restauración de prueba de los datos.		X	X
8.1.6	Verifique que las copias de seguridad se almacenen de forma segura para evitar que los datos sean robados o dañados.		X	X

V8.2 Protección de datos del lado del cliente.

Las aplicaciones web controlan la divulgación de datos confidenciales en los encabezados para controlar el caching en el cliente.

Item	Descripción	L1	L2	L3
8.2.1	Verifique que la aplicación establezca suficientes encabezados anti-caching para que los datos confidenciales no se almacenen en caché en los navegadores modernos.		X	X
8.2.2	Verifique que los datos almacenados en el almacenamiento del lado del cliente (como el almacenamiento local de HTML5, el almacenamiento de sesión, IndexedDB, las cookies normales o las cookies de Flash) no contengan datos confidenciales o PII.		X	X
8.2.3	Verifique que los datos autenticados se borran del almacenamiento del cliente, como el DOM del navegador, una vez que se termina el cliente o la sesión.		X	X

V8.3 Datos Privados Sensibles.

Las aplicaciones web deben usar controles para eliminar o exportar datos privados o confidenciales de los usuarios con los correspondientes mecanismos de trazabilidad.

Item	Descripción	L1	L2	L3
8.3.1	Verifique que los datos confidenciales se envíen al servidor en el cuerpo del mensaje HTTP o los encabezados, y que los parámetros de la cadena de consulta de cualquier verbo HTTP no contengan datos confidenciales.		X	X
8.3.2	Verifique que los usuarios tengan un método para eliminar o exportar sus datos a pedido.		X	X
8.3.3	Verifique que los usuarios reciban un lenguaje claro con		X	X

	respecto a la recopilación y el uso de la información personal suministrada y que los usuarios hayan otorgado su consentimiento para el uso de esos datos antes de que se utilicen de alguna manera.			
8.3.4	Verifique que se hayan identificado todos los datos confidenciales creados y procesados por la aplicación de acuerdo con una política de tratamiento de los datos confidenciales.			X
8.3.5	Verificación que el acceso a los datos confidenciales se audita (sin registrar los datos confidenciales en sí mismos), si los datos se recopilan según las directivas de protección de datos relevantes o cuando se requiere el registro de acceso.			X
8.3.6	Verifique que la información confidencial contenida en la memoria se sobrescriba tan pronto como ya no sea necesaria para mitigar los ataques de volcado de memoria, utilizando ceros o datos aleatorios.			X
8.3.7	Verifique que la información confidencial o privada que debe estar encriptada, esté encriptada utilizando algoritmos aprobados que brinden confidencialidad e integridad.			X
8.3.8.	Verifique que la información personal confidencial esté sujeta a la clasificación de retención de datos, de manera que los datos antiguos o desactualizados se eliminen automáticamente, según lo programado, o según lo requiera la situación.			X

V9: Requisitos de verificación de comunicaciones

V9.1 Requisitos de seguridad de comunicaciones

La aplicación utiliza protocolos de comunicaciones seguros y vigentes.

Item	Descripción	L1	L2	L3
9.1.1	Verifique que el TLS seguro se use para toda la conectividad del cliente y no recurra a protocolos inseguros o no cifrados.		X	X
9.1.2	Verifique mediante el uso de herramientas de prueba TLS en línea o actualizadas que solo estén habilitados los algoritmos, cifrados y protocolos sólidos, con los algoritmos y los cifrados más sólidos configurados como preferidos.		X	X
9.1.3	Verifique que las versiones anteriores de los protocolos SSL y TLS, los algoritmos, los cifrados y la configuración estén deshabilitados, como SSLv2, SSLv3 o TLS 1.0 y TLS 1.1. La última versión de TLS debería ser la suite de cifrado preferida.		X	X

V9.2 Requisitos de seguridad de comunicaciones del servidor.

Las aplicaciones web deben utilizar certificados autofirmados o generados internamente.

Item	Descripción	L1	L2	L3
9.2.1	Verifique que las conexiones hacia y desde el servidor utilicen certificados TLS de confianza. Cuando se utilizan certificados autofirmados o generados internamente, el servidor debe configurarse para que solo confíe en las CA internas específicas y en los certificados autofirmados específicos. Todos los demás deben ser rechazados.		X	
9.2.2	Verifique que las comunicaciones cifradas, como TLS, se utilicen para todas las conexiones entrantes y salientes, incluidas las conexiones de puertos de administración, monitoreo, autenticación, API o servicio web, bases de datos, nube, servidor, mainframe, externos y asociados. El servidor no debe		X	

	recurrir a protocolos inseguros o no cifrados.			
9.2.3	Verifique que todas las conexiones cifradas a sistemas externos que involucren información o funciones confidenciales estén autenticadas.		X	
9.2.4	Verifique que la revocación de la certificación adecuada, como el Grapado del Protocolo de estado de certificado en línea (OCSP), esté habilitada y configurada.		X	
9.2.5	Verifique que las fallas de la conexión TLS del back-end estén registradas.		X	

V10: Requisitos de verificación de código malicioso

V10.1 Controles de integridad de código.

En el desarrollo de aplicaciones web se deben utilizar herramientas de análisis de código.

Item	Descripción	L1	L2	L3
10.1.1	Verifique que se esté utilizando una herramienta de análisis de código que pueda detectar códigos potencialmente maliciosos, como funciones de tiempo, operaciones de archivos no seguras y conexiones de red.		X	

V10.2 Búsqueda de código malicioso.

En el desarrollo web se deben utilizar bibliotecas de terceros y código fuente validado para que no contenga mecanismos de recolección de datos privados, maleware o generación de eventos innecesarios.

Item	Descripción	L1	L2	L3
10.2.1	Verifique que el código fuente de la aplicación y las bibliotecas de terceros no contengan capacidades de recopilación de datos o datos personales no autorizados. Donde exista dicha funcionalidad, obtenga el permiso del usuario para que funcione antes de recopilar datos.		X	
10.2.2	Verifique que la aplicación no solicite permisos innecesarios o excesivos para funciones o sensores relacionados con la privacidad, como contactos, cámaras, micrófonos o ubicación.		X	
10.2.3	Verifique que el código fuente de la aplicación y las bibliotecas de terceros no contengan puertas traseras, como cuentas o claves no documentadas o con código rígido, ofuscación de código, blobs binarios no documentados, rootkits o anti-depuración, funciones de depuración inseguras, o De lo contrario, no está actualizado, es una funcionalidad insegura u oculta que podría usarse de manera maliciosa si se descubre.		X	
10.2.4	Verifique que el código fuente de la aplicación y las bibliotecas de terceros no contengan bombas de tiempo buscando funciones relacionadas con la fecha y la hora.		X	
10.2.5	Verifique que el código fuente de la aplicación y las bibliotecas de terceros no contengan código malicioso, como ataques de salami, desvíos lógicos o bombas lógicas.		X	
10.2.6	Verifique que el código fuente de la aplicación y las bibliotecas de terceros no contengan huevos de Pascua ni ninguna otra funcionalidad potencialmente no deseada.		X	

V10.3 Controles de integridad de aplicación desplegados.

Los desarrollos web deben contemplar controles de actualización automática de sus componentes sin canales validados de actualización o de firma digital.

Item	Descripción	L1	L2	L3
10.3.1	Verifique si la aplicación tiene una característica de actualización automática del cliente o servidor, las actualizaciones deben obtenerse a través de canales seguros y firmarse digitalmente. El código de actualización debe validar la firma digital de la actualización antes de instalar o ejecutar la actualización.		X	
10.3.2	Verifique que la aplicación emplee protecciones de integridad, como la firma de código o la integridad de los sub-recursos. La aplicación no debe cargar ni ejecutar código de fuentes que no sean de confianza, como la inclusión de módulos, complementos, códigos o bibliotecas de fuentes que no sean de confianza o de Internet.		X	
10.3.3	Verifique que la aplicación tenga protección contra las tomas de subdominio si la aplicación se basa en entradas de DNS o subdominios de DNS, como nombres de dominio caducados, punteros de DNS o CNAME, caducados, proyectos caducados en repositorios de código fuente público, o API transitorias en la nube, funciones sin servidor o depósitos de almacenamiento (autogen-bucket-id.cloud.example.com) o similares. Las protecciones pueden incluir asegurarse de que los nombres DNS utilizados por las aplicaciones se verifican regularmente para ver si caducan o cambian.		X	

V11: Requisitos de verificación de la lógica de negocios

V11.1 Requisitos de seguridad de la lógica de negocios.

La aplicación web debe procesar únicamente la lógica de negocio de acuerdo con los privilegios o roles de los usuarios.

Item	Descripción	L1	L2	L3
11.1.1	Verifique que la aplicación solo procesará flujos de lógica de negocios para el mismo usuario en orden de pasos secuenciales y sin omitir pasos.		X	
11.1.2	Verifique que la aplicación solo procesará flujos de lógica de negocios con todos los pasos que se procesan en tiempo humano real, es decir, las transacciones no se envían demasiado rápido.		X	
11.1.3	Verifique que la aplicación tenga límites adecuados para acciones comerciales o transacciones específicas que se apliquen correctamente por usuario.		X	
11.1.4	Verifique que la aplicación tenga suficientes controles anti-automatizados para detectar y proteger contra la exfiltración de datos, solicitudes excesivas de lógica de negocios, cargas excesivas de archivos o ataques de denegación de servicio.		X	
11.1.5	Verifique que la aplicación tenga límites de lógica de negocios o validación para protegerse contra posibles riesgos o amenazas de negocios, identificados mediante modelos de amenazas o metodologías similares.		X	
11.1.6	Verifique que la aplicación no tenga problemas de "tiempo de verificación a tiempo de uso" (TOCTOU) u otras condiciones de carrera para operaciones delicadas.		X	
11.1.7	Verifique que la aplicación supervise eventos o actividades		X	

	inusuales desde una perspectiva de lógica empresarial. Por ejemplo, los intentos de realizar acciones fuera de orden o acciones que un usuario normal nunca intentaría.			
11.1.8	Verifique que la aplicación tenga alertas configurables cuando se detectan ataques automatizados o actividad inusual.		X	

V12: Requisitos de verificación de archivos y recursos

V12.1 Requisitos de carga de archivos.

En el desarrollo de aplicaciones web se debe controlar el tamaño de los archivos o la captura de archivos de gran tamaño o controles de malware en archivos comprimidos.

Item	Descripción	L1	L2	L3
12.1.1	Verifique que la aplicación no acepte archivos grandes que puedan llenar el almacenamiento o causar un ataque de denegación de servicio.		X	X
12.1.2	Verifique que los archivos comprimidos se verifiquen en busca de "zip bombs": pequeños archivos de entrada que se descomprimirán en archivos enormes, agotando así los límites de almacenamiento de archivos.		X	X
12.1.3	Verifique que se aplique una cuota de tamaño de archivo y un número máximo de archivos por usuario para garantizar que un solo usuario no pueda llenar el almacenamiento con demasiados archivos o archivos excesivamente grandes.		X	X

V12.2 Requisitos de integridad de archivos.

Las aplicaciones web deben controlar los archivos de fuentes no confiables para determinar un contenido pertinente a la funcionalidad requerida.

Item	Descripción	L1	L2	L3
12.2.1	Verifique que los archivos obtenidos de fuentes no confiables se validen para que sean del tipo esperado en función del contenido del archivo.		X	X

V12.3 Requisitos de ejecución de archivos.

Las aplicaciones web deben controlar los metadatos de los archivos para evitar su divulgación no autorizada.

Item	Descripción	L1	L2	L3
12.3.1	Verifique que los metadatos de nombre de archivo enviados por el usuario no se usen directamente con el sistema o el archivo de marco y la API de URL para protegerse contra el cruce de rutas.		X	X
12.3.2	Verifique que los metadatos de nombre de archivo enviados por el usuario se validen o se ignoren para evitar la divulgación, creación, actualización o eliminación de archivos locales (LFI).		X	X
12.3.3	Verifique que los metadatos de nombre de archivo enviados por el usuario se validen o se ignoren para evitar la divulgación o ejecución de archivos remotos (RFI), lo que también puede conducir a SSRF.		X	X
12.3.4	Verifique que la aplicación proteja contra la descarga de archivos reflexivos (RFD) al validar o ignorar los nombres de archivos enviados por el usuario en un parámetro JSON,		X	X

	JSONP o URL, el encabezado Content-Type de la respuesta debe configurarse en texto / sin formato, y el Contenido - Dispositivo de disposición debe tener un nombre de archivo fijo.			
12.3.5	Verifique que los metadatos de los archivos que no son de confianza no se usan directamente con la API del sistema o las bibliotecas, para proteger contra la inyección de comandos del sistema operativo.		X	X
12.3.6	Verifique que la aplicación no incluya y ejecute funciones de fuentes no confiables, como redes de distribución de contenido no verificadas, bibliotecas de JavaScript, bibliotecas de npm de nodo o DLL del lado del servidor.		X	X

V12.4 Requisitos de almacenamiento de archivos.

Las aplicaciones web deben controlar la fuente de archivos no confiables, los permisos asignados en el repositorio y que su almacenamiento no quede en la raíz web.

Item	Descripción	L1	L2	L3
12.4.1	Verifique que los archivos obtenidos de fuentes no confiables se almacenen fuera de la raíz web, con permisos limitados, preferiblemente con una validación sólida.		X	X
12.4.2	Verifique que los archivos obtenidos de fuentes no confiables sean analizados por los escáneres antivirus para evitar la carga de contenido malicioso conocido.		X	X

V12.5 Requisitos de descarga de archivos

Los desarrollos web deben controlar las extensiones de los archivos para evitar fuga de información y permisos de ejecución no autorizadas.

Item	Descripción	L1	L2	L3
12.5.1	Verifique que el nivel web esté configurado para servir solo archivos con extensiones de archivo específicas y necesarias para evitar la información no intencionada y la fuga de código fuente.		X	X
12.5.2	Verifique que las solicitudes directas a archivos cargados nunca se ejecutarán como contenido HTML / JavaScript.		X	X

V12.6 Requisitos de protección SSRF.

Las aplicaciones web deben controlar el uso de recursos informáticos para su funcionamiento mediante la validación de listas blancas.

Item	Descripción	L1	L2	L3
12.6.1	Verifique que el servidor web o de aplicaciones esté configurado con una lista blanca de recursos o sistemas a los que el servidor puede enviar solicitudes o cargar datos / archivos.		X	X

V13: Requisitos de verificación de servicios web y API

V13.1 Requisitos de verificación de seguridad del servicio web genérico.

En los desarrollos web se debe utilizar componentes con estándares de uso para la codificación o de acceso a funcionalidades de administración de recursos o de contenidos faltantes en las sentencias.

Item	Descripción	L1	L2	L3
13.1.1	Verifique que todos los componentes de la aplicación utilicen las mismas codificaciones y analizadores para evitar los ataques de análisis que explotan un comportamiento diferente de URI o de análisis de archivos que se podría usar en los ataques de SSRF y RFI.		X	X
13.1.2	Verifique que el acceso a las funciones de administración y administración esté limitado a los administradores autorizados.		X	X
13.1.3	Verifique que las URL de la API no expongan información confidencial, como la clave de la API, los tokens de sesión, etc.		X	X
13.1.4	Verifique que las decisiones de autorización se tomen tanto en la URI, aplicadas por la seguridad programática o declarativa en el controlador o enrutador, como en el nivel de recursos, aplicadas por los permisos basados en modelos.		X	X
13.1.5	Verifique que las solicitudes que contienen tipos de contenido faltantes o inesperados se rechacen con los encabezados apropiados (estado de respuesta HTTP 406 inaceptable o 415 tipo de medio no compatible).		X	X

V13.2 Requisitos de verificación del servicio web RESTful

La aplicación web debe utilizar métodos válidos para los usuarios de HTTP RESTful o uso de JSON para controlar los privilegios de DELETE o PUT o de recursos protegidos.

Item	Descripción	L1	L2	L3
13.2.1	Verifique que los métodos HTTP RESTful habilitados sean una opción válida para el usuario o la acción, como evitar que los usuarios normales utilicen DELETE o PUT en API o recursos protegidos		X	X
13.2.2	Verifique que la validación del esquema JSON esté en su lugar y verificada antes de aceptar la entrada.		X	X
13.2.3	Verifique que los servicios web RESTful que utilizan cookies están protegidos contra la falsificación de solicitudes entre sitios mediante el uso de al menos uno o más de los siguientes: patrón de cookies de envío triple o doble (ver referencias), CSRF o encabezado de solicitud ORIGIN cheques		X	X
13.2.4	Verifique que los servicios REST tengan controles anti-automatizados para protegerse contra llamadas excesivas, especialmente si la API no está autenticada.		X	X
13.2.5	Verifique que los servicios REST verifiquen explícitamente que el Tipo de contenido entrante sea el esperado, como application / xml o application / JSON.		X	X
13.2.6	Verifique que los encabezados de mensaje y la carga útil sean confiables y no se modifiquen en tránsito. Requerir un cifrado sólido para el transporte (solo TLS) puede ser suficiente en muchos casos, ya que brinda protección tanto de confidencialidad como de integridad. Las firmas digitales por mensaje pueden proporcionar una seguridad adicional además de las protecciones de transporte para aplicaciones de alta seguridad, pero conllevan una complejidad y riesgos adicionales para compararlos con los beneficios.		X	X

V13.3 Requisitos de verificación del servicio web SOAP.

Las aplicaciones web deben validar el uso de esquemas XSD para controlar la validación de campos para gestionar correctamente el dato.

Item	Descripción	L1	L2	L3
13.3.1	Verifique que se lleve a cabo la validación del esquema XSD para garantizar un documento XML correctamente formado, seguido de la validación de cada campo de entrada antes de que tenga lugar el procesamiento de esos datos.		X	X
13.3.2	Verifique que la carga útil del mensaje esté firmada mediante WS-Security para garantizar un transporte confiable entre el cliente y el servicio.		X	

V13.4 GraphQL y otros requisitos de seguridad de la capa de datos del servicio web.

La aplicación web debe utilizar listas blancas de consulta para evitar ataques de denegación de servicio o análisis de costos de consultas.

Item	Descripción	L1	L2	L3
13.4.1	Verifique que se debe usar la lista blanca de consultas o una combinación de limitación de profundidad y limitación de cantidad para evitar la denegación de servicio (DoS) de GraphQL o expresión de capa de datos como resultado de consultas anidadas y caras. Para escenarios más avanzados, se debe utilizar el análisis de costos de consulta.		X	
13.4.2	Verifique que GraphQL u otra lógica de autorización de capa de datos se debe implementar en la capa de lógica de negocios en lugar de la capa GraphQL		X	

V14: Requisitos de verificación de la configuración

V14.1 Construir.

En el desarrollo de aplicaciones web se controlar los procesos de compilación, alistamiento de plataformas y despliegue para identificar y ejecutar los controles así como las advertencias o registros de alertas en la plataforma tecnológicas que soportaran las aplicaciones web.

Item	Descripción	L1	L2	L3
14.1.1	Verifique que los procesos de compilación y despliegue de la aplicación se realicen de manera segura y repetible, como la automatización de CI / CD, la administración de configuración automatizada y los scripts de implementación automatizados.		X	X
14.1.2	Verifique que los indicadores del compilador estén configurados para habilitar todas las protecciones y advertencias de desbordamiento del búfer disponibles, incluida la aleatorización de la pila, la prevención de la ejecución de datos y para romper la compilación si se encuentran operaciones de puntero, memoria, cadena de formato, entero o cadena no seguras.		X	
14.1.3	Verifique que la configuración del servidor se refuerce según las recomendaciones del servidor de aplicaciones y los marcos en uso.		X	
14.1.4	Verifique que la aplicación, la configuración y todas las dependencias puedan volver a implementarse mediante scripts de implementación automatizada, compilarse a partir de un runbook documentado y probado en un tiempo razonable, o restaurarse desde copias de seguridad de manera oportuna.		X	
14.1.5	Verifique que los administradores autorizados puedan verificar la integridad de todas las configuraciones relevantes	X	X	

	para la seguridad para detectar la manipulación indebida.			

V14.2 Dependencia

En el desarrollo de aplicaciones web se debe verificar que todos los componentes estén actualizados y configurados con lo mínimo suficiente o con parámetros innecesarios.

Item	Descripción	L1	L2	L3
14.2.1	Verifique que todos los componentes estén actualizados, preferiblemente utilizando un verificador de dependencias durante el tiempo de compilación o compilación.		X	X
14.2.2	Verifique que se eliminen todas las características, la documentación, las muestras y las configuraciones innecesarias, como las aplicaciones de muestra, la documentación de la plataforma y los usuarios predeterminados o de ejemplo.		X	X
14.2.3	Verifique que si los activos de la aplicación, como las bibliotecas de JavaScript, las hojas de estilo CSS o las fuentes web, se alojan externamente en una red de entrega de contenido (CDN) o un proveedor externo, se utiliza la Subresource Integrity (SRI) para validar la integridad del activo.		X	X
14.2.4	Verifique que los componentes de terceros provengan de repositorios predefinidos, confiables y mantenidos continuamente.		X	X
14.2.5	Verifique que se mantenga un catálogo de inventario de todas las bibliotecas de terceros en uso.		X	X

V14.3 Requisitos de divulgación de seguridad no deseados.

En el desarrollo de aplicaciones web se debe controlar la generación de mensajes necesarios para dar respuestas personalizadas a los usuarios o de la publicación de información no necesaria de la plataforma.

Item	Descripción	L1	L2	L3
14.3.1	Verifique que la web o el servidor de aplicaciones y los mensajes de error del marco estén configurados para entregar respuestas personalizadas y procesables por el usuario para eliminar cualquier divulgación de seguridad no intencionada.		X	X
14.3.2	Verifique que la web o el servidor de aplicaciones y los modos de depuración del marco de la aplicación estén deshabilitados en la producción para eliminar las características de depuración, las consolas de desarrolladores y las revelaciones de seguridad no deseadas.		X	X
14.3.3	Verifique que los encabezados HTTP o cualquier parte de la respuesta HTTP no expongan información detallada de la versión de los componentes del sistema.		X	X

V14.4 Requisitos de encabezados de seguridad HTTP.

Las aplicaciones web deben controlar las respuestas HTTP y API, DOM, JSON o de inyección de código.

Item	Descripción	L1	L2	L3
14.4.1	Verifique que cada respuesta HTTP contenga un encabezado de tipo de contenido que especifique un conjunto de caracteres seguro (por ejemplo, UTF-8, ISO 8859-1).		X	X
14.4.2	Verifique que todas las respuestas API contengan Content-Disposition: attach; filename = "api.json" (u otro nombre de archivo apropiado para el tipo de contenido).		X	X
14.4.3	Verifique que exista una política de seguridad de contenido (CSPv2) que ayude a mitigar el impacto de ataques XSS como		X	X

	HTML, DOM, JSON y vulnerabilidades de inyección de JavaScript.			
14.4.4	Verifique que todas las respuestas contengan X-Content-Type-Options: nosniff.		X	X
14.4.5	Verifique que las cabeceras de Seguridad de transporte estricta de HTTP estén incluidas en todas las respuestas y para todos los subdominios, como Seguridad de transporte estricta: max-age = 15724800; includeSubdomains.		X	X
14.4.6	Verifique que se incluya un encabezado adecuado de "Política de referencia", como "sin referencia" o "del mismo origen".		X	X
14.4.7	Verifique que se esté utilizando un encabezado de Opciones de X-Frame o Política de Seguridad de Contenido: marcos-antepasados para sitios donde el contenido no debe estar incrustado en un sitio de terceros.		X	X

V14.5 Validar los requisitos de encabezado de solicitud HTTP.

La aplicación web debe controlar los métodos HTTP o API definidos.

Item	Descripción	L1	L2	L3
14.5.1	Verifique que el servidor de la aplicación solo acepte los métodos HTTP utilizados por la aplicación o la API, incluidas las OPCIONES previas al vuelo.		X	X
14.5.2	Verifique que el encabezado Origin suministrado no se usa para las decisiones de autenticación o control de acceso, ya que un atacante puede cambiar fácilmente el encabezado Origin.		X	X
14.5.3	Verifique que el encabezado Access-Control-Allow-Origin de recursos compartidos de dominio cruzado (CORS) use una lista blanca estricta de dominios de confianza con los que se comparen y no admita el origen "nulo".		X	X
14.5.4	Verifique que las cabeceras HTTP agregadas por un proxy de confianza o dispositivos SSO, como un token de portador, estén autenticadas por la aplicación.		X	X