Modelo de gestión de incidentes de seguridad alineado al negocio y con énfasis hacia la infraestructura de servidores de la Contraloría General de la Republica

Víctor Ferley Perea Asprilla

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

2018

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

MODELO DE GESTIÓN DE INCIDENTES DE SEGURIDAD ALINEADO AL NEGOCIO Y CON ÉNFASIS HACIA LA INFRAESTRUCTURA DE SERVIDORES DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA

ALUMNO: VÍCTOR FERLEY PEREA ASPRILLA

DIRECTOR: RICHARD GARCÍA RONDÓN

MAESTRÍA EN CIBERSEGURIDAD Y CIBERDEFENSA

TRABAJO DE GRADO PARA OPTAR AL TÍTULO DE MÁGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA

BOGOTÁ - COLOMBIA
2018

Ministerio de Defensa Nacional
Comando General de las Fuerzas Militares
Escuela Superior de Guerra
Maestría en Ciberseguridad y Ciberdefensa

Modelo de gestión de incidentes de seguridad alineado al negocio y con énfasis hacia la infraestructura de servidores de la contraloría general de la república

Víctor Ferley Perea Asprilla

Director
Richard García Rondón

Políticas y modelos en seguridad y defensa
Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá - Colombia
2018

Dedicatoria

Dedicado a mí familia, novia y amigos, por ser ese pilar y ese respaldo que siempre ha estado ahí a pesar de las situaciones, gracias por haber sido tan incondicionales para conmigo.

Agradecimientos

Gracias a Dios por darme la fortaleza y sabiduría necesaria para sacar adelante mis estudios. Gracias a mis padres, hermanos, a mi novia Vania, y aquellos familiares y amigos por siempre haber estado cuando les necesité. Gracias a los funcionarios de la Contraloría General de la República y especial a los pertenecientes a la oficina de sistemas por su apoyo incondicional, a la ingeniera Victoria E. Díaz directora de la oficina, la ingeniera Gloria Amanda Cruz y en especial al ingeniero Mario Yepes por ser un hermano en el trabajo. Gracias al ingeniero Richard García por la orientación tan acertada para el desarrollo de esta monografía y gracias a toda la comunidad educativa de la ESDEGUE.

Resumen ejecutivo

La Contraloría General de la República, al igual que cualquier entidad estatal en alineación con la política nacional de seguridad digital se encuentra en la necesidad de fortalecer la seguridad de sus sistemas informáticos; de modo, que pueda garantizar la continuidad del negocio ante la ocurrencia de incidentes de seguridad que lleguen a afectarla. Aunque si bien, la entidad ha dado fuertes avances en torno al tema, le hacen falta definir procesos y recursos orientados específicamente hacia el campo de la ciberseguridad que permitan conocer el que hacer en el momento de ocurrencia de eventos relacionados con ataques informáticos hacia la infraestructura de los servidores de la entidad. Es así que mediante la utilización de una metodología de investigación proyectiva, se pretende dar solución práctica al problema basando su desarrollo en 3 actividades estructuradas de la siguiente forma:

- El análisis de antecedentes, normas vigentes y algunos modelos existentes que pueden ser tomados como base de partida.
- la realización de un cruce de información con el fin de conocer el estado y las necesidades específicas de la entidad respecto a la seguridad de su información.
- Planteamiento de una propuesta sintetizada en un modelo de gestión de incidentes de seguridad ajustado a las necesidades de la entidad.

Como tal; el producto final de este documento, concluye con la propuesta de un modelo de gestión de incidentes de seguridad de la información alineado al negocio de la Contraloría General de la República y aplicable a su plataforma de servidores.

Palabras clave:

Ciberseguridad, control fiscal, contraloría, incidente, seguridad, modelo de gestión

Abstract

The Colombian Supreme Audit Institution (Contraloría General de la República CGR), as an institutional entity in compliance with national digital security policy has the need to fortify the security of its information systems, so that it can guarantee the business continuity in case of security incidents occurrence that may affect it and although the entity has made strong advances around the issue, it need to define processes and resources targeted toward cybersecurity that allow to know what to do at the time of events related to computer attacks to the server infrastructure of the institution. It's so by using a projective research methodology it is tried to give a practical solution to the problem, basing its development on 3 activities to know:

- The background analysis, current standards and some existing models that can be taken like starting base.
- The completion of an information survey in order to know the state and the specific needs of the institution regarding to the information security.
- A proposal synthesized in a security incident management model adjusted to the needs of the institution.

So; the final product proposed in this document, concludes with the proposal of a security incident management model aligned to the Contraloría General de la República business and applicable to its server infrastructure.

Key words:

Cybersecurity, fiscal control, comptroller, incident, security, management model.

Modelo de Gestión de incidentes de seguridad CGR.

Lista de Abreviaturas

BCP: Business Continuity Plan (Plan de Continuidad del Negocio)

BID: Banco Interamericano de Desarrollo.

CCD: Centro de Excelencia para la Cooperación en Ciberdefensa.

CCIT: Cámara Colombiana de Informática y Telecomunicaciones.

CCOC: Comando Conjunto Cibernético.

CCP: Centro Cibernético Policial.

CIMF: Ciber Incident Management Framework (Marco de gestión de incidentes cibernéticos)

CGR: Contraloría general de la república.

COINFO: Comisión Intersectorial de Política y Gestión de Información en la Administración Pública

ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Ministerio de Defensa de Colombia).

CONPES: Consejo Nacional de Política Económica y Social.

CVE: Common Vulnerabilities and Exposures (Vulnerabilidades y exposiciones communes)

DANE: Departamento Administrativo Nacional de Estadística.

DMA: Direct Memory Access (Acceso Directo a Memoria).

DRP: Disaster Recovery Plan (Plan de Recuperación de Desastres).

CRC: Comisión de Regulación de Comunicaciones

CSIRT: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad informática.

ENISA: European Network and Information Security Agency (Agencia de seguridad de la información y la red europea).

Modelo de Gestión de incidentes de seguridad CGR.

FBI: Federal Bureau of Investigation (Oficina Federal de Investigación)

HTTPS: Hyper Text Transfer Protocol Secure (Protocolo Seguro de Transferencia de Hipertexto)

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional)

IPS: Intrusión prevention Sistem (sistema para prevención de intrusos).

ISO: International Organization for Standarization (Organización Internacional de Normalización)

MinTIC: Ministerio de Tecnologías de la Información y las comunicaciones.

NIST: National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología)

NVD: National Vulnerability Database (Base de datos nacional de vulnerabilidades de EEUU)

OEA: Organización de Estados Americanos.

OSEI: Oficina de Sistemas e Informática.

SAN: Storage Area Network (Red de Area de Almacenamiento)

SCIGC: Sistema de Control Interno y Gestión de Calidad.

SGSI: Sistema de Gestión de Seguridad de la Información.

SSH: Secure Shell (Consola segura)

USATI: Unidad de Seguridad y Aseguramiento Tecnológico e Informático.

WAF: Web Aplication Firewall (Firewall de aplicaciones web)

Contenido

Objetivos del Proyecto

El objetivo principal del proyecto consiste en desarrollar un modelo de gestión de incidentes de seguridad de la información alineado al negocio de la Contraloría General de la República (en adelante CGR) y aplicable a su plataforma de servidores. El alcance de este objetivo se logrará mediante los siguientes objetivos específicos:

1. Desarrollar el análisis con el objeto de proponer las herramientas necesarias para la elaboración del modelo de gestión de incidentes adaptado a la CGR.
2. Desarrollar el análisis con el objeto de proponer los procedimientos necesarios para la elaboración del modelo de gestión de incidentes adaptado a la CGR.
3. desarrollar el análisis con el objeto de proponer los recursos humanos y sus competencias necesarias para la elaboración del modelo de gestión de incidentes adaptado a la CGR.

Para el logro de los mismos el proyecto contempla un desarrollo en tres pasos:

- El estudio de los antecedentes de mayor relevancia que han conformado lo que significa la gestión de incidentes en la actualidad, con el fin de tener las bases necesarias para proponer un modelo ajustado a los estándares de mayor recomendación.
- Un análisis de la realidad actual de la plataforma con base en el negocio y la gestión del riesgo, con el fin de proponer un modelo ajustado a las necesidades de la entidad, en relación con su infraestructura y en concordancia con los objetivos misionales de la entidad.
- Propuesta de un modelo de gestión de incidentes con su respectiva descripción de procedimientos, herramientas y talento humano necesarios para la aplicación del modelo en la entidad.

Metodología

Hurtado (2000) en su libro Metodología de la investigación holística describe la investigación proyectiva como aquella que consiste en:

> La elaboración de una propuesta o de un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social o de una institución, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y las tendencias futuras. (p.325).

Lo que en resumen, se puede interpretar como aquella que permite el desarrollo de inventos, modelos, diseños, programas, etc. como solución a problemas prácticos; con base, en un diagnóstico preciso del problema o las necesidades. (Hurtado Barrera, 2000).

Basado en ello, el desarrollo de este documento hace uso de una metodología de investigación proyectiva, debido, principalmente, a que el mismo contempla la elaboración de un modelo a partir de necesidades detectadas en torno al área de tecnología de la Contraloría General de la República (CGR), necesidades que corresponden a la implementación de procedimientos, herramientas y recursos necesarios para la adecuada gestión de incidentes de seguridad a nivel de esta entidad. La correcta utilización de esta metodología no solo permite la identificación clara del problema a resolver y sus posibles causas; sino, que permite plantear propuestas de valor con base en las mismas, consolidándose en un producto final útil para la entidad, permitiéndole contar con procedimientos eficientes para la respuesta a incidentes de seguridad en su plataforma de servidores.

En síntesis esta metodología permite no solo describir el "¿qué está ocurriendo?" y sus posibles causas, sino, igualmente determinar el "¿qué se quiere?", "¿cómo hacerlo?", las alternativas posibles y lo más importante: presentar propuestas que contribuyan con una solución adecuada con base en los problemas detectados durante el proceso objeto de la investigación.

Introducción

El estado colombiano mediante documento CONPES 3854 de 2016 estableció la política nacional de seguridad digital, la cual, reconoce la gestión del riesgo como uno de los elementos más importantes para la seguridad digital, y en acuerdo con la estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC establece una política que involucra a todas las partes; tanto privadas, como públicas, con el fin de fortalecer la capacidades de las mismas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades de negocio en el entorno digital (Consejo Nacional de Política Económica y Social, 2016). De esta forma la Contraloría General de la República, como ente institucional a la cabeza del control fiscal, se encuentra en la obligación no solo de facilitar el acceso a los ciudadanos mediante medios digitales e internet a los servicios prestados por la entidad, sino también, de cumplir con las recomendaciones y pautas de seguridad necesaria con el fin de garantizar la continuidad del negocio mediante la debida protección de su información. Lo que conlleva; además, de una fuerte inversión en tecnología, la preparación del personal, al igual que la implementación y aplicación de modelos que permitan recuperar la operatividad del negocio en caso eventos de seguridad, pérdidas de información o desastres informáticos.

La importancia de estas medidas de seguridad para proteger la información radica principalmente en el alto número de delitos informáticos[1], los cuales, se han visto impulsados principalmente por el uso masivo de internet y la gran cantidad de dispositivos conectados[2] que de múltiples formas facilitan en gran medida el actuar de los delincuentes cibernéticos, tomando más relevancia aún si se considera el papel que juega la Contraloría General de la República como primer ente de control fiscal del país, dado que la hacen un digno candidato a sufrir ciberataques, ya que en sus bases de datos reposa una gran cantidad de información sensible constituida principalmente por denuncias ciudadanas de malos manejos de recursos públicos, procesos de responsabilidad fiscal, boletín de responsables fiscales y nómina de empleados, entre otros. (Contraloría General de la República, 2014).

---

[1] 13.774 casos reportados para Colombia entre el 2014 y el 2017 (Policía Nacional, 2017)

[2] 4900 millones de dispositivos conectados para marzo de 2017 según informes del Centro cibernético Policial CCP (Policía Nacional, 2017).

Modelo de Gestión de incidentes de seguridad CGR.

De hecho, dada la sensibilidad e importancia de la información, la entidad dentro de sus iniciativas, a fin de proteger la misma, cuenta con un moderno sistema de copias de seguridad, un eficiente sistema de dispositivos perimetrales, un plan de recuperación de desastres y un proceso de gestión de incidentes implementado recientemente. Aunque si bien; el plan se encuentra en proceso de implementación, este ha permitido visualizar falencias donde es clara la necesidad de un refuerzo en seguridad sobre todo a nivel de procedimientos que no han sido cubiertos por actual proceso de gestión de incidentes por tratarse de temas muy específicos a nivel de seguridad y que impactan mayormente a la plataforma de servidores que sustentan el negocio a nivel informático. Esta situación ha llevado al planteamiento de la pregunta de investigación que se pretende resolver con la elaboración de este documento: ¿Cómo contar con procedimientos establecidos a nivel de la Contraloría General de la República que permitan reducir el riesgo producido por las amenazas existentes sobre la infraestructura de servidores y reaccionar ante los posibles ciberataques a la misma?

La solución a esta interrogante plantea la elaboración de este proyecto, donde se contempla un modelo de gestión de incidentes de seguridad aplicado específicamente a las necesidades de la plataforma de servidores, pero con el potencial de poder ser utilizado en otras entidades con simples modificaciones al mismo.

1. Capítulo Uno – Análisis de Antecedentes.

La elaboración de un modelo de incidentes de seguridad requiere en gran parte del conocimiento de aquellas normas y referentes que han permitido el desarrollo de los distintos modelos actualmente existentes. Con el desarrollo de este análisis se espera obtener las bases necesarias para estructurar el modelo de gestión de incidentes de seguridad propuesto.

1.1. Marco Normativo

El proceso de gestión de incidentes nace debido a la necesidad de brindar a una comunidad objetivo: llámese empresa, gobierno, entidad o persona; las herramientas necesarias para gestionar, prevenir o reparar de manera rápida y efectiva los eventos que sin formar parte de la operación estándar del negocio, lo afecten de forma negativa, ya sea reduciendo u interrumpiendo la calidad de los servicios prestados en el desarrollo del mismo.

En relación con el proceso de gestión de incidentes el concepto no es nada nuevo, ya que, de hecho existen modelos orientados su desarrollo y aplicación, de los cuales para el presente estudio se tendrán en cuenta los siguientes:

1.1.1. ITIL.

El conjunto de lineamientos y buenas prácticas para la gestión de los servicios de tecnología informática ITIL (Information Technology Infraestructure Library) ofrece una guía para la prestación de servicios de Tecnologías de la Información (llámese TI) con calidad, orientados hacia procesos y totalmente alineados hacia las necesidades del negocio. Su edición actual correspondiente a ITIL V3 edición 2011 o ITIL 2011, representa una mejora a la versión 3 del 2007, por lo que no es considerada como una nueva versión, sino como una actualización de esta. La misma corrige algunas inconsistencias que existían a nivel de diagramas y textos en la versión 3, además de introducir algunos nuevos procesos a la misma. ITIL 2011 propone un ciclo de vida del servicio conformado por 5 etapas (ver Figura 1) constituidas por cerca de 32 diferentes procesos y funciones entre las cuales se contempla la gestión de incidentes como un proceso enmarcado en la fase de operación del servicio (Best Management Practice, 2011).

Modelo de Gestión de incidentes de seguridad CGR.

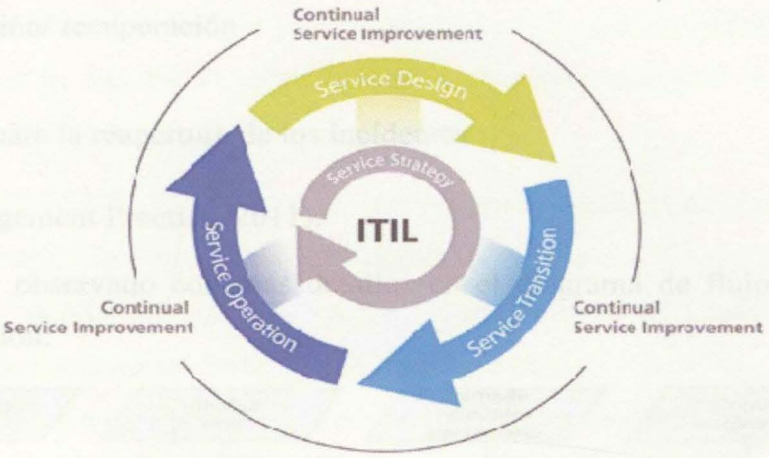

Figura 1. Ciclo del servicio ITIL. Recuperado de: https://iaap.files.wordpress.com/2015/03/itil_v3_cms.gif

ITIL 2011 define la gestión de incidentes como el proceso encargado de manejar o gestionar ciclo de vida de todos los incidentes; definiendo incidente como la reducción de la calidad o interrupción no planeada de un servicio de TI, o la falla de algún elemento de configuración (así este no haya impactado aún el servicio). La gestión de incidentes según ITIL, tiene como principal objetivo de restaurar la operatividad del negocio de la manera más rápida posible, minimizando el impacto negativo sobre la operatividad normal del mismo (Best Management Practice, 2011). Entendiéndose operatividad normal como aquella que se encuentra dentro de los límites acordados o ANS (Acuerdos de nivel de servicio).

El incidente según ITIL, debe contar, no solo, con un modelo de incidencia que los registre o tipifique de una forma que permita optimizar el proceso de resolución del problema, sino que también debe de contar con un proceso para la gestión del incidente, conformado por las siguientes actividades:

- Identificación
- Registro
- Categorización
- Priorización
- Diagnóstico inicial
- Escalado
- Investigación y diagnóstico

Modelo de Gestión de incidentes de seguridad CGR.

- Resolución/ recuperación
- Cierre
- Reglas para la reapertura de los incidentes

(Best Management Practice, 2011).

Lo que puede ser observado con más detalle en el diagrama de flujos de la Figura 2 presentado a continuación:

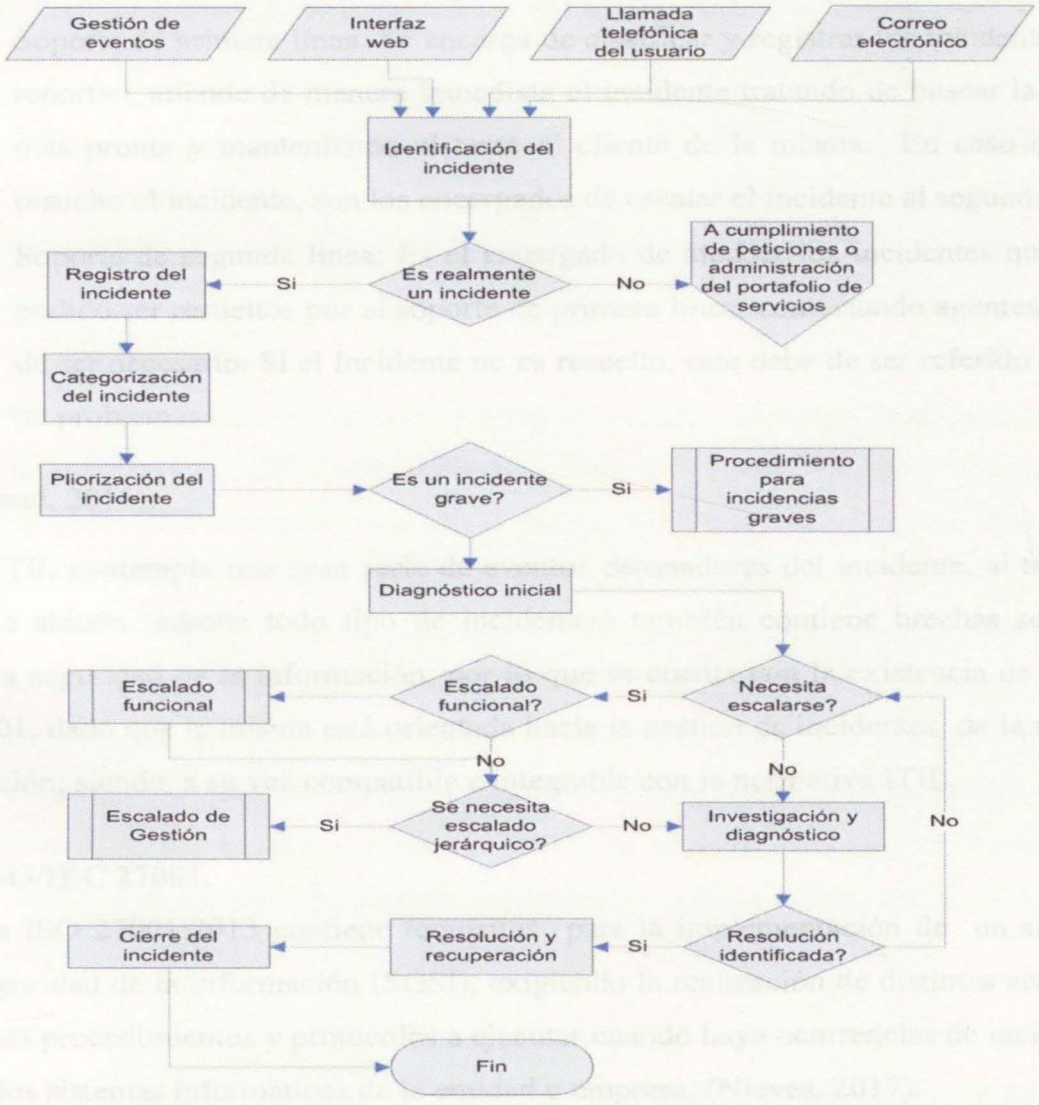

Figura 2. Diagrama del Proceso de Gestión de Incidencia. Traducido de: ITIL Service operation (Best Management Practice, 2011).

Modelo de Gestión de incidentes de seguridad CGR.

La gestión de incidentes desde el punto de vista de ITIL incluye cualquier evento que pueda interrumpir o interrumpa un servicio y/o que puedan ser reportados por los usuarios, incluyendo fallas del sistema, caída de la red, fallas eléctricas, etc. Implementado para la atención de los mismos una serie de roles conformados de la siguiente forma:

- Gestor del incidente: El responsable de la implementación del proceso de gestión y de elaborar los informes correspondientes.
- Equipo de incidentes graves: Es un grupo multidisciplinario encargado de solucionar los incidentes catalogados como graves.
- Soporte de primera línea: Se encarga de clasificar y registrar los incidentes que se reportan, atiende de manera inmediata el incidente tratando de buscar la solución más pronta y manteniendo al tanto al cliente de la misma. En caso de no ser resuelto el incidente, son los encargados de escalar el incidente al segundo nivel.
- Soporte de segunda línea: Es el encargado de atender los incidentes que no han podido ser resueltos por el soporte de primera línea, contactando agentes externos de ser necesario. Si el incidente no es resuelto, este debe de ser referido a gestión de problemas.

(Baud, 2015).

Si bien, ITIL contempla una gran serie de eventos detonadores del incidente, al tratarse de una normativa abierta (admite todo tipo de incidentes) también contiene brechas sobre todo orientadas a la seguridad de la información, por lo que se cuenta con la existencia de la norma ISO/IEC 27001, dado que la misma está orientada hacia la gestión de incidentes de la seguridad de la información; siendo, a su vez compatible e integrable con la normativa ITIL.

1.1.2. ISO/IEC 27001.

La norma ISO 27001:2013 contiene requisitos para la implementación de un sistema de gestión de seguridad de la información (SGSI), exigiendo la realización de distintas actividades, como lo son los procedimientos y protocolos a ejecutar cuando haya ocurrencias de incidentes de seguridad en los sistemas informáticos de la entidad o empresa. (Nieves, 2017).

Vale la pena mencionar, que al igual que el sistema ISO 27001 existen varias normas que simplemente corresponden a un conjunto de políticas orientadas hacia la seguridad de la

información, buscando garantizar la confidencialidad, la integridad y la disponibilidad (CID) de la misma, y reduciendo a su vez los riesgos inherentes a esta. Entre este conjunto de políticas o normas destacan:

- COBIT 5 (Control Objectives for Information and related Technology): Si bien, esta norma corresponde a una guía de mejores prácticas orientada al control y supervisión de tecnologías de la información, su marco de referencia como tal incluye la gestión de los riesgos de TI, permitiendo a su vez el desarrollo de políticas claras y buenas prácticas para la gestión de estas tecnologías, lo que garantiza el cumplimiento, la privacidad, la seguridad y la continuidad del negocio con base en la aplicación de controles más amplios que la norma ISO 27001 en torno a la seguridad de la información. (Preittigun, Chantatub, & Vatanasakdakul, 2012).
- SOGP (Information Security Forum's Standard of Good Practice): Se encuentra orientado hacia el uso de buenas prácticas con base en un conjunto de experiencias previas.
- ISM3 (Information Security Management Maturity Model): Construida con base a estándares como ITIL, ISO 9001 y algunos otros más, puede ser utilizada como plantilla para cumplimiento del estándar ISO 9001. Se basa en procesos, al contrario del ISO 27001 que está basada en controles (Sanchez Crespo, 2006).
- UNE 71502:2004 Norma española que establece especificaciones para los SGSI y se encuentra basada en la norma BS7799-2:2002, la cual, fue publicada por BSI (British Standards Institution) en el año 2006. Está dedicada a la gestión de riesgos de seguridad de la información, y contiene requisitos para establecer, implantar, documentar y evaluar un SGSI de acuerdo a los riesgos identificados a nivel de la entidad, empresa u organización. Dicha norma cedió su lugar a la norma ISO 27001 de alcance internacional. (Pardo Cuenca, 2015).

Si bien, todas estas normas son importantes, es necesario centrarse en una norma de amplia utilización como lo es la norma ISO/IEC 27001, por lo que se proporciona una información más amplia de esta, sin que ello desmerite el papel que han tenido otras normas en el desarrollo de la gestión y gobierno de las tecnologías de la información, en especial en lo relacionado con el

proceso de gestión de incidentes de seguridad de la información (International Organization for Standardization , 2013).

Es claro que garantizar la seguridad de la totalidad de la información es algo prácticamente imposible (esto demandaría un costo demasiado elevado), un sistema de seguridad de la información busca garantizar no solo que se conozcan los riesgos con respecto a la seguridad de dicha información, sino que los mismos se asuman, se gestionen y posteriormente se minimicen por parte de la organización, documentándolos, clasificándolos y organizándolos de la forma más eficiente posible, por lo que la gestión del riesgo no solo es un componente fundamental de cualquier SGSI sino que en algún momento determina la viabilidad de las elaboración y ejecución de un proyecto dado; esto debido, a que si los riesgos contemplados resultan ser muy altos o de muy alto costo para el proyecto, el mismo terminará siendo desechado.

La implementación de un SGSI con base en la norma ISO 27001 contempla el seguimiento de un ciclo de mejora continua PDCA denominado ciclo Deming como el que se muestra en la Figura 3 a continuación:

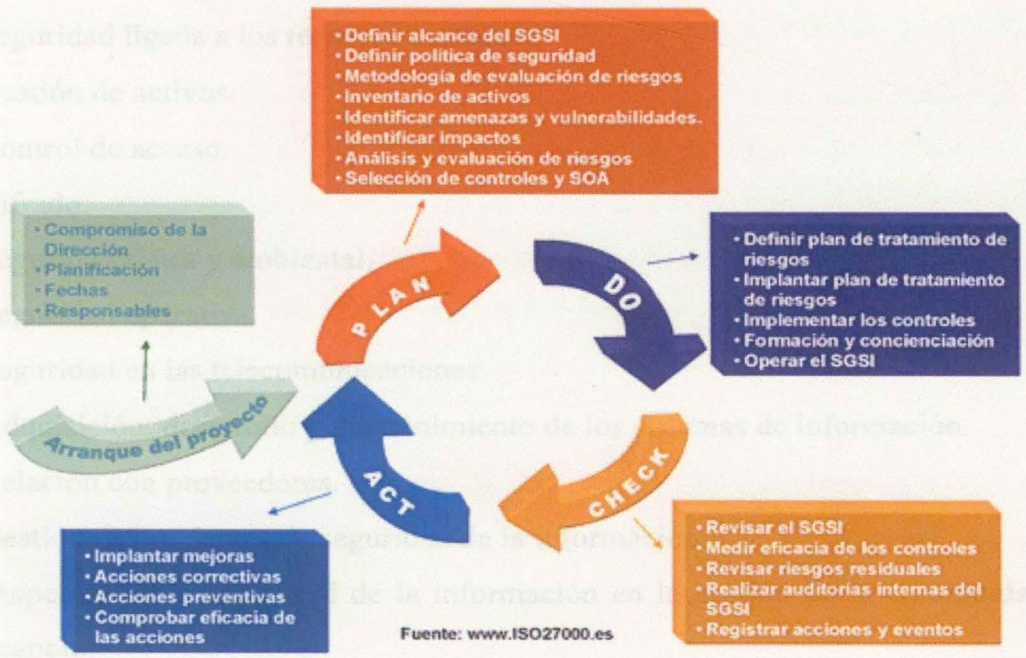

Figura 3. Ciclo PDCA. Recuperado de www.iso27000.es

Modelo de Gestión de incidentes de seguridad CGR.

Este ciclo se encuentra constituido por las etapas de planificar, hacer, verificar y actuar, lo que se constituye en la columna vertebral de la metodología utilizada por la norma, permitiendo mejorar continuamente una vez se inicie el proyecto, logrando que con el avance del tiempo se vayan superando los distintos inconvenientes surgidos durante la ejecución de este.

1.1.3. ISO/IEC 27002.

Denominado anteriormente como ISO 17799 la norma ISO/IEC 27002 es un estándar para la seguridad de la información implementado con el fin de proporcionar recomendaciones en pro de las mejores prácticas en la gestión de la seguridad de la información; preservando la confidencialidad, la integridad y la disponibilidad de la misma. Al contrario de la norma ISO 27001 no distingue entre cuales controles pueden ser aplicables y cuáles no, dado que no exige una evaluación del riesgo como sucede con la ISO 27001, y más importante aún, ISO 27002 no es una norma de gestión certificable como si ocurre con ISO 27001, aunque esta ofrece un mayor número de detalles (Huacanés Chávez, 2016). La norma está conformada por alrededor de 14 dominios, los cuales se muestran resumidos a continuación:

- Políticas de Seguridad.
- Aspectos organizativos de la Seguridad de la Información.
- Seguridad ligada a los recursos humanos.
- Gestión de activos.
- Control de acceso.
- Cifrado.
- Seguridad física y ambiental.
- Seguridad operativa.
- Seguridad en las telecomunicaciones.
- Adquisición, desarrollo y mantenimiento de los sistemas de información.
- Relación con proveedores.
- Gestión de incidentes de seguridad de la información.
- Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento. (iso27000.es, 2013).

Modelo de Gestión de incidentes de seguridad CGR.

1.1.4. NIST SP 800: Modelo de ciberseguridad.

El instituto nacional de normas y tecnología NIST, por sus siglas en inglés (National Institute of Standards and Technology), quien realiza implementación de estándares en estado unidos, cuenta con una recopilación de documentos en torno a las tecnologías de la información publicados mediante el estándar NIST SP 800; los cuales, se caracterizan por ser muy didácticos y contar con una gran practicidad a diferencia de la norma ISO 27001, que contiene una clara tendencia hacia la evaluación del riesgo y que pesar de ser menos amigable tiende a contemplar no solo políticas y procedimientos sino también elementos de seguridad del personal, procedimiento de operación, sensibilización en seguridad informática, reglamentación para entornos de seguridad, etc. El NIST SP 800 puede ser una alternativa bastante buena como orientación para la aplicación de los controles de la norma ISO 27001 remplazando en esta tarea la consecuente norma ISO 27002, dado que como se afirmó anteriormente, el NIST SP 800 se trata de una recolección de documentos creados con el fin de brindar herramientas efectivas para la gestión de la seguridad de la información y la evaluación del riesgo, cubriendo tanto la gestión, como la parte operativa en la seguridad de la información y conteniendo como tal un amplio margen de estándares como el caso del documento NIST SP 800-61 que pertenece a una guía para gestionar incidentes de seguridad y que será tratado con un poco más de detalle a medida que avance este documento. (National Institute of Standards and Technology, 2017)

El NIST posee bajo su autoría la publicación de un marco para el mejoramiento de la ciberseguridad en infraestructuras críticas, marco que ha servido no solo como referencia, sino también como punto de partida para muchas de las políticas de ciberseguridad utilizadas en gran variedad de empresas, dado que el mismo contiene un conjunto específico de actividades que tienen como finalidad el logro de resultados orientados hacia la seguridad de la información mediante la utilización de variados ejemplos didácticos. (National Institute of Standards and Technology, 2017).

Las actividades contempladas por la norma se encuentran representadas en cinco etapas correspondientes a identificación, protección, detección, respuesta y recuperación; como se observa en la Figura 4.

Modelo de Gestión de incidentes de seguridad CGR.

Figura 4. Estructura del modelo NIST. Recuperado de NIST SP 800 Estándard (National Institute of Standards and Technology, 2017)

Cada una de las etapas de este modelo provee un acercamiento flexible, repetible con alto desempeño y de bajo costo en la administración del riesgo relacionado con la seguridad de la información y los sistemas informáticos de la empresa o entidad. (National Institute of Standards and Technology, 2017)

1.1.5. CONPES 3701 de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa.

El Consejo Nacional de Política Económica y Social (CONPES) dio el primer paso en materia ciber hacia el año 2011 con la publicación de este documento, el cual buscaba generar lineamientos de política en ciberseguridad y ciberdefensa con el objetivo de desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que de una u otra forma puedan afectar el país (Consejo Nacional de Politica Económica y Social, 2011). Para el momento del desarrollo de esta política el estado no contaba con una estrategia clara para enfrentar las amenazas cibernéticas de la época, por lo que este disponía de una capacidad muy limitada para responder ciberataques que se presentasen llegado el momento.

El documento CONPES, se realiza un breve análisis de la situación del país para dicha época centrándose en el sector tecnología. Listando por medio de este análisis un cuadro con iniciativas nacionales e internacionales, que de una u otra forma no solo sirvieron como insumo para su elaboración, sino que permitieron el desarrollo y la aplicación del documento mismo, de acuerdo a las necesidades presentadas por el estado en materia de ciberseguridad.

Modelo de Gestión de incidentes de seguridad CGR.

Para el logro de sus objetivos el CONPES 3701 contempla la creación de 4 instancias (Figura 5) conformadas por:

- Comisión intersectorial
- ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- CCP: Centro Cibernético Policial.
- CCOC: Comando Conjunto Cibernético.

Figura 5. Modelo de Coordinación. Recuperado de CONPES 3701 (Consejo Nacional de Politica Económica y Social, 2011)

La comisión intersectorial tiene la función de fijar una visión estratégica de la gestión de la información, al igual, que de establecer los lineamientos de política respecto a la gestión de la infraestructura, la información pública y por último, la ciberseguridad y la ciberdefensa. Es conformada por el presidente de la república y estar integrada, como mínimo por el alto asesor para la seguridad nacional, el ministro de defensa nacional, el ministro de tecnologías de información y comunicaciones, el director de planeación nacional, y el coordinador del ColCERT.

El ColCERT uno de los grupos creados con el fin de atender las distintas emergencias cibernéticas que se puedan presentar mediante reportes realizados por los distintos sujetos,

entidades o empresas. Es el coordinador a nivel nacional en aspectos relacionados con la ciberseguridad y la ciberdefensa, prestando apoyo y colaboración a instancias como el Centro Cibernético Policial CCP, el Comando Conjunto Cibernético CCOC y los distintos grupos de ciberseguridad y ciberdefensa pertenecientes a distintas empresas y entidades del estado (Figura 6). Está conformado por personal perteneciente al Ministerio de Defensa Nacional, entre los que se destacan personal civil, militar y algunos designados por otras entidades del estado (Consejo Nacional de Politica Económica y Social, 2011).

Figura 6. Modelo Relacional del colCERT. Recuperado de Ministerio de Defensa Nacional, Colombia.

El Comando Conjunto Cibernético CCOC perteneciente a las fuerzas militares tiene la labor de defender y contrarrestar las amenazas cibernéticas que afecten los intereses nacionales y se encuentra encabezado por su comando general, el cual toma decisiones y coordina acciones con la ayuda del ColCERT (Consejo Nacional de Politica Económica y Social, 2011).

El Centro Cibernético Policial CCP a cargo de la policía se encarga de brindar apoyo la ciudadanía en temas de ciberseguridad, dando respuesta operativa a estos delitos y desarrollando labores de información y prevención (Consejo Nacional de Politica Económica y Social, 2011).

1.1.6. CONPES 3854 de 2016: Política Nacional de Seguridad Digital.

Con el objetivo claro de "fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital" (Consejo Nacional de Política Económica y Social, 2016), esta política nace para complementar la política CONPES 3701 y con el fin de

contrarrestar el incremento de las amenazas cibernéticas, partiendo de los objetivos de la defensa del país y la lucha contra el cibercrimen. Esta política se basa en la gestión del riesgo como uno de sus elementos principales, para lo que parte de 4 principios fundamentales y 5 dimensiones estratégicas.

Como plan de acción para alcanzar su objetivo el CONPES 3854 propone:

- Establecer un marco institucional para la seguridad de la información desde el enfoque de la gestión del riesgo.
- Implementar la política de seguridad digital, haciendo uso de un marco institucional orientado hacia la articulación de las múltiples partes interesadas.
- Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital
- Crear espacios que faciliten la gestión del riesgo de las múltiples partes autorizadas.
- Desde el punto de gestión del riesgo, fortalecer la seguridad tanto del estado, como la de los individuos.
- Generar mecanismos para impulsar la cooperación desde el punto de vista de la seguridad digital.

(Consejo Nacional de Política Económica y Social, 2016)

1.2. Marco de Referencia - Modelos y/o Guías Para Gestión de Incidentes de Seguridad

Dado el objetivo principal de este documento correspondiente a el diseño de un "Modelo de gestión de incidentes de seguridad de la información alineado al negocio de la contraloría general de la república", se hace importante conocer no solo el estado actual de la contraloría en materia de gestión de incidentes, sino igualmente, que otros modelos o guías existen que pueden ser aplicables o servir como referentes para el modelo a desarrollar, por lo que este marco de referencia comprende los siguientes elementos:

1.2.1. Gestión de incidentes en la contraloría general.

En cumplimiento con el Consejo Nacional de Política Económica y Social de la República de Colombia, quien mediante documento CONPES 3701 del 14 de julio de 2011 fijó los

lineamientos de la política para ciberseguridad y ciberdefensa, buscando generar mecanismos efectivos que permitan garantizar la seguridad de la información a nivel nacional, y en alineación con la estrategia 2.0 del programa gobierno en línea mediante la cual el estado colombiano adopta un modelo de seguridad de información basado en la necesidad de reconocer la seguridad informática como un factor primordial para la apropiación de las TIC, a través de la aplicación de la norma técnica NTC: ISO/IEC 27001:2005 (Contraloría General de la República, 2014), la contraloría general mediante plan estratégico 2010-2014 denominado "*por un control fiscal oportuno y efectivo*" y mediante acta 003 del 29 de mayo de 2013 aprueba la "*Política de seguridad de la información*" (Contraloría General de la República, 2013), que contiene los criterios necesarios para garantizar en la entidad la gestión y la administración de la información de forma segura con base en los lineamientos contemplados en la norma ISO 27001.

Adicionalmente a esta política de seguridad de la información, la ley 1474 de 2011 correspondiente al estatuto anticorrupción, ordenó la creación de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático (USATI) con el fin principal consistente en:

> Prestar apoyo profesional y técnico para la formulación y ejecución de las políticas y programas de seguridad de los servidores públicos, de los bienes y de la información de la entidad, así como llevar el inventario y garantizar el uso adecuado y mantenimiento de los equipos de seguridad adquiridos o administrados por la Contraloría; promover la celebración de convenios con entidades u organismos nacionales e internacionales para garantizar la protección de las personas, la custodia de los bienes y la confidencialidad e integridad de los datos manejados por la institución. (Presidencia de la República, 2011, pág. 71)

Siendo por lo tanto la USATI la responsable de implementar los controles recomendados en la norma técnica colombiana NTC:ISO/IEC 27001:2005.

La contraloría general entre sus activos cuenta con una infraestructura formada por:

- Una plataforma de virtualización de 12 servidores de última generación que aloja un total de ciento cuarenta máquinas virtuales con sistemas operativos Linux, Unix, Windows.
- 16 servidores físicos operativos.
- 350TB de almacenamiento.

Modelo de Gestión de incidentes de seguridad CGR.

- Elementos de seguridad como firewall de última generación, antivirus y correlacionador de eventos.
- Sistema de copias de seguridad con respaldo a disco duro y cinta.

Esta infraestructura aloja el 100% de aplicativos misionales de la entidad y juega un papel determinante en las funciones de vigilancia y control que ella ejerce, razón por la cual, la estrategia de gestión de incidentes es una prioridad institucional.

Así mismo, la contraloría General dentro del programa de fortalecimiento institucional 2016-2019 (Contraloría General de la República, 2016), financiado por el Banco Interamericano de Desarrollo (BID) mediante el proyecto CO-L1154 (http://www.iadb.org/es/proyectos/project-information-page,1303.html?id=CO%2DL1154), con una inversión de treinta millones de dólares (US $30.000.000) y orientado a fortalecer la efectividad del ejercicio del control fiscal, ha contemplado dentro del componente de gestión de la información para el control fiscal un presupuesto de catorce punto siete millones de dólares (US$14.700.000), el cual se encuentra orientado no solo a la incorporación de tecnologías de la información y la comunicación (TIC), sino también a la optimización de la gestión de la información y al mejoramiento de la eficiencia de la misma como se muestra en la Figura 7.

Figura 7. Componentes proyecto BID. Recuperado de Programa de Fortalecimiento Institucional CGR. (Contraloría General de la República, 2016).

De acorde con este plan, la contraloría general a través de su oficina de sistemas e informática OSEI, ha contemplado además del mejoramiento de la infraestructura tecnológica,

la implementación de un DRP (Disaster Recovery Plan) tendiente a brindar la entidad contra futuros desastres que puedan ocurrir a nivel de su infraestructura (Figura 8).

Figura 8. Componentes proyecto BID. Recuperado de presentación programa de fortalecimiento institucional CGR. (Contraloría General de la República, 2016).

Como parte del programa de fortalecimiento, en la actualidad la contraloría general en el desarrollo de su ejecución ha realizado implementación del sistema de mesa de ayuda y gobierno de TICS, incluyendo la adquisición de una herramienta para la gestión de incidentes al igual que el respectivo manual de procedimientos con base en normas ITIL v3, el cual aún está siendo optimizado. (Contraloría General de la República, 2016).

Como contraprestación, vale la pena mencionar que ITIL tiene el inconveniente de contemplar una gran serie de eventos detonadores con lo que pueden existir brechas en las medidas implementadas, sobre todo hacia la parte de la seguridad; así bien, el desarrollo del modelo a proponer en este proyecto va dirigido a servir como fuente de insumo, no solo al proyecto actual en el cual se encuentra inmersa la contraloría general, sino también para futuros proyectos, dado que el mismo es un puente al campo de la seguridad informática que le permitirá contar con un modelo de gestión de incidentes de seguridad de la información ajustado a sus necesidades.

La Figura 9 muestra el procedimiento de gestión de incidentes implementado en la entidad:

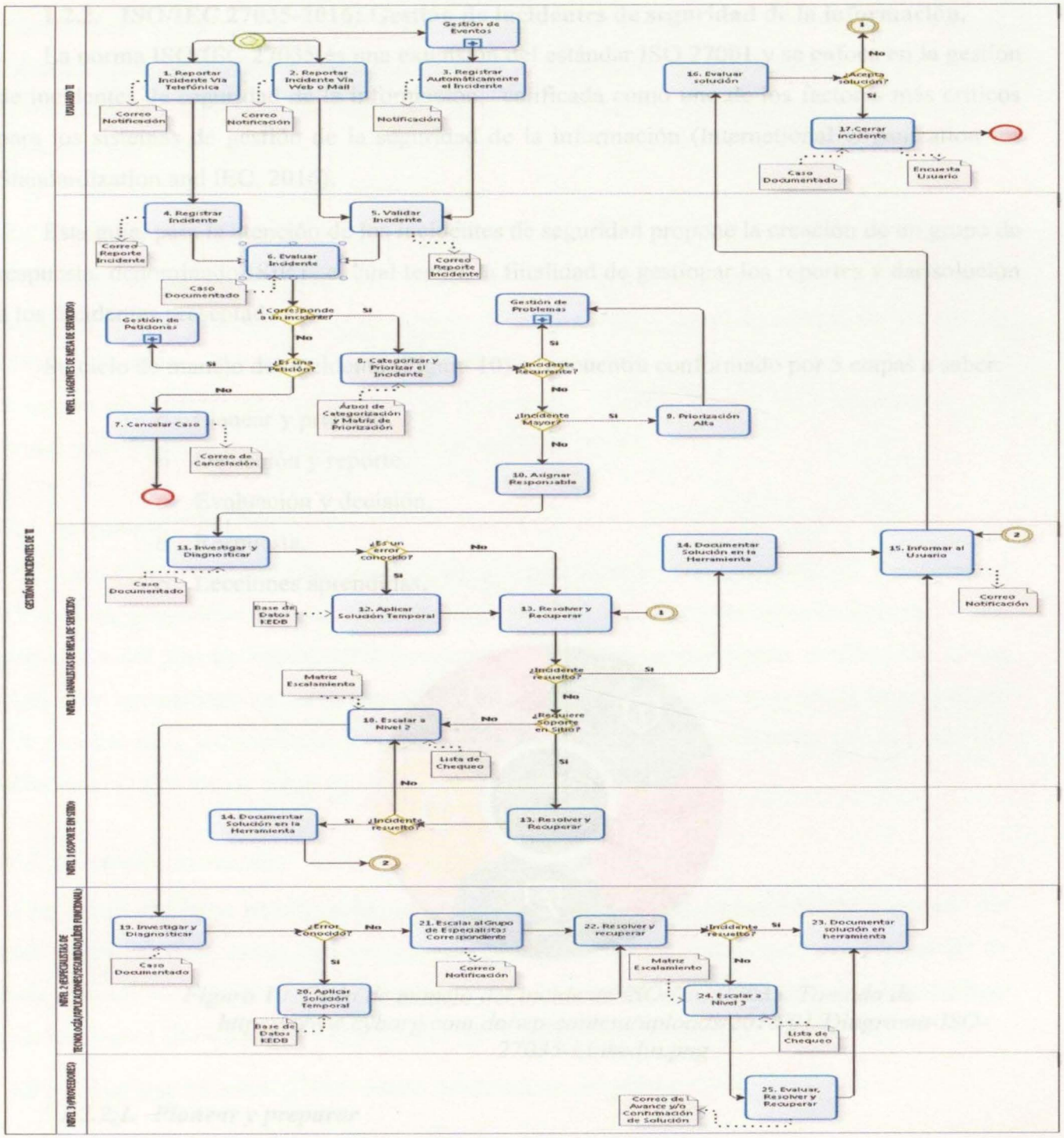

Figura 9. Diagrama del procedimiento para la gestión de incidentes CGR. Recuperado de manual procedimiento gestión de incidentes oficina de sistemas CGR. (Contraloría General de la República, 2016).

Modelo de Gestión de incidentes de seguridad CGR.

1.2.2. ISO/IEC 27035-2016: Gestión de incidentes de seguridad de la información.

La norma ISO/IEC 27035 es una extensión del estándar ISO 27001 y se enfoca en la gestión de incidentes de seguridad de la información, calificada como uno de los factores más críticos para los sistemas de gestión de la seguridad de la información (International Organization for Standardization and IEC, 2016).

Esta guía, para la atención de los incidentes de seguridad propone la creación de un grupo de respuesta denominado ISIRT, el cual tendrá la finalidad de gestionar los reportes y dar solución a los incidentes presentados.

Su ciclo de manejo del incidente (Figura 10) se encuentra conformado por 5 etapas a saber:

- Planear y preparar.
- Detección y reporte.
- Evaluación y decisión.
- Respuesta.
- Lecciones aprendidas.

Figura 10. Ciclo de manejo del incidente ISO/IEC 27035. Tomado de https://www.cyborg.com.do/wp-content/uploads/2018/01/Diagrama-ISO-27035-Linkedin.png

1.2.2.1. Planear y preparar

La etapa de planear y preparar incluye todas aquellas actividades necesarias para tener una respuesta efectiva al incidente, incluyendo la adquisición de las herramientas necesarias para llevar a cabo la tarea de una forma eficiente y la conformación del respectivo equipo de respuesta (International Organization for Standardization and IEC, 2016).

Modelo de Gestión de incidentes de seguridad CGR.

1.2.2.2. Detección y reporte

Se realizan todas las actividades encaminadas a la detección y reporte de anomalías relacionadas con el incidente. Se debe realizar la recepción de los reportes, el análisis y categorización del incidente, estimación del daño, el plan de respuesta, etc. (International Organization for Standardization and IEC, 2016).

1.2.2.3. Evaluación y decisión

Mediante el gestor del reporte el Equipo de Respuesta a Incidentes de Seguridad de la Información ISIRT debe validar si el reporte dado si clasifica como incidente, de seguridad, definiendo el alcance del mismo para proceder a categorizarlo de acuerdo a una prioridad determinada en su relación con el impacto al negocio, tamaño, tiempo de recuperación, etc. (International Organization for Standardization and IEC, 2016).

1.2.2.4. Respuesta

De acuerdo a la información obtenida de la etapa anterior y la categoría del incidente, el ISIRT debe de programar y tomar las medidas necesarias para controlar el incidente, tales como identificación del tipo de respuesta, documentación de las respuestas dadas, notificación de los resultados de las medidas tomadas, etc. con el fin de que al final todas estas medidas concluyan con la erradicación, recuperación y normalización de los servicios afectados por el incidente (International Organization for Standardization and IEC, 2016).

1.2.2.5. Lecciones aprendidas

Una vez el incidente ha sido solucionado, se debe realizar una documentación completa del incidente, identificando causa, tipo de incidente, medidas tomadas para contenerlo, resultado de análisis forense, etc. con el fin de generar una base de conocimiento orientada al tratamiento de futuros incidentes (International Organization for Standardization and IEC, 2016).

Es de notar que ISO/IEC 27035 está conformado por 2 partes:

- Parte 1: Principios para la administración de incidentes.
- Parte 2: directrices para planear y preparar una respuesta a incidentes.

Modelo de Gestión de incidentes de seguridad CGR.

1.2.2.6.ISO/IEC 27035-2: Directrices para planear y preparar la respuesta a incidentes

La guía ISO/IEC 27035, como tal, se posiciona como una ayuda al momento de planear la respuesta a incidentes; basándose esta, en dos fases de la gestión de incidentes de seguridad de la información: las fases de "planear y preparar" y "lecciones aprendidas". (International Organization for Standardization and IEC, 2016). El ISO/IEC 27035 plantea principios genéricos, por lo que los mismos aplican para todo tipo de organizaciones sean pequeñas o grandes, privadas o públicas, así como a organizaciones que se dediquen a prestar sus servicios en la gestión de incidentes de seguridad de la información.

La fase de "planear y preparar" involucra directrices tales como:

- Elaboración de la política de gestión de los incidentes.
- Actualización de la información de las políticas de seguridad.
- La creación de un plan de gestión de los incidentes.
- Establecer un equipo de respuestas a incidentes (IRT).
- Relaciones de mutua cooperación con otras entidades.
- Concientización y entrenamiento del personal.
- Pruebas al plan de gestión.

La fase de "lecciones aprendidas" contiene directrices más puntuales orientadas a la creación de una base de conocimientos que en determinados casos pueda servir para solucionar problemas con un 'modus operandi' ya identificado o registrado, facilitando la resolución del incidente. (International Organization for Standardization and IEC, 2016)

1.2.3. NIST 800-61: Computer security incident handling guide.

Nace con el fin de asistir a las entidades estatales de los Estados Unidos de América en el desarrollo de mecanismos para mitigar el riesgo proveniente de incidentes de seguridad informáticos, mediante la implementación de una respuesta a incidentes eficiente y efectiva. Esta guía constituye una serie de orientaciones para la elaboración de un programa de respuesta a incidentes efectivo, enfocándose en la detección, el análisis, la priorización y el manejo de estos; permitiéndole constituirse como una guía fundamental para cualquier entidad, sea gubernamental o no, que desee implementar un plan de gestión de incidentes efectivo. (National Institute of Standards and Technology, 2012).

Modelo de Gestión de incidentes de seguridad CGR.

La guía determina una serie de características que las distintas empresas y/o entidades deben poseer para contar con verdaderas capacidades de respuesta a incidentes:

- Creación de un plan y una política de respuesta a incidentes.
- Definir procedimientos para desempeñar manejo y reporte de incidentes.
- Establecer directrices para la comunicación con otras partes relacionadas con los incidentes.
- Selección de la estructura de un equipo de trabajo y el perfil de sus integrantes.
- Establecer las relaciones, el canal y el protocolo de comunicación entre el equipo encargado de atender los incidentes y otros grupos tanto internos, como externos a la entidad o empresa.
- Establecer los servicios a proveer por el equipo de respuesta.
- Preparación y entrenamiento del equipo de respuesta.

Por lo que el desarrollo de la guía contempla los siguientes temas entre otros:

- La importancia y necesidad de la respuesta a incidentes, la necesidad de tener equipos de respuesta bien estructurados y su interacción con otros grupos.
- Consejos y pasos para proporcionar una respuesta a incidentes más efectiva
- La necesidad de compartir la información y coordinar operaciones con otros equipos de respuesta a incidentes.
- La identificación de recursos útiles para la planificación y la respuesta a incidentes.
- El ¿qué se debe hacer? ante un evento de seguridad informática.

(National Institute of Standards and Technology, 2012).

1.2.3.1. Organizando las capacidades de respuesta a incidentes informáticos.

La organización de una capacidad realmente efectiva de respuesta a incidentes de seguridad informática, requiere de varias acciones, incluyendo una clara definición de lo que el término "incidente" puede significar, al igual que la implementación de las políticas y el plan de respuesta a incidentes. Se deben identificar los servicios a ser prestados por el equipo de respuesta, al igual, que la estructura y el modelo del equipo a implementar; con base en ello

decidir si implementar uno o varios equipos de respuesta. Las políticas, los planes y los procedimientos deben reflejar la interacción entre los distintos equipos y organizaciones de respuesta a incidentes. (National Institute of Standards and Technology, 2012)

Estos son los elementos que una política de respuesta a incidentes debe llevar:

- Declaración de compromiso de la dirección.
- Propósito y objetivo de la política.
- Alcance.
- Definición de términos relacionados.
- Definición de roles y estructura organizacional.
- Clasificación de los incidentes de acuerdo a la gravedad y su prioridad.
- Medidas del desempeño.
- Formularios de informes y contactos.

Estos son los elementos que un plan de respuesta a incidentes debe llevar:

- Misión.
- Estrategias y metas.
- Aprobación de la alta dirección
- Enfoque organizativo
- Como debe comunicarse el equipo de respuesta a incidentes con el resto de la organización y con otras organizaciones.
- Métrica para las capacidades de respuesta y su efectividad.
- Hoja de ruta con el objetivo de fortalecer las capacidades de respuesta a incidentes.
- Como el programa encaja en la organización general.

Para el caso de los procedimientos, los elementos de los procedimientos de operación estándar están delimitados por procesos técnicos específicos, técnicas, listas de chequeo y formularios utilizados por el equipo de respuesta a incidentes. (National Institute of Standards and Technology, 2012).

Modelo de Gestión de incidentes de seguridad CGR.

1.2.3.2.Atendiendo un incidente:

El proceso de respuesta a incidentes tiene cuatro fases o etapas como se puede observar en la Figura 11.

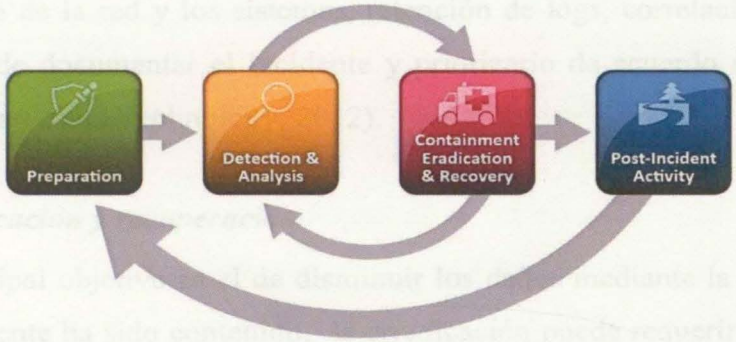

Figura 11. Ciclo de manejo del incidente NIST SP 800-61. Recuperado de Computer Security Incident Handling Guide (National Institute of Standards and Technology, 2012).

1.2.3.3. Preparación.

La fase inicial requiere de establecer y capacitar el equipo de respuesta a incidentes, además de la adquisición de herramienta y recursos necesarios. Durante esta etapa se deben hacer esfuerzos por limitar el número de incidentes que puedan ocurrir, implementando para ello medidas con base en los resultados de un estudio de los riesgos. En la preparación se implementan las pautas no solo para el manejo, sino también para la prevención de incidentes. (National Institute of Standards and Technology, 2012).

1.2.3.4.Detección y análisis.

En esta fase se detectan y analizan las brechas de seguridad con el fin de alertar a la organización cuando hay ocurrencia de incidentes. Se identifican vectores de ataque tales como:

- Medios externos
- Web
- Correo electrónico
- Suplantación de identidad
- Uso inapropiado
- Pérdida o robo de equipos.

Modelo de Gestión de incidentes de seguridad CGR.

En esta fase se deben encontrar las huellas del incidente, como ocurrió, porqué, cuando, dado que esto resulta de vital importancia al momento de realizar actividades de prevención.

El análisis del incidente será más fácil a medida que más información se tenga, por lo que el equipo de respuesta debe realizar las actividades necesarias con el fin de garantizar esta información (Conocimiento de la red y los sistemas, retención de logs, correlación de eventos, etc.). Igualmente, se sebe de documentar el incidente y priorizarlo de acuerdo a su severidad. (National Institute of Standards and Technology, 2012).

1.2.3.5.Contención, erradicación y recuperación.

En esta etapa el principal objetivo es el de disminuir los daños mediante la contención del incidente. Una vez el incidente ha sido contenido, la erradicación puede requerir la eliminación de componentes del incidente como la eliminación de malwares o cuentas de usuarios comprometidos; esto con el objetivo de identificar y mitigar todas las vulnerabilidades que hayan sido explotadas. La recuperación implica regresar el sistema a su operación normal. (National Institute of Standards and Technology, 2012).

1.2.3.6.Actividad post-incidente.

Una de las partes más importantes de la respuesta a incidentes, es aprender de los mismos, motivo por el cual se debe de crear una base de conocimiento, con el fin de mitigar futuras incidencias que puedan presentar similitud con la incidencia ya atendida.

1.2.3.7.Pasos a seguir ante un evento de seguridad informática.

Los pasos a seguir ante un evento de seguridad informática son los siguientes:

1. Documentar todo.
2. Encontrar un compañero de trabajo que pueda proporcionar ayuda.
3. Analizar la evidencia con el fin de confirmar el incidente.
4. Notificar a las personas apropiadas dentro de la organización.
5. Notificar a las entidades competentes.
6. Frenar el incidente si este aún está en proceso.
7. Preservar la evidencia del incidente.
8. Limpiar los efectos del incidente.

Modelo de Gestión de incidentes de seguridad CGR.

9. Identificar y mitigar todas las vulnerabilidades que fueron explotadas.
10. Confirmar la restauración normal de la operación.
11. Crear un reporte final.

(National Institute of Standards and Technology, 2012)

1.2.4. MINTIC: Guía para la gestión y clasificación de incidentes de seguridad de la información.

Guía elaborada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) con base en las mejores prácticas recomendadas y publicadas por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) mediante su documento 800-61: "Computer Segurity Incident Handling Guide", e igualmente con base en los lineamientos contemplados en la norma ISO IEC 27001. (MINTIC, 2016). La guía fue elaborada con el objetivo de que la misma sea adoptada por las entidades públicas de orden nacional, las entidades públicas del orden territorial, el proveedores de servicios de gobierno en línea y cualquier tercero que desee adoptar el modelo de seguridad TI en el marco de la estrategia de gobierno en línea, la cual es liderada por el MINTIC.

Esta guía entrega lineamientos básicos para poner en marcha un sistema de gestión de incidentes de seguridad de la información, pudiendo integrar los incidentes de seguridad sobre los activos de la información de manera independiente al medio donde esta se encuentre.

Para la implementación del sistema de gestión de incidentes de seguridad de la información, la guía se basa en la implementación de los procesos según se observa en la Figura 12.

Figura 12. Procesos del modelo de gestión de incidentes. Recuperado de Guía para la gestión y clasificación de incidentes de seguridad de la información MINTIC (MINTIC, 2016).

Para la atención de los incidentes que puedan generarse, la guía recomienda la creación de un equipo de atención a incidentes de seguridad CSIRT (Computer Security Incident Response Team), el cual tendrá las tareas de: definir los distintos procedimientos, atender el incidente,

Modelo de Gestión de incidentes de seguridad CGR.

manejar las relaciones con otros entes, clasificar los incidentes, emitir anuncios de seguridad, certificar productos nuevos de acuerdo a las políticas de seguridad, administración de los dispositivos de seguridad, etc. En resumen, atender cualquier incidente relacionado con la seguridad de la información. (MINTIC, 2016).

A los procesos ilustrados en la figura 10, le fueron adicionados componentes definidos por el NIST, alineados con la normatividad ISO IEC 27035. De forma tal que el proceso del modelo de gestión de incidentes, contempla las siguientes actividades: (MINTIC, 2016)

1.2.4.1.Etapa de preparación.

Esta etapa debe de ser apoyada por la dirección de la oficina de tecnologías de la información, en esta se disponen los recursos necesarios para cumplir con todos los procesos que supone el proceso de gestión de incidentes e igualmente se desarrollan actividades de mejores prácticas que busquen prevenir la ocurrencia de incidentes de seguridad (MINTIC, 2016). La etapa de preparación puede incluir las siguientes actividades:

- Gestión de parches de seguridad
- Aseguramiento de la plataforma
- Seguridad en redes
- Prevención de código malicioso
- Actividades de sensibilización y entrenamiento de usuarios.
- Políticas de comunicación.

1.2.4.2. Etapa de detección, evaluación y análisis.

Comprende las siguientes actividades:

- Detección mediante el establecimiento de indicadores tales como: alertas de sistemas de seguridad, caída de servidores, reportes de usuario, informes del software antivirus, log de eventos, etc.
- Para el caso del procedimiento de análisis, es necesario tener conocimiento de la plataforma, tener conocimiento del comportamiento de la misma, tener información detallada, tener una base de conocimientos, y cualquier otra herramienta que pueda facilitar el desarrollo de las actividades contempladas.

Modelo de Gestión de incidentes de seguridad CGR.

- Para el proceso de evaluación se debe tener en cuenta la severidad del incidente de acuerdo al nivel de impacto del mismo.
- Clasificación del incidente de acuerdo a las normas de la entidad.
- Priorización del incidente con el fin de permitir una atención adecuada.
- Establecimiento de los tiempos de respuesta de acuerdo a la clasificación del incidente.
- Declarar y notificar el incidente de forma que se pueda responder al mismo de forma sistemática y rápida.

1.2.4.3.Etapa de contención, erradicación y recuperación.

Contempla la elaboración de una estrategia que permita tomar decisiones oportunamente orientadas a disminuir los daños, evitando la propagación del incidente, así como, la afectación en la confidencialidad, integridad y disponibilidad de la información. (MINTIC, 2016).

1.2.4.4.Actividades post-incidente.

Se deben realizar los reportes adecuados y tener una ficha de conocimientos con las lecciones aprendidas, de forma tal, que sirvan de insumo para el próximo incidente. (MINTIC, 2016).

1.2.5. AGESIC: Guía de procesos en gestión de incidentes.

Documento elaborado por la Agencia de Gobierno Electrónico y Sociedad de la Información de Chile con el objeto de dar los lineamientos básicos para la elaboración de manuales de gestión de incidentes en acuerdo con las mejores prácticas, para lo que se basa en la normativa ISO/IEC18044, NIST 800-61 y el handbook publicado por CERT/CC. (Agencia de Gobierno Electrónico y Sociedad de la Información, 2010).

Esta guía define la el concepto de gestión de incidentes como:

> El conjunto de acciones y procesos tendientes a brindar a las organizaciones de la comunidad objetivo de fortalezas y capacidades para responder en forma adecuada a la ocurrencia de incidentes de seguridad informática que afecten real o potencialmente sus servicios. (Agencia de Gobierno Electrónico y Sociedad de la Información, 2010, pág. 6).

Modelo de Gestión de incidentes de seguridad CGR.

Igualmente, la guía determina los principales aspectos para la política de gestión de incidente:

- Comunidad objetivo.
- Clasificación del incidente (tipo, severidad).
- Proceso de gestión de incidentes.

El proceso de gestión de incidentes estará conformado a su vez por 3 procesos a saber (Figura 13):

- Proceso de preparación y planificación para enfrentar incidentes de seguridad.
- Proceso de atención a incidentes.
- Proceso de mejora continua.

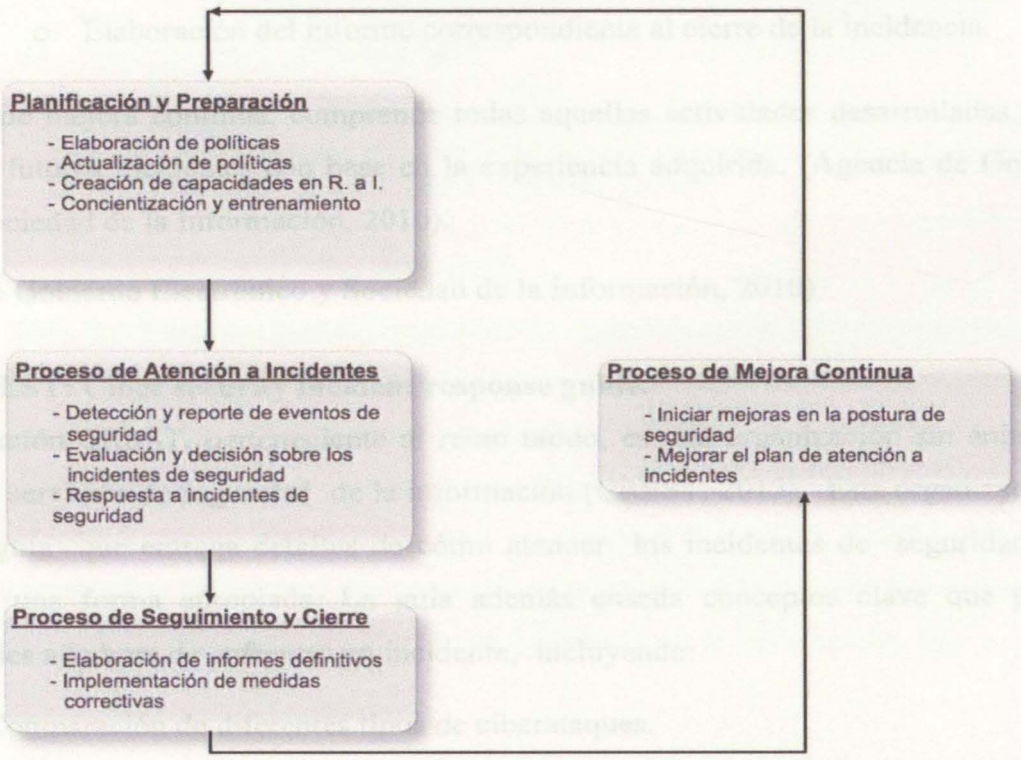

Figura 13. Diagrama de procesos. Recuperado de Guía de procesos en gestión de incidentes Agesic (Agencia de Gobierno Electrónico y Sociedad de la Información, 2010).

El proceso de preparación y planificación para enfrentar incidentes de seguridad incluye:

Modelo de Gestión de incidentes de seguridad CGR.

- Análisis de alertas y amenazas.
- Actividades de sensibilización.
- Evaluaciones de seguridad.
- Definición de procedimientos.
- Etc.

El Proceso de atención a incidentes incluyendo actividades como:

- Recepción y reporte de los incidentes.
- Clasificación y valoración del impacto.
- Elaboración de un plan de respuesta al incidente con sus respectivas recomendaciones.
- Gestión de los permisos necesarios para la aplicación del plan de respuesta.
- Aplicación de las medidas de contención y mitigación.
- Elaboración del informe correspondiente al cierre de la incidencia.

El proceso de mejora continua, comprende todas aquellas actividades desarrolladas con el fin de enfrentar futuros incidentes con base en la experiencia adquirida. (Agencia de Gobierno Electrónico y Sociedad de la Información, 2010).

(Agencia de Gobierno Electrónico y Sociedad de la Información, 2010)

1.2.6. CREST: Ciber security incident response guide.

La organización CREST, perteneciente al reino unido, es una organización sin ánimos de lucro que presta servicios de seguridad de la información (CREST, 2013). Esta organización ha publicado esta guía que entrega detalles de cómo atender los incidentes de seguridad de la información de una forma apropiada. La guía además enseña conceptos clave que pueden resultar muy útiles a la hora de enfrentar un incidente, incluyendo:

- Comparación de diferentes tipos de ciberataques.
- La anatomía de un ciberataque.
- Los principales retos al responder a un incidente de ciberseguridad y cómo hacerlo.
- Como ayudar ante un incidente de ciberseguridad

Modelo de Gestión de incidentes de seguridad CGR.

CREST, como se observa en la Figura 14 considera 3 fases claves para enfrentar adecuadamente los incidentes cibernéticos. Estas son:

- Preparación para el incidente.
- Respuesta al incidente.
- Seguimiento del incidente.

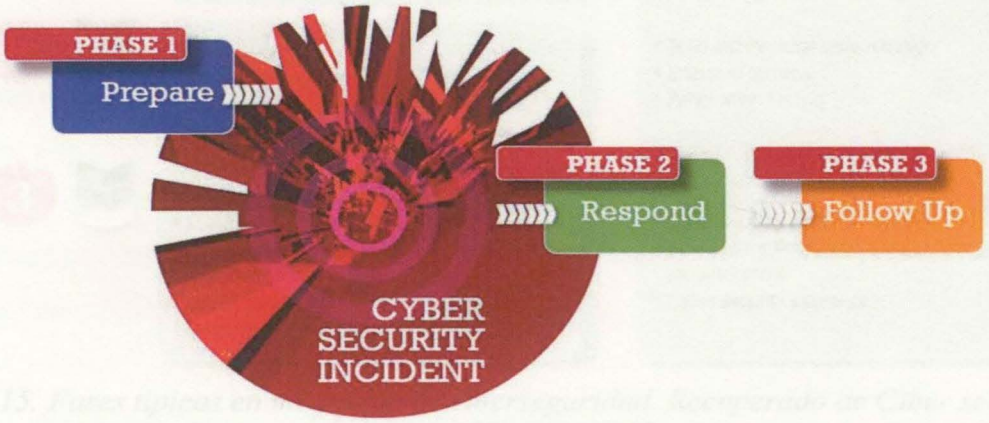

Figura 14. Ciclo de manejo del incidente CREST. Elementos clave en la capacidad de atención de incidentes de ciberseguridad. Recuperado de Ciber security incident response guide CREST (CREST, 2013).

1.2.6.1.Definiendo un incidente de ciberseguridad.

Según la guía, hay muchos tipos de incidentes de seguridad de la información que podrían ser catalogados como incidentes de ciberseguridad, ya sea un ataque serio a la infraestructura nacional, un simple mal uso de los sistemas, o un mal funcionamiento del software (CREST, 2013). Y aunque no hay una definición común para los incidentes de ciberseguridad, el término parece estar asociado a ataques maliciosos o APT's (Avanced Persistend Threats), cosa que no es de común acuerdo hoy. Como sea, los términos en relación con incidentes de ciberseguridad son catalogados como tradicionales incidentes de seguridad de la información, por lo que son manejados como tal. (CREST, 2013).

1.2.6.2.Fases típicas en un ataque de ciberseguridad.

Como se ilustra en la Figura 15, la guía CREST contempla las siguientes fases:

1. Realizar el reconocimiento.

2. Atacar el objetivo.
3. Alcanzar el objetivo
4. Contramedidas.

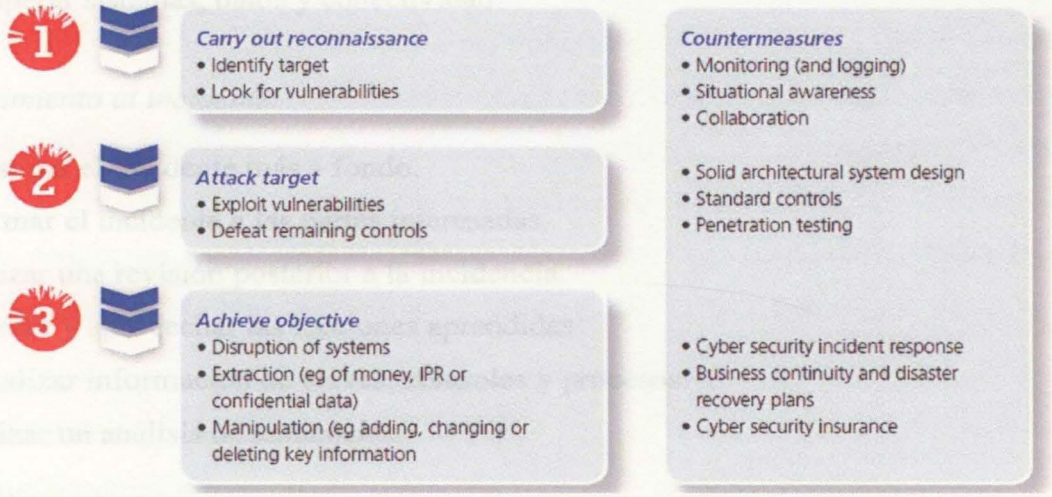

Figura 15. Fases típicas en un ataque de ciberseguridad. Recuperado de Ciber security incident response guide CREST (CREST, 2013)

1.2.6.3.Implementando capacidades de respuesta a incidentes de seguridad informática.

La implementación de la capacidad de respuesta a incidentes de seguridad informática conlleva las siguientes actividades:

A. Preparación para el incidente.

Contiene las siguientes tareas:

1. Realizar una evaluación crítica de la organización.
2. Realizar un análisis de amenazas a nivel de ciberseguridad.
3. Considerar las implicaciones de las personas, los procesos, la tecnología y la información.
4. Crear un apropiado marco de control.
5. Revisar el estado de preparación en torno a las respuestas a incidentes de la información.

Modelo de Gestión de incidentes de seguridad CGR.

B. Respuesta al incidente.

1. Identificar el incidente de ciberseguridad.
2. Definir los objetivos e investigar la situación.
3. Tomar las acciones apropiadas
4. Recuperar sistemas, datos y conectividad.

C. Seguimiento al incidente.

1. Investigar el incidente más a fondo.
2. Informar el incidente a las partes interesadas.
3. Realizar una revisión posterior a la incidencia.
4. Difundir y aprovechar las lecciones aprendidas.
5. Actualizar información de claves, controles y procesos.
6. Realizar un análisis de tendencias.

(CREST, 2013)

1.2.7. Goverment of Canada: Ciber incident management framework for Canada.

La gestión de incidentes en Canadá utiliza un enfoque con un punto de vista que contempla todos los riesgos o peligros. Diseñado de tal forma que pueda abarcar todos los incidentes independientemente de su subyacente causa. Enfoque que podría ser aplicado cuando un incidente causa consecuencias en el dominio físico, causando que dichas consecuencias fueran efectivamente gestionadas (Goverment of Canada, 2013). Con el ciberespacio ocurre un caso especial, pues este es controlado por empresas públicas y privadas que evitan la aplicación de este enfoque y por lo que un marco explícitamente en incidentes cibernéticos es necesario para complementar las políticas en gestión de incidentes existentes en dicho país. (Goverment of Canada, 2013).

De esta forma, el marco (framework) es una guía aplicable tanto a empresas gubernamentales, infraestructura crítica y empresas privadas que deseen adoptarlo con el fin de contar con capacidades de ciberdefensa.

El marco define roles y responsabilidades de las partes interesadas tales como:

- El gobierno federal.

Modelo de Gestión de incidentes de seguridad CGR.

- Otros niveles del gobierno.
- Infraestructuras críticas y operadas por tercero, al igual que otras organizaciones del sector público y privado.

1.2.7.1.Concepto operacional.

Cada organización es responsable por su propia defensa, por lo que con el fin de contar con verdaderas capacidades de ciberdefensa esta debe trabajar colaborativamente con socios externos expertos en seguridad cibernética como el CCIRC (Centro de Respuesta para Incidentes Cibernéticos de Canadá). El CCIRC categoriza la severidad de los incidentes de ciberseguridad de forma tal que provee las bases para el concepto operacional del framework. Estos son los cinco niveles de severidad definidos (Goverment of Canada, 2013).

- Operaciones de ciberseguridad normal.
- Incidentes de muy bajo impacto.
- Incidentes de bajo impacto.
- Incidentes de impacto medio.
- Incidentes de Alto impacto/ muy alto impacto.

Para lo que se definen acciones como:

- Una investigación de seguridad nacional.
- Una investigación de acuerdo con la ley.
- Compartir la información del incidente con otras partes, de acuerdo a los términos de uso dictados por la ley.

(Goverment of Canada, 2013)

1.3. Marco Comparativo

No es necesario profundizar mucho en el tema respecto a las guías MINTIC, AGESIC, o cualquier otra, dado que en su gran mayoría dichas guías se encuentran basadas en el modelo NIST, e igualmente, el modelo a desarrollar debe estar en concordancia con las recomendaciones del MINTIC, por lo que este marco comparativo se centrará en analizar modelos como NIST, ISO e ITIL.

Modelo de Gestión de incidentes de seguridad CGR.

Disponer de un marco comparativo entre los modelos o guías analizados resulta bastante concluyente desde el punto de vista de la ciberseguridad, en el cual que modelos como ITIL contemplan un contenido macro o globalizado de la gestión de incidentes, mientras que la familia de estándares ISO 27000 y NIST lo hacen de una forma orientada hacia la seguridad de la información, permitiendo que tanto ISO, como la normativa NIST, aunque cuentan con una perspectiva más ajustada a los riesgos presentes actualmente en el ciberespacio, tengan diferencias, siendo la norma NIST un poco más amplia y precisa en su alcance respecto a la ciberseguridad, mientras la norma ISO en cabeza del estándar ISO 27001 se orienta de manera fuerte hacia la gestión del riesgo. El I

De la misma forma, desde el punto de vista procedimental, existe una marcada diferencia entre las normas ISO 27001 y NIST SP800, pues la familia de estándares ISO 27000 pasa a ser un conjunto de reglas de cumplimiento, mientras la NIST va más allá de políticas y procedimientos, esta equivale a una guía, que contiene procedimientos operativos, sensibilización, una serie de pasos más descriptivos de lo que se debe o no hacer.

De otro lado, es claro es que NIST SP800 se corresponde a un marco especializado y orientado hacia la ciberseguridad que nace con el fin de implementar estrategias de ciberseguridad a nivel de infraestructuras críticas, por lo que ISO 27001 como norma contiene un amplio espectro de acción que sobrepasa estos límites, haciéndola menos técnica, pero a su vez mas aplicable que NIST SP800.

Por lo que tenemos que tanto ITIL, como ISO y NIST forman entre sí un conjunto de normas complementarias, comenzando desde la aplicación de las recomendaciones del NIST a un nivel más interno para luego enmarcarse dentro de la norma ISO 27001 y finalmente bajo la serie de buenas prácticas ITIL de manera más global; permitiéndole a una entidad que realiza la gestión de sus recursos informáticos bajo ITIL contar con la implementación de sus procesos de gestión de incidentes de seguridad de acuerdos a la guías proporcionadas por el NIST y a su vez ser cumplir con la certificación ISO 27001 sin ningún problema.

Con respecto a la norma ISO vs la norma NIST, es de notar que tanto la familia ISO 27000 como la norma NIST SP 800 forman un amplio compendio de documentos y publicaciones, donde los documentos NIST 800-61 e ISO/IEC 27035 (que complementa la norma ISO 27001) se encuentran centrados en la gestión de incidentes, por lo que contienen las acciones necesarias

para el establecimiento de la capacidad de respuesta a estos, y motivos por el cual significan un buen punto de partida para la elaboración de un modelo nuevo a partir de los mismos.

Estos documentos contemplan como mínimo las siguientes actividades:

- Creación de un plan y política de respuesta a incidentes.
- Establecimiento de procedimientos para el manejo y el reporte de incidentes.
- Establecimiento de canales de comunicación con terceras partes.
- Establecimiento de un equipo encargado de gestionar y contrarrestar los incidentes.
- Establecimiento de los servicios a prestar por este equipo.
- Entrenamiento del equipo de respuesta.

Pero si bien, es claro que estos documentos pertenecen a guías que proceden de empresas distintas, las mismas poseen en muchas ocasiones algunas similitudes al igual que diferencias en sus formas de abordar la gestión de incidentes.

Adicionalmente debe tenerse en cuenta que ISO/IEC 27035 se encuentra conformado por dos partes, ISO/IEC 27035-1 "Principios de la gestión de incidentes" e ISO/IEC37035-2 "Guía para planear y preparar la respuesta a incidentes", ambas partes se complementan entre sí, siendo la parte 2 la más aplicable al momento del desarrollo del plan de gestión de incidentes, al establecerse como una guía de fácil utilización para los distintos actores en el proceso (International Organization for Standardization, 2016).

1.3.1. Enfoque y propósito de la guía.

- NIST 800-61: Para el caso de la guía NIST 800-61, esta se encuentra enfocada hacia la mitigación del riesgo de incidentes de seguridad en computadores mediante una respuesta a incidentes efectiva y eficiente, permitiendo establecer un programa de respuesta a incidentes óptimo, con alto nivel de priorización y el adecuado manejo del incidente.
- ISO/IEC 27035-2: Esta guía pertenece a una extensión de la serie de estándares ISO/IEC 27000, se encuentra enfocada hacia la gestión de incidentes de seguridad de la información, constituyéndose en un factor crítico para los sistemas de gestión de seguridad de la información plasmados a nivel del estándar. Esta

guía se encuentra orientada hacia el incremento de la confidencialidad de la información en las organizaciones con el fin de responder a los incidentes de seguridad de manera ágil mediante políticas y planes asociados a la gestión del incidente; al igual, que con el establecimiento de equipos de respuesta a incidentes que puedan mejorar su desempeño mediante la adopción de lecciones aprendidas y evaluaciones. La guía se encuentra sustentada en 2 fases: "Planear y preparar" y "Lesiones aprendidas", aunque el modelo en sí contempla un rango más amplio en cada una de sus fases.

1.3.2. Mercado objetivo.

- NIST 800-61: El enfoque de la guía NIST 800-61 se encuentra orientado hacia equipos de gestión de seguridad de incidentes de computador (CSIRT), administradores de redes y sistemas, personal de seguridad, personal de soporte técnico, oficiales de seguridad y cualquier otra persona o equipo responsable de preparar o responder a incidentes de seguridad. NIST recomienda la aplicación de la guía NIST 800-61 de acuerdo con la misión y las necesidades de seguridad específicas de las empresas o del personal encargado de ejecutar la respuesta a incidentes.
- ISO/IEC 27035-2: Contiene principios genéricos con la intensión de que los mismos puedan ser aplicados a todo tipo de organizaciones independientemente de su naturaleza, tipo o tamaño; permitiendo a las mismas ajustar la aplicación de la guía en relación a la situación o riesgo que estas posean. La guía también se encuentra diseñada igualmente para empresas que presten servicios de gestión de incidentes de seguridad de la información a terceros.

1.3.3. Ciclo de manejo de incidentes.

El autor Grzegorz Pohorecki mediante el sitio web https//komunity.komand.com (Pohorecki, 2017) publica resultados de la comparación entre las guías NIST 800-61 e ISO/IEC 27035 que como sabemos son muy similares, obteniéndose los siguientes datos relevantes:

- Ciclo en el manejo de incidentes según la norma NIST 800-61 (National Institute of Standards and Technology, 2012):
  - Preparación.

Modelo de Gestión de incidentes de seguridad CGR.

- Detección y análisis.
- Contención, erradicación y recuperación.
- Actividad post-incidente.

(Ver Figura 11).

- Ciclo en el manejo de incidentes según la norma ISO/IEC 27035 (International Organization for Standardization, 2016):
  - Planear y preparar.
  - Detección y reporte.
  - Evaluación y decisión.
  - Respuesta.
  - Lecciones aprendidas.

(Ver Figura 10

Ambas son basadas en el ciclo Deming (Planear, Hacer, Revisar y Actuar), pero se observa que en el ciclo de detección la norma ISO se enfoca en el reporte, mientras la norma NIST lo hace en el análisis. Igualmente se observa que el ciclo NIST es más agresivo pues incluye una etapa de contención, erradicación y recuperación, algo que no se puede observar directamente sobre la norma ISO pues no se define muy claramente la consistencia de la fase de respuesta a simple vista. ISO incluye una etapa de lecciones aprendidas, cosa que se considera bastante acertada.

1.3.4. Atención del incidente.

Ambas normas plantean la atención del incidente mediante la creación de equipos de respuesta de acuerdo a la categorización del incidente. Para el caso del NIST 800-61 dicha atención se hace mediante sencillos pasos contenidos en una lista, que para el caso de ISO/IEC 27035 son procesos detallados sobre todo en la categorización de los incidentes, pues, esta es orientada a la obtención de datos estadísticos e históricos, al igual que en compartir la información sobre el ataque (Pohorecki, 2017).

1.3.5. Equipo de respuesta a incidentes.

El equipo de respuesta a incidentes (IRT por sus siglas en inglés) es un grupo de personas y recursos con las capacidades apropiadas para evaluar, responder y aprender de los incidentes; de

modo que puedan actuar de la forma más asertiva posible a fin de solventarlo, gestionarlo o contrarrestarlo con efectividad. Para ISO los IRTs pueden ser estructurados de acuerdo a las necesidades de la empresa, esto dependiendo de su tamaño, los miembros del equipo y el tipo de industria. ISO plantea tres estructuras básicas para el equipo de respuesta (International Organization for Standardization, 2016):

- Única: Un solo IRT para realizar las labores de monitoreo, respuesta y operación.
- Jerárquico: Uno o más IRT desarrollan las actividades relacionadas con el servicio.
- Remoto: Recolección de eventos de seguridad desde un sitio remoto por parte del IRT.

El equipo debe de estar conformado por personal interdisciplinario con capacidades no solo de tomar decisiones, sino también de actuar a nivel técnico según sea las necesidades.

Desde el punto de vista del NIST (National Institute of Standards and Technology, 2012), plantea seis modelos de equipos de respuesta a saber:

- Equipo de respuesta a incidentes central: Pertenece a un solo equipo de respuestas, normalmente recomendado para empresas pequeñas.
- Equipo de respuesta a incidentes distribuido: Obedece al hecho de contar con múltiples equipos de respuesta a incidentes respondiendo cada uno por un segmento particular de la organización.
- Equipo coordinado: Un equipo de respuesta a incidentes aconseja a otros sin tener autoridad sobre los mismos.
- Empleados: la organización desempeña todas las labores relacionadas con la gestión del incidente, contando con personal técnicos y de soporte aportados por un contratista.
- Outsourcing parcial: La organización contrata parte de las labores de gestión del incidente con terceros.
- Outsourcing completo: El total de las labores de gestión del incidente, son desarrolladas por un tercero o contratista.

Modelo de Gestión de incidentes de seguridad CGR.

NIST recomienda que para la elección del modelo del equipo de respuesta, la organización debe tener en cuenta detalles como: disponibilidad del equipo, el compromiso de los empleados, jornadas de trabajo, costo, número de sedes, Experticia del personal, oferta del mercado, confidencialidad, etc.

1.3.6. Colaboración con otras áreas y terceros.

La colaboración con terceros en ambas normas representa un punto importante, esto debido a que las mismas pueden representar en algún momento una fuente de información invaluable al momento de enfrentar un incidente. Compartir información con otros grupos de respuesta puede simplificar una amplia reducción en las tareas a realizar, dado que es muy posible que alguno de estos grupos ya hayan sufrido incidentes similares y tengan información clara de cómo enfrentarlo; y por lo general, muchos ataques son dirigidos a varias instituciones, personas o empresas a la vez. NIST recomienda mantener buenos canales de comunicación tanto con los proveedores de acceso a internet (ISP), como con los vendedores del software y otros equipos de respuesta a incidentes. Se debe participar en grupos de discusión, compartir con departamentos legales, organizaciones públicas, autoridades con conocimiento en la materia y cualquier otra parte que haya sido afectada por incidentes similares (National Institute of Standards and Technology, 2012). Por su parte ISO, igualmente hace énfasis en que otras partes de la organización no deben ser ajenas al incidente, por lo que se debe tener en cuenta contar con representantes de las oficinas talento humano, recursos físicos, comunicaciones, departamento legal, etc. (International Organization for Standardization, 2016).

2. Capítulo Dos – Planteamiento del Modelo: Análisis de Riesgos y Alineación con el Negocio

El modelo de gestión de incidentes corresponde a una guía de procesos que le permitirán a la entidad conocer el cómo actuar frente a la ocurrencia de un incidente de seguridad, de forma tal, que el negocio prestado a través de los servicios informáticos de la entidad se vea lo menos afectado posible.

Para ello es necesario tener una idea clara de los riesgos que en cualquier momento pueden terminar materializándose en incidentes, y que en alguna medida terminarán afectando la disponibilidad de los servicios prestados por la entidad.

2.1. Justificación

El presente documento se encuentra justificado, además de en las necesidades propias de seguridad de la contraloría general de la República, en los siguientes puntos a saber:

2.1.1. La política de seguridad digital CONPES 3854.

Mediante la cual se fijan y se establecen las políticas de seguridad orientadas a fortalecer las capacidades tanto de la infraestructura crítica como del sector público y privado con el fin de identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas del entorno digital. (Consejo Nacional de Política Económica y Social, 2016).

2.1.2. El Modelo Nacional de gestión del riesgo de seguridad digital MGRSD.

El MGRSD tiene el objetivo de "alcanzar beneficios sociales y económicos, proveer servicios esenciales, operar infraestructuras críticas, preservar los derechos humanos y los valores fundamentales y proteger a las personas frente a las amenazas de seguridad digital" (Ministerio de Tecnologías de la Información y las Comunicaciones, 2017, pág. 12), está diseñado para entidades pública, privadas y de fuerza pública habiéndose creado como una guía orientada al uso cotidiano en el entorno digital, basándose para ello en riesgos comunes del entorno y las herramientas para gestionarlo.

La Figura 16 corresponde al marco conceptual del modelo:

Modelo de Gestión de incidentes de seguridad CGR.

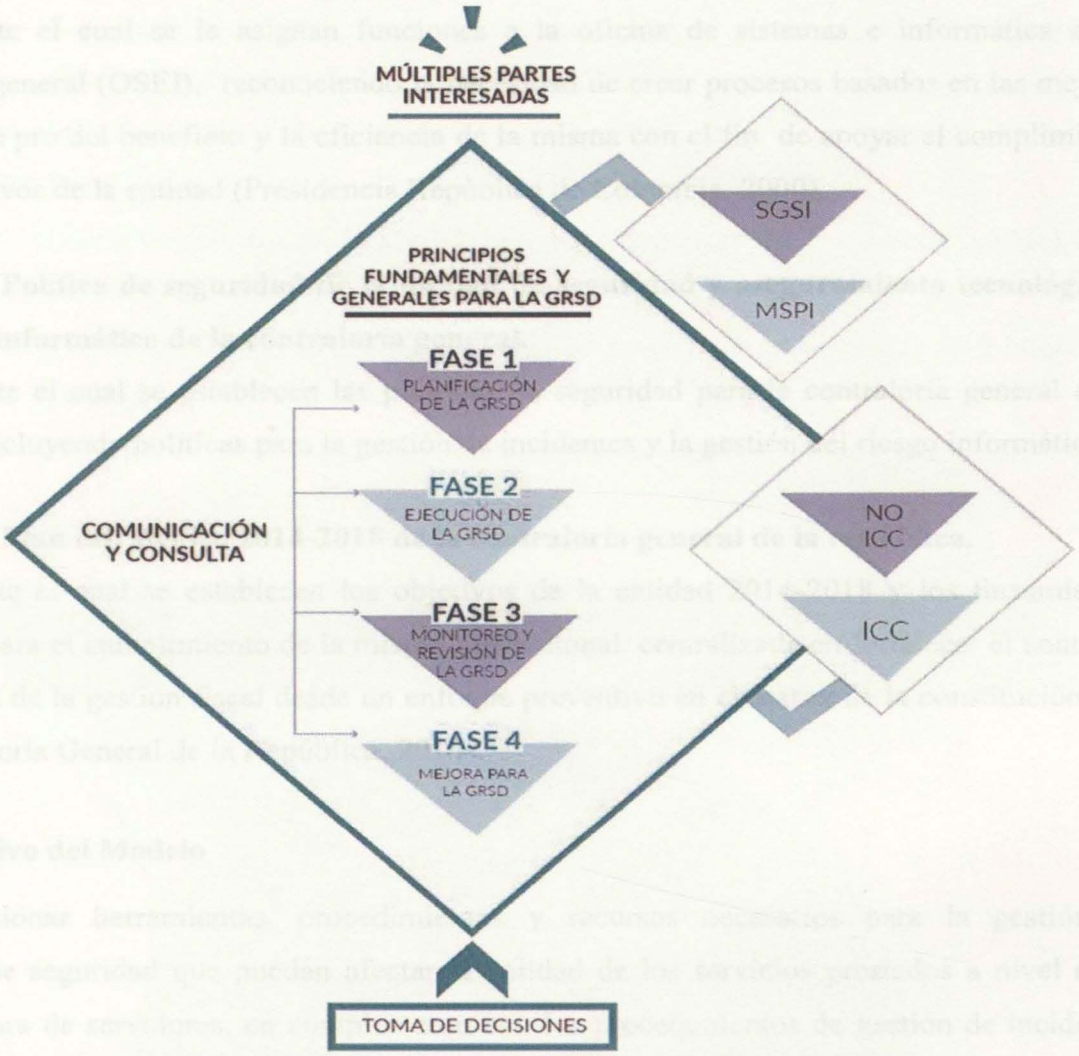

Figura 16.Marco conceptual del modelo MGRSD. Recuperado de Mintic. http://mintic.gov.co/portal/604/ w3-article-61854.html

2.1.3. Decreto 1078 de 2015.

Decreto único reglamentario del sector de las tecnologías de la información y las telecomunicaciones donde en el marco de la implementación del proyecto de Gobierno el Línea (GEL), determina la necesidad de que las entidades planteen, acojan e implementen modelos de seguridad y privacidad de la información con el objetivo de contar con un sistema de gestión de seguridad de la información eficiente y acorde a las necesidades de la empresa o entidad. (Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, 2015)

Modelo de Gestión de incidentes de seguridad CGR.

2.1.4. Decreto 267 de 2000.

Mediante el cual se le asignan funciones a la oficina de sistemas e informática de la contraloría general (OSEI), reconociendo la necesidad de crear procesos basados en las mejores prácticas en pro del beneficio y la eficiencia de la misma con el fin de apoyar el complimiento de los objetivos de la entidad (Presidencia República de Colombia, 2000).

2.1.5. Política de seguridad de la unidad de seguridad y aseguramiento tecnológico e informático de la contraloría general.

Mediante el cual se establecen las políticas de seguridad para la contraloría general de la república, incluyendo políticas para la gestión de incidentes y la gestión del riesgo informático.

2.1.6. Plan estratégico 2014-2018 de la contraloría general de la república.

Mediante el cual se establecen los objetivos de la entidad 2014-2018 y los lineamientos necesarios para el cumplimiento de la misión institucional centralizada en fortalecer el control y la vigilancia de la gestión fiscal desde un enfoque preventivo en el marco de la constitución y la ley (Contraloría General de la República, 2015).

2.2. Objetivo del Modelo

Proporcionar herramientas, procedimientos y recursos necesarios para la gestión de incidentes de seguridad que puedan afectar la calidad de los servicios prestados a nivel de la infraestructura de servidores, en complemento con los procedimientos de gestión de incidentes existentes en la entidad implementados mediante el programa de fortalecimiento institucional vigente.

2.3. Alineación con el Negocio y Apoyo a los Objetivos Institucionales

Para el logro de su misión institucional de "Fortalecer el control y la vigilancia de la gestión fiscal con enfoque preventivo en el marco de la constitución y la ley, para garantizar el buen manejo de los recursos públicos, en la búsqueda de la eficiencia y la eficacia de la gestión pública, con participación de la ciudadanía, para el logro de los fines del Estado" (Contraloría General de la República, 2015), la Contraloría General de la República mediante su plan estratégico 2014-2018 define los siguientes objetivos corporativos:

- Fortalecer el modelo de la vigilancia y control fiscal orientado a resultados efectivos y a la mejora de la gestión pública.
- Ejercer el control fiscal macro a las políticas públicas en sus objetivos de mediano y largo plazo.
- Lucha frontal, oportuna y efectiva contra la corrupción e inadecuada gestión de los recursos públicos.
- Construir ciudadanía solidaria, incluyente y activa en el control fiscal a la gestión pública.
- Asegurar el funcionamiento y la organización de la CGR para lograr resultados.

Objetivos que se encuentran plasmados en la Figura 17 a continuación:

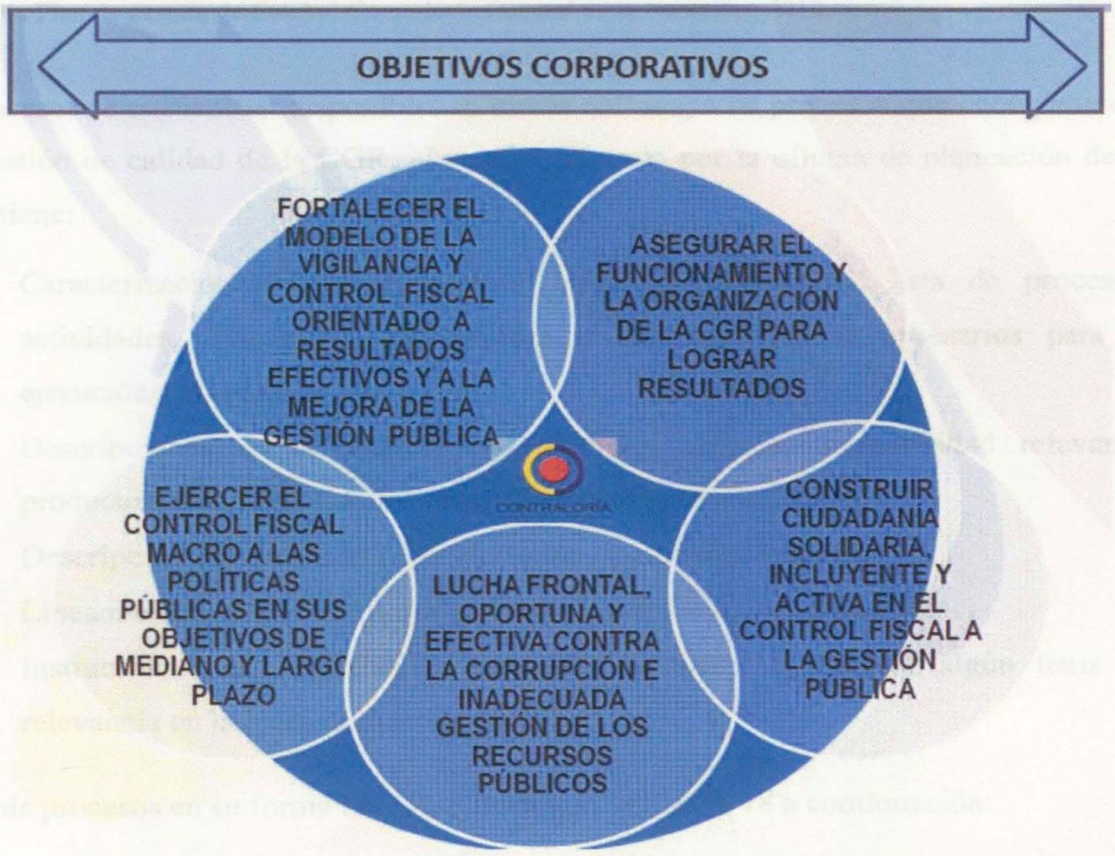

Figura 17. Objetivos corporativos CGR. Recuperado de Plan estratégico- Contraloría general de la República 2014-2018.

Modelo de Gestión de incidentes de seguridad CGR.

Para el alcance de estos objetivos la Contraloría General plantea el desarrollo de procesos clasificados de la forma observada en la Tabla 1.

Tabla 1
Clasificación de procesos CGR.

Clasificación del proceso	**Descripción**
Misionales	Procesos orientados al cumplimiento de la misión institucional de la entidad.
Estratégicos	Procesos que alinean la entidad hacia el cumplimiento de la visión y la misión institucional.
Apoyo	Procesos necesarios para soportar la operación diaria de la CGR.
Evaluación y control	Procesos que propenden por el mejoramiento continuo de la entidad

Nota. Adaptado de Plan de gestión de Calidad Contraloría General de la República 2018.

Estos procesos se encuentran disponibles a través del mapa de procesos que hace parte del sistema de gestión de calidad de la CGR, el cual es liderado por la oficina de planeación de la entidad y contiene:

- Caracterización del Macroproceso: objetivo, responsable, lista de procesos, actividades, descripción de entradas y salidas, recursos necesarios para la ejecución y riesgos.
- Descripciones de procedimientos: objetivo, alcance, normatividad relevante, productos, actividades de los procedimientos y responsables.
- Descripción del resultado de la ejecución de un procedimiento.
- Lineamientos corporativos que guían la ejecución de sus procesos.
- Instrucciones que detallan la forma de gestionar o manejar algún tema de relevancia en la ejecución de los procesos.

El mapa de procesos en su forma básica se ilustra en la Figura 18 a continuación:

Modelo de Gestión de incidentes de seguridad CGR.

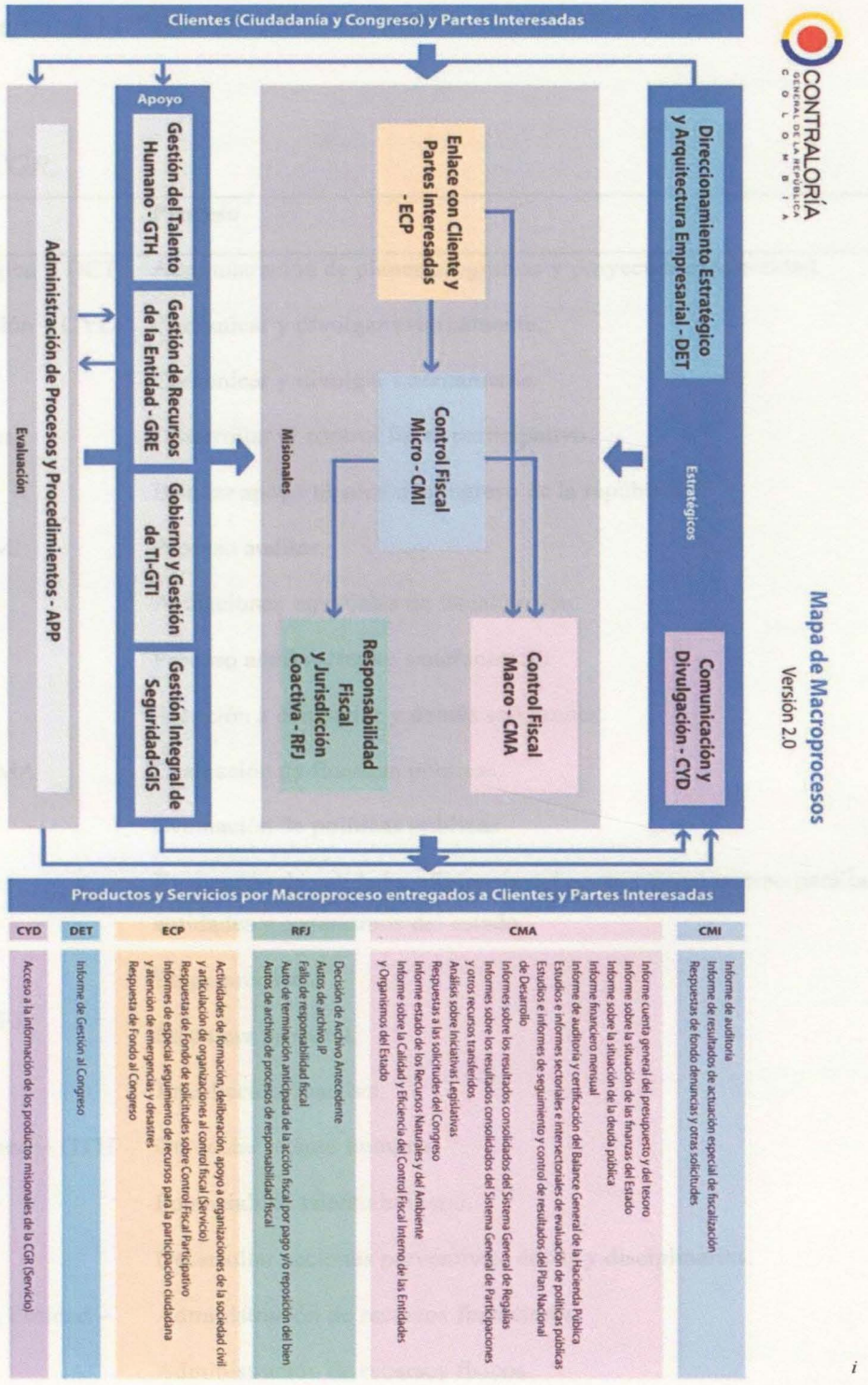

Figura 18. Mapa macroprocesos CGR. Recuperado de Plan de gestión de calidad Contraloría General de la República, 2018.

Modelo de Gestión de incidentes de seguridad CGR.

Dentro de cada uno de los macroprocesos anteriores la entidad cuenta con los siguientes procesos como se observa en la Tabla 2.

Tabla 2
Cuadro de procesos CGR.

Macroproceso	**Proceso**
Direccionamiento Estratégico – DET	Administración de planes programas y proyectos en la entidad.
Comunicación y Divulgación – CYD	Comunicar y divulgar externamente.
	Comunicar y divulgar internamente.
Enlace con Cliente y Partes Interesadas – ECP	Desarrollar el control fiscal participativo.
	Brindar apoyo técnico al congreso de la república.
Control Fiscal Micro – CMI	Proceso auditor.
	Actuaciones especiales de fiscalización.
	Proceso administrativo sancionatorio
	Atención a denuncias y demás solicitudes.
Control Fiscal Macro – CMA	Evaluación de finanzas públicas.
	Evaluación de políticas públicas
	Evaluación de calidad y eficiencia del control fiscal interno para las entidades y organismos del estado.
Responsabilidad Fiscal y Jurisdicción Coactiva – RFJ	Etapa procesal.
	Etapa pre procesal.
	Jurisdicción coactiva.
Gestión del Talento Humano – GTH	Gerenciar talento humano.
	Potencializar talento humano.
	Desarrollar acciones preventivas, éticas y disciplinarias.
Gestión de Recursos de la Entidad – GRE	Administración de recursos financieros.
	Administración de recursos físicos.
	Administración de recursos informáticos.
	Administración de la documentación.

	Administración de seguridad y aseguramiento.
Gobierno y Gestión de Tecnologías de la información – GTI	Estrategia y gobierno de TI.
	Desarrollo e implementación de soluciones tecnológicas y servicios de TI.
	Administrar servicios de TI.
Administración de Procesos y Procedimientos – APP	Administración del sistema integrado de gestión y control de calidad.
	Evaluación y control independiente.
Gestión Integral de la Seguridad – GIS	Administrar sistemas de gestión de seguridad.
	Gestión de incidentes de seguridad.
	Gestión de continuidad del negocio.

Nota. Adaptado de Plan estratégico Contraloría General de la República, 2018.

2.3.1. Alineación a nivel de procesos de apoyo.

La alineación con los procesos de la entidad se lleva a cabo a nivel de los macroprocesos de apoyo "Gobierno y gestión de las tecnologías de la información-GTI" y "Gestión integral de la seguridad –GIS", los cuales contemplan las actividades listadas en la Tabla 3 y Tabla 4 para su desarrollo (Contraloría General de la República, 2015).

Tabla 3
Macroproceso GTI. Fuente: Plan estratégico CGR.

MACROPROCESO	**Gobierno y Gestión de Tecnologías de la información – GTI**
PROCESOS	Estrategia y gobierno de TI.
	Desarrollo e implementación de soluciones tecnológicas y servicios de TI.
	Administrar servicios de TI.
DEPENDENCIA RESPONSABLE	Oficina de Sistemas e Informática OSEI.
ACTIVIDADES	Administrar la operación de los servicios de ti
	Administrar servicios de ti
	Definir acciones derivadas del seguimiento al portafolio y de la asignación de recursos.
	Desarrollar y mantener sistemas de información

	Diseñar servicios de ti
	Distribuir recursos en proyectos, servicios y operación de ti
	Establecer direccionamiento estratégico de ti
	Gestionar entrega de servicios de ti (implementación y puesta en producción)
	Gestionar proyectos de ti
	Realizar seguimiento al portafolio de ti y a la asignación de recursos

Nota. Adaptado de Plan estratégico Contraloría General de la República, 2018.

Tabla 4

Macroproceso GIS. Fuente: Plan estratégico CGR.

MACROPROCESO	**Gestión Integral de la Seguridad – GIS**
PROCESOS	Administrar sistemas de gestión de seguridad.
	Gestión de incidentes de seguridad. (bajo implementación)
	Gestión de continuidad del negocio
DEPENDENCIA RESPONSABLE	Unidad de Seguridad y Aseguramiento Tecnológico e Informático USATI.
ACTIVIDADES	Administrar la información relacionada con los incidentes de seguridad
	Apoyar a los servidores públicos de la CGR en el trámite para la solicitud de su protección ante la unidad nacional de protección.
	Dar respuesta a incidentes de seguridad.
	Definir lineamientos de seguridad de la información en proyectos e iniciativas.
	Definir los controles de seguridad de bienes
	Desarrollar actividades de sensibilización de la continuidad del negocio
	Establecer, implementar, mantener y mejorar el sistema de gestión de seguridad - SGS.
	Evaluar incidentes de seguridad para registro e implementación de las lecciones aprendidas
	Formular planes de prevención y detección de incidentes de seguridad
	Gestionar autorizaciones de ingreso y egreso de personas a las instalaciones de la CGR, cuando así se requiera.

	Gestionar la entrada y salida de bienes institucionales, cuando así se requiera.
	Gestionar los riesgos de seguridad y verificar la efectividad de sus controles asociados.
	Liderar la implementación de buenas prácticas para el desarrollo de la continuidad del negocio.
	Monitorear la implementación de buenas prácticas para el desarrollo de la continuidad del negocio y reportar su estado a las instancias pertinentes.
	Orientar a las áreas en la elaboración y actualización de los planes de continuidad del negocio
	Realizar análisis de información (laboratorio de informática forense - LIF).
	Verificar y monitorear el cumplimiento normativo sobre el componente de seguridad y privacidad de la información.

Nota. Adaptado de plan estratégico Contraloría General de la República, 2018.

A cargo de estos macroprocesos la entidad cuenta con 2 dependencias a saber:

2.3.1.1.Oficina de sistemas e informática OSEI.

Creada bajo decreto 267 de 2000 mediante el cual se dictan normas de la organización y funcionamiento de la CGR, y de acuerdo con el artículo 50 del mismo decreto (Presidencia República de Colombia, 2000). La OSEI tiene las siguientes funciones:

- Asistir al Contralor General y por su conducto a la administración de la Contraloría General de la República, en el desarrollo de los sistemas, normas y procedimientos de informática requeridos por las dependencias de la entidad.
- Elaborar los diseños de programas, la codificación y las otras tareas requeridas para la programación de reportes y cómputo de información.
- Determinar las tecnologías y técnicas requeridas para la recolección, el procesamiento y la emisión de información.
- Establecer los controles sobre utilización de equipos y verificar la calidad del trabajo que se realice sobre los mismos.
- Asesorar en el procesamiento de la información que requieran las diferentes dependencias de la Contraloría General de la República.

- Realizar investigaciones para diseñar y sugerir la utilización óptima de equipos electrónicos, de los sistemas y del software.
- Realizar estudios que permitan determinar la factibilidad técnica y económica de sistematizar las aplicaciones que requiera la Contraloría General de la República.
- Realizar o participar técnicamente en los procesos de contratación tendientes al análisis, diseño y programación de las aplicaciones que vayan a ser sistematizadas.
- Elaborar los diferentes manuales de aplicación ajustados a las normas existentes.
- Realizar el mantenimiento adecuado a los programas de computación para satisfacer los cambios en las especificaciones de los sistemas.
- Establecer los controles necesarios para llevar el historial de las modificaciones que se efectúen en los programas o aplicaciones.
- Velar por la seguridad del acceso a las instalaciones donde se encuentren los equipos electrónicos.
- Definir las prioridades y prestar los servicios de cómputo que se requieran.
- Dictaminar sobre requerimientos de mantenimiento y conservación de los equipos por las diferentes dependencias y garantizar las reparaciones correspondientes.
- Las demás que le asigne la ley.

Para el desempeño de sus funciones la OSEI cuenta con la organización ilustrada en la Figura 19.

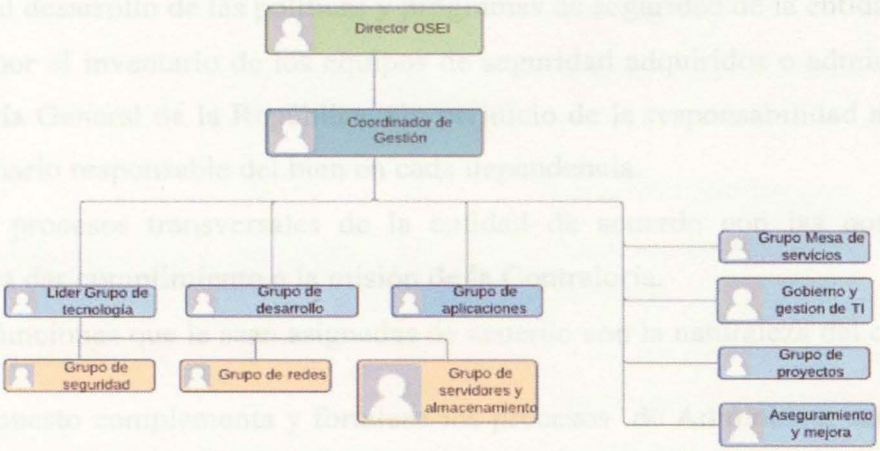

Figura 19. Organigrama oficina de sistemas e informática. Fuente: Elaboración propia.

Modelo de Gestión de incidentes de seguridad CGR.

2.3.1.2. Unidad de seguridad y aseguramiento tecnológico e informático USATI.

La USATI es la dependencia encargada de administrar la seguridad tanto física como tecnológica e informática de la entidad, y con base en el artículo 4 de la resolución reglamentaria 205 de 2012 por la cual se determina su funcionamiento tiene las siguientes funciones (Contraloría General de la República, 2012):

- Dirigir y adoptar las Políticas, Planes, Programas y estrategias para el desarrollo de la seguridad y aseguramiento tecnológico en el cumplimiento de la misión organizacional de la Contraloría General de la República.
- Formular estrategias encaminadas a ejecutar las políticas, planes y programas de seguridad de los servidores públicos de la Contraloría General de la República y de los bienes y de la información de la entidad de acuerdo con las normas legales vigentes para el cumplimiento de los objetivos institucionales.
- Promover la celebración de convenios con entidades y organismos nacionales e internacionales para garantizar la protección de las personas, la custodia de los bienes y confidencialidad e integridad de los datos manejados por la institución de acuerdo con las normas legales vigentes para cumplir con la misión de la entidad.
- Garantizar el uso y mantenimiento adecuado de los equipos de seguridad adquiridos o administrados por la Contraloría General de la República, de acuerdo con las normas legales vigentes para el cumplimiento de los objetivos institucionales.
- Presentar al Contralor General de la República y al Vicecontralor las estrategias que coadyuven al desarrollo de las políticas y programas de seguridad de la entidad.
- Responder por el inventario de los equipos de seguridad adquiridos o administrados por la Contraloría General de la República, sin perjuicio de la responsabilidad adquirida por cada funcionario responsable del bien en cada dependencia.
- Apoyar los procesos transversales de la entidad de acuerdo con las normas legales vigentes para dar cumplimiento a la misión de la Contraloría.
- Las demás funciones que le sean asignadas de acuerdo con la naturaleza del cargo.

El modelo propuesto complementa y fortalece los procesos de Administrar servicios de TI de la oficina de sistemas e informática y Gestión de incidentes de seguridad de la unidad de seguridad y aseguramiento tecnológico e informático contribuyendo con procedimientos y

conocimientos relevantes al desarrollo de cada uno de estos procesos y dependencias involucradas en pro del logro de sus objetivos.

2.3.1.3.Responsabilidades de la OSEI y la USATI frente al proceso de gestión de incidentes.

Con el fin de enmarcar las responsabilidades de las dependencias involucradas en el desarrollo del proceso de gestión de incidentes y con base en la política de continuidad del negocio de la entidad (documento SGS-I-A17-PO-001), se relacionan en la Tabla 5 cada uno de los elementos pertenecientes al ciclo Deming de mejora continua, conocido generalmente como ciclo PHVA (Planear, Hacer, Verificar, Actuar).

Tabla 5
Ciclo Deming del modelo

Responsabilidad frente a la gestión de incidentes de seguridad.	**OSEI**	**USATI**	**COMENTARIOS**
PLANEAR			
Identificación de vulnerabilidades		X	Con base en las funciones definidas para la dependencia.
Determinación de políticas		X	Con base en el manual de funciones definidas para la dependencia.
Identificación de parches de seguridad	X	X	De acuerdo a sus funciones.
Determinación de los servicios críticos de TI.	X		De acuerdo a sus funciones de administración.
Definición de estrategias	X	X	De acuerdo a sus funciones.
HACER			
Aplicación de políticas	X	X	De acuerdo a sus funciones.
Implementación del modelo	X		Cuenta con el acceso directo a la plataforma.
Acciones de erradicación de amenazas		X	De acuerdo a sus funciones. Administra las herramientas.
Acciones de recuperación	X		De acuerdo a sus funciones.
VERIFICAR			

Monitoreo y revisión continua	X		Mediante vigilancia y pruebas periódicas
Monitoreo y revisión semanal		X	De acuerdo a la frecuencia programada por la dependencia, varía de acuerdo al estado de alerta.
ACTUAR			
Revisión del modelo	X	X	Debe de ser un trabajo conjunto.
Mejoramiento del modelo	X	X	Debe de ser un trabajo conjunto.

Nota. Elaboración propia.

2.3.2. Apoyo a procesos misionales y servicios.

La entidad cuenta con 4 macroprocesos misionales y dos macroprocesos estratégicos encargados de prestar los servicios a clientes y partes interesadas según lo ilustran la Tabla 6 y Tabla 7.

Tabla 6
Catálogo de servicios para procesos misionales.

PROCESOS MISIONALES	
MACROPROCESO	PRODUCTOS O SERVICIOS
Control Fiscal Micro – CMI	Informe de Auditoría.
	Informe de resultados de actuación especial de fiscalización.
	Respuesta de fondo denuncias y otras solicitudes.
Control Fiscal Macro – CMA	Informe cuenta general del presupuesto y del tesoro.
	Informe sobre situación de las finanzas del estado.
	Informe sobre la situación de la deuda pública.
	Informe financiero mensual
	Informe de auditoría y certificación del balance general de la hacienda pública.
	Estudios e informes sectoriales e intersectoriales de evaluación de políticas públicas.
	Estudios e informes de seguimiento y control de resultados del plan

	nacional de desarrollo.
	Informes sobre los resultados consolidados del sistema general de regalías.
	Informes sobre los resultados consolidados del sistema general de participaciones y otros recursos transferidos.
	Análisis sobre iniciativas legislativas.
	Respuestas a solicitudes del congreso.
	Informe estado de los recursos naturales y del ambiente.
	Informe sobre la calidad y eficiencia del control fiscal interno de las entidades y organismos del estado.
Responsabilidad Fiscal y Jurisdicción Coactiva – RFJ	Decisión de archivo antecedente.
	Autos de archivo IP.
	Fallo de responsabilidad fiscal.
	Auto de terminación anticipada de la acción fiscal por pago y/o reposición del bien.
	Autos de archivo de procesos de responsabilidad fiscal.
Enlace con Cliente y Partes Interesadas – ECP	Actividades de formación, deliberación, apoyo a organizaciones de la sociedad civil y articulación de organizaciones al control fiscal.
	Respuestas de fondo a solicitudes sobre control fiscal participativo.
	Informes de especial seguimiento de recursos para la participación ciudadana y atención de emergencias y desastres.
	Respuesta de fondo al congreso.

Nota. Tomado de plan estratégico Contraloría General de la República, 2018.

Tabla 7

Catálogo de servicios procesos estratégicos.

PROCESOS ESTRATÉGICOS	
MACROPROCESO	**PRODUCTOS O SERVICIOS**
Direccionamiento Estratégico y Arquitectura Empresarial– DET	Informe de gestión al congreso.

Comunicación y divulgación - CYD	Servicio de acceso a la información de los de los productos misionales de la entidad.

Nota. Tomado de plan estratégico Contraloría General de la República, 2018.

Los servicios e igualmente los macroprocesos misionales, estratégicos y de apoyo de la entidad para su desarrollo en pro de los objetivos de la entidad se encuentran apalancados en un conjunto de aplicaciones que a su vez están sustentadas sobre la infraestructura de servidores de la entidad como se observa en la Tabla 8, la cual lista algunas de las aplicaciones más importantes para la entidad.

Tabla 8
Aplicaciones principales CGR.

APLICACIONES	
Nombre	**Descripción**
SIRECI	Sistema de rendición de Electrónica de la Cuenta e Informes que permite a los sujetos de control y entidades del estado presentar su rendición de cuentas e informes a la entidad.
SIREF	Sistema de información de responsabilidad fiscal. Proporciona un registro de todas las actuaciones relacionadas con la responsabilidad fiscal.
SIPAR	Sistema de información de participación ciudadana. Lleva un registro de las diferentes mecanismos de participación ciudadana, como las quejas, denuncias, solicitudes, etc.
SIGEDOC	Sistema de gestión documental.
SIBOR	Boletín de responsables fiscales. Expedición de certificados.
KACTUS	Software de Nomina funcionarios.
PORTAL	Portal institucional. Su importancia radica en que se constituye en la puerta de acceso a servicios de Sibor, Sireci y otros.
INTRANET	Portal interno CGR
INVENTARIOS	Inventario de recursos del almacén asignados a los funcionarios.
SAE	Sistema de aseguramiento electrónico de expedientes

DEUDA PÚBLICA	Registro de la deuda pública estatal.
PRORROGAS	Gestión de prorrogas en el sistema de rendición de cuentas.

Nota. Tomado de plan estratégico CGR, 2018.

En concordancia con lo anterior, la Tabla 9 representa la relación de las aplicaciones con los macroprocesos de la Figura 18 pertenecientes a la entidad.

Tabla 9
Relación aplicaciones vs macroprocesos.

	MACROPROCESOS									
APLICACIONES	**DET**	**CYD**	**ECP**	**CMI**	**CMA**	**RFJ**	**GTH**	**GRE**	**GTI**	**APP**
SIRECI				X	X					
SIREF						X				
SIPAR			X							
SIGEDOC			X							
SIBOR			X							
KACTUS							X	X		
PORTAL		X								X
INTRANET		X							X	X
INVENTARIOS								X		
SAE				X	X	X				
DEUDA PÚBLICA					X					
PRORROGAS				X	X					

Nota. Tomado de Plan Estratégico CGR, 2018.

Y con base en la Tabla 9 es posible identificar cuales aplicaciones pueden considerarse de apoyo, estratégicas o misionales como se observa en la Tabla 10.

.

Tabla 10
Clasificación aplicaciones.

APLICACIÓN	CLASIFICACIÓN		
	ESTRATÉGICA	MISIONAL	APOYO
SIRECI		X	
SIREF		X	
SIPAR		X	
SIGEDOC		X	
SIBOR		X	
KACTUS			X
PORTAL	X		
INTRANET	X		
INVENTARIOS			X
SAE		X	
DEUDA PÚBLICA		X	
PRORROGAS		X	

Nota. Elaboración propia.

Luego, mediante el análisis de las Tablas 9 y 10 es claro definir que las tecnologías de la información forman un componente principal en el alcance de los objetivos de la entidad, dado que se encuentran relacionados con todos los macroprocesos misionales de la misma, por lo que una afectación a la infraestructura de servidores al influir directamente sobre las aplicaciones y macroprocesos, puede lesionar gravemente el cumplimiento de los objetivos y la misión institucional. La importancia del modelo de gestión de incidentes para la infraestructura de servidores radica en reducir los riesgos de materialización de un incidente al igual que en minimizar sus efectos en caso de ocurrencia del mismo.

2.4. Identificación del Riesgo Sobre la Infraestructura de Servidores

Para determinar el riesgo a nivel de seguridad presente en la infraestructura, es necesario conocer cuáles son las vulnerabilidades y amenazas que existen al respecto, dado que la

adecuada gestión de las mismas podrá evitar y minimizar el daño causado con la ocurrencia de algún incidente.

Las siguientes son algunas de las amenazas más comunes y de más impacto que podrían afectar la infraestructura:

- Denegación de servicio (DoS): Consiste en saturar los servicios prestados por el servidor o servidores de forma tal que este ya no pueda resolver más las peticiones de usuarios y termine bloqueado.
- Ejecución de código remoto: El aprovechamiento de este tipo de vulnerabilidades permitiría la ejecución de código malicioso en la maquina atacada por parte del atacante.
- Escalamiento de privilegios: Darle privilegios por lo general de administrador a cuentas de usuarios básicas, utilizadas por el atacante.
- Cross-site scripting (XSS): inyectar código malicioso (por lo general javascript) en páginas web visitadas saltando por encima de las políticas de seguridad del servidor.
- Inyección de código SQL: Inyección de código SQL que permite extraer información no autorizada de las bases de datos.
- Desbordamiento de buffer (Buffer overflow): Ocasionar el desbordamiento del área de memoria reservada para el buffer, de forma tal que se puedan escribir datos en áreas de memoria adyacentes provocando un mal funcionamiento tanto a nivel de software, como del hardware de la máquina.
- Acceso no autorizado a información sensible: Mediante la ejecución de códigos o programas, obtiene información sensible del servidor o equipo.

Para conocer las necesidades de la entidad al respecto de la seguridad y la gestión de incidentes relacionados, se realiza un análisis de la infraestructura sobre la cual corren algunos de los servicios más importantes, identificando alguna de las vulnerabilidades más comunes y que podrían estar afectando CGR, con la identificación de estas vulnerabilidades se podrá hacer un acercamiento a un mapa de riegos a nivel de ciberseguridad que se constituirá en un insumo necesario para el planteamiento de un modelo adecuado y ajustado lo más posible a las necesidades del negocio.

Es de notar que con base en las implicaciones legales y de reserva requeridas por la entidad, la información del levantamiento no revelará información sensible y se limitará a resaltar vulnerabilidades conocidas a nivel de sistemas, procesos y/o procedimientos transversales de mayor utilización. En el caso de que la misma llegase a contemplarse como confidencial por la CGR, se deberá tener en cuenta el acuerdo de confidencialidad anexo en el apéndice B.

El modelo de la infraestructura de servidores de la contraloría general corresponde a un ambiente virtualizado constituido desde un punto de vista amplio por 4 componentes como lo ilustra la Figura 20:

- Red de almacenamiento SAN (Storage Area Nekwork).
- Maquina o servidor físico (host).
- Hipervisor o software de virtualización.
- Máquina virtual.

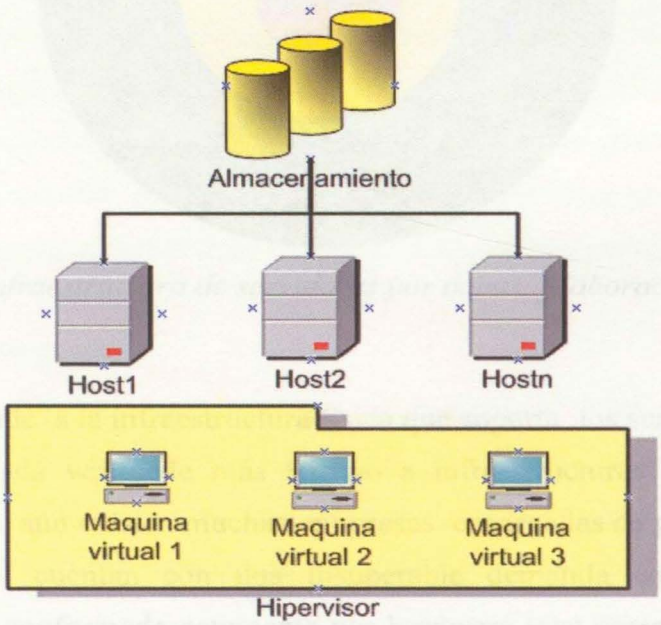

Figura 20. Modelo infraestructura de servidores CGR. Elaboración propia.

La unión de estos componentes permite que cada máquina virtual funcione como un único equipo donde es posible instalar además de un sistema operativo, el software necesario para publicar los servicios que la Contraloría necesita para cumplir con su misión institucional, por

lo que con base en esto se plantea un análisis de vulnerabilidades contemplado a partir de cuatro capas donde las capas más internas dependen de las más externas para funcionar (ver Figura 21). Estas capas son:

- Física
- Virtualización
- Sistema operativo
- Aplicación

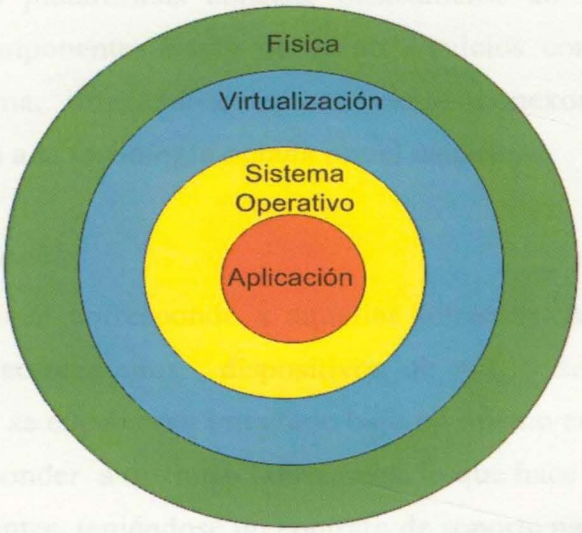

Figura 21. Modelo Infraestructura de servidores por capas. Elaboración propia.

2.4.1. Capa física

La capa física corresponde a la infraestructura física que soporta los servidores, y aunque si bien, esta infraestructura cada vez cede más terreno a infraestructuras virtuales, como los actuales servicios en la nube, aún existen muchas empresas encargadas de proveer estos bienes, dado que los mismos aun cuentan con una insuperable demanda en el mercado. Esta infraestructura se encuentra conformada netamente por hardware y su correspondiente software de administración y cuenta de varios componentes como lo son: los servidores, el almacenamiento SAN (Storage Area Network), switches de red y almacenamiento, etc. Entre los fabricantes más destacados para este tipo de productos se pueden encontrar: Hewlett Packard, Dell EMC, IBM, Cisco, Hitachi, Oracle, Etc. Cada fabricante se esfuerza por dar un toque de innovación a su producto, de forma tal, que pueda sobresalir más que el de sus competidores,

aunque la ventaja al final termina definiéndose en relación precio-calidad – beneficio, donde aquellos fabricantes con el mejor precio y calidad terminan por llevarse la mejor parte del pastel.

A nivel de estos servidores los fabricantes se han enfocado en tres tipos de tecnologías para sus plataformas:

- Infraestructura Tradicional
- Infraestructura convergente.
- Infraestructura hiperconvergente.

La diferencia entre estas plataformas consiste básicamente en el nivel de integración existente tanto a nivel de componentes hardware como servicios conexos para los distintos componentes de la plataforma, refiriéndose con servicios conexos al soporte postventa especialmente dado de acuerdo a la tecnología optada por el usuario.

2.4.1.1.Infraestructura tradicional.

La infraestructura tradicional corresponde a aquellas infraestructuras donde los distintos componentes tales como almacenamiento, dispositivos de red, y servidores son elementos independientes, por lo cual no se encuentran integrado bajo un mismo entorno de administración y normalmente pueden corresponder a distintos fabricantes, lo que hace que el soporte postventa generalmente sea por componentes, teniéndose un contrato de soporte para cada uno de ellos.

2.4.1.2.Infraestructura convergente.

La infraestructura convergente a diferencia de la tradicional trata de recoger todos los componentes bajo un mismo entorno de administración, proveyendo simplicidad y flexibilidad entre los mismos, dado que no se centra en uno de sus componentes en especial, permitiendo hacer combinaciones a nivel de hardware con la facilidad de contar con un servicio de soporte centralizado. Este tipo de infraestructura se encuentra orientado a las virtualizaciones, debido que en la gran mayoría de ocasiones el soporte también incluye este componente de software, todo con el fin de obtener el mejor rendimiento e integración posible. (Almeida Galárraga, 2015).

2.4.1.3.Infraestructura hiperconvergente.

La infraestructura hiperconvergente HCI (Hyper Converged Infrastructure) obedece a un modelo muy similar al de la infraestructura convergente, pues se trata de tener sus componentes soportados y administrados desde una única plataforma (simplicidad de administración) como un único equipo que combina servidores, almacenamiento, componentes de red y software de virtualización, pero con la característica de que todo se encuentra contenido dentro de un mismo rack o dispositivo escalable, donde la adquisición de más capacidad de computo u almacenamiento significa un upgrade o escalamiento de la plataforma adquirida. Por lo general, al simplificarse tanto la administración y al ser una plataforma que viene integrada desde fábrica, se posee un rendimiento mejorado, dado que el software de virtualización viene ajustado a las necesidades del equipo. (VmWare Inc., 2018).

Con respecto a empresas líderes en una u otra tecnología, la competencia ha sido pareja, aunque como se observa en la Figura 22 la competencia a nivel de hiperconvergencia es dominada por unas pocas compañías que cuentan con una mejor calificación.

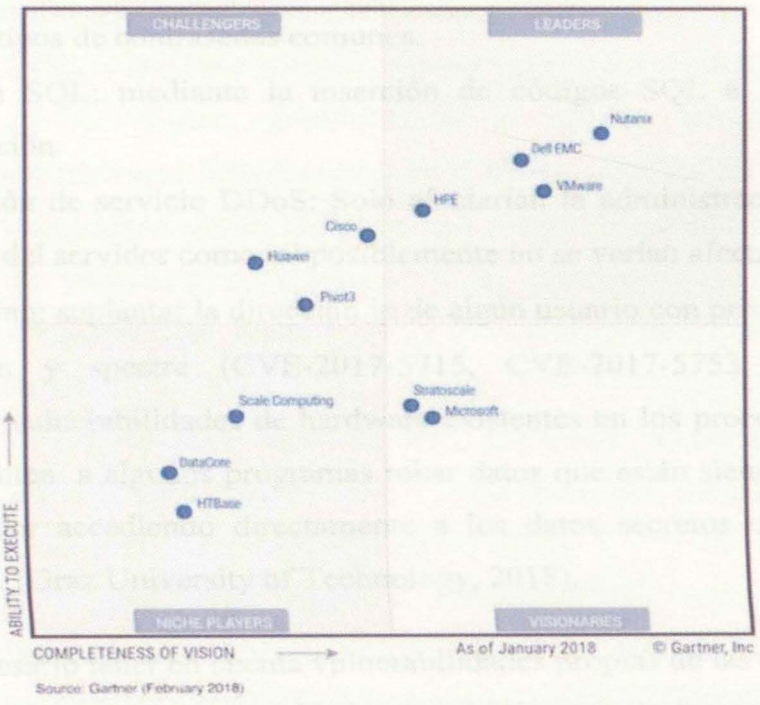

Figura 22. Cuadrante mágico de Gartner, empresas lideres en hiperconvergencia. Tomado de www.nutanix.com (Nutanix, 2018).

2.4.1.4. Vulnerabilidades conocidas en la infraestructura física.

Al poseer un software cerrado de uso específicamente de administración los mayores vectores de ataques corresponden a factores humanos, partiendo de debilidades como: las contraseñas de administración, faltas de actualización y el uso de equipos poco seguros para el acceso. Por lo que para este caso el modelo propuesto estará centrado en mitigar estos riesgos con el establecimiento de políticas seguras y mejores prácticas, siendo correspondiente resaltar que por tratarse de un sistema informático conformado por hardware y software existe una gran cantidad de vulnerabilidades implícitas, sobre todo en la forma como se accede a su administración, la cual por lo general es realizada mediante terminales con consola segura SSH (Secure Shell), Acceso seguro HTTPS (Hyper Text Transfer Protocol Secure) y software de administración propio de la marca.

Entre las vulnerabilidades más comunes que pueden llegar a afectar estos sistemas se tienen:

- Ingeniería Social y phising: Tratar de obtener las distintas contraseñas directamente de los usuarios.
- Fuerza Bruta: Intentar acceder al sistema mediante la prueba ensayo y error de distintos tipos de contraseñas comunes.
- Inyección SQL: mediante la inserción de códigos SQL a los formularios de autenticación.
- Denegación de servicio DDoS: Solo afectarían la administración, por lo que los servicios del servidor como tal posiblemente no se verían afectados.
- IP Spoofing: suplantar la dirección ip de algún usuario con privilegios.
- Meltdown y spectre (CVE-2017-5715, CVE-2017-5753, CVE-2017-5754): Explotan vulnerabilidades de hardware existentes en los procesadores modernos, que permiten a algunos programas robar datos que están siendo procesados en el computador accediendo directamente a los datos secretos que permanecen en memoria. (Graz University of Technology, 2018).

Igualmente es necesario tener en cuenta vulnerabilidades propias de las marcas que han sido descubiertas por personal experto en seguridad o los fabricantes de los equipos, dado que las misma representan un elemento muy importante para la elaboración del modelo. Las siguientes

corresponden a las vulnerabilidades publicadas para 2 fabricantes de infraestructura conocidos en el mercado como lo son Dell y Hewlett Packard (HPE):

- Dell EMC
  - CVE-2017-15548: Permite al atacante ingresar con privilegios de administrador a la plataforma de almacenamiento sin pasar por ningún control de autenticación. Esto se logra mediante el uso de cualquier servidor de que permita autenticarse, incluyendo aquellos que se encuentran comprometidos. (Dawn-Hiscox, 2018).
  - CVE-2017-15549: Permite al atacante descargar cualquier archivo contenido en la plataforma de almacenamiento usando privilegios de super usuario root. (Dawn-Hiscox, 2018).
  - CVE-2018-1213: Esta vulnerabilidad permite obtener privilegios de escalamiento mediante el uso del usuario compadmin, el cual puede correr el binario tcpdump con privilegios de root vía sudo, lo que permite posteriormente ejecutar comandos del Shell o código Python[3] con dichos privilegios. (Townsend, 2018).
  - CVE-2018-1204: permite obtener privilegios mediante escalamiento vía soporte remoto, permitiéndole al usuario ejecutar código Python arbitrario con privilegios de root. (Townsend, 2018). Igualmente Permite al atacante acceder mediante una cuenta de soporte remoto que contiene un password por defecto y se almacena en la herramienta de administración Open Manage Essentials (OME). (MITRE Corporation, 2018).
  - CVE-2018-1215: Un usuario malicioso autenticado remotamente, potencialmente puede subir código malicioso a cualquier ubicación del webserver. (MITRE Corporation, 2018).
  - CVE-2018-1216: Algunos aplicativos de administración virtuales contienen una cuenta por defecto (msc) con una contraseña que puede ser utilizada con ciertos programas residentes en el equipo. Un atacante

[3] Python: leguaje de programación interpretado, de uso muy popular.

remoto con el conocimiento de esta contraseña podría utilizar estos programas para concederse acceso. (MITRE Corporation, 2018).

La Figura 23 presenta un resumen de las vulnerabilidades encontradas en la totalidad de productos DELL.

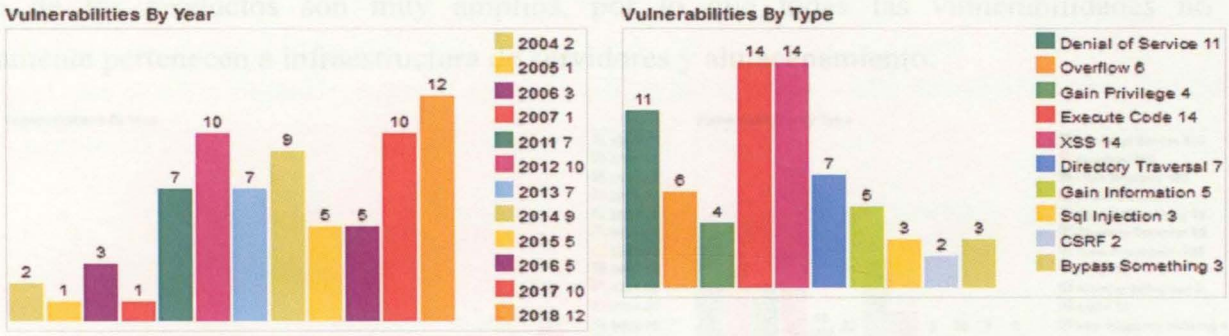

Figura 23. Histórico de vulnerabilidades que han afectado a los productos Dell. Tomado de www.cvedetails.com (MITRE Corporation, 2018)

- Hewlett Packard HPE
  - CVE-2015-5443: El procesador de servicios SPOCC del almacenamiento 3par permite la autenticación de usuarios remotos con el fin de obtener información sensible por medio de un vector desconocido. (MITRE Corporation, 2018).
  - CVE-2010-4115: HP storage Works p2000 un atacante puede ingresar a la interfaz de administración por medio de una cuenta admin que contiene una contraseña por defecto, lo que le permitiría al atacante darse privilegios. (Beyond Security, 2018).
  - CVE-2017-8987: Afecta a la interfaz de administración Hilo3, provocando una condición de denegación de servicio por alrededor de 10 minutos, (Barth, 2018).
  - CVE-2017-8994: una vulnerabilidad en la validación de entrada permite la ejecución de código remoto en el producto orquestador de operaciones HPE. (MITRE Corporation, 2018)
  - CVE-2016-4375: Múltiples vulnerabilidades sin especificar en la interfaz de administración Hilo3 e Hilo4 permiten que el atacante

obtenga información sensible, modifique datos o cause denegación de servicios. (MITRE Corporation, 2018).

La Figura 24 muestra un resumen histórico de las vulnerabilidades que han afectado a la totalidad de productos HP, es necesario especificar que al igual que en la Figura 23 el número el rango de los productos son muy amplios, por lo que todas las vulnerabilidades no necesariamente pertenecen a infraestructura de servidores y almacenamiento.

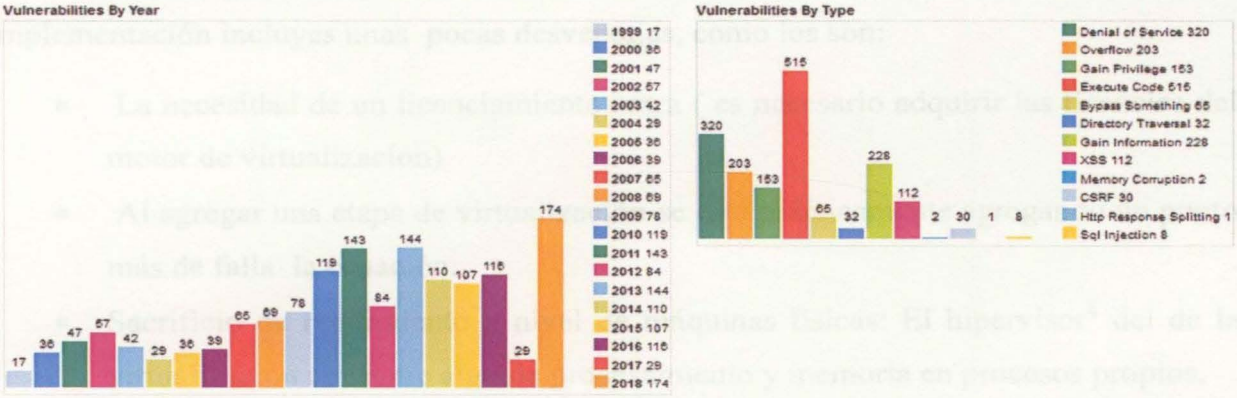

Figura 24. Histórico de vulnerabilidades que han afectado a los productos HP. Tomado de www.cvedetails.com. (MITRE Corporation, 2018)

2.4.2. Capa de virtualización.

La virtualización desde el punto de vista descrito por Microsoft y VMware, dos de las empresas líderes en este campo, consiste en utilizar software para recrear un entorno informático de equipos físicos (Microsoft Corporation, 2018) (VMWare Inc., 2018), lo que quiere decir que mediante herramientas de software es posible emular los dispositivos físicos necesarios para que una máquina o computador funcione. Esto conlleva una gran cantidad de beneficios entre los cuales se incluyen:

- Optimización de recursos.
- Administración simple.
- Movilidad.
- Independencia de hardware.
- Resiliencia.
- Respaldo.
- Recursos compartidos.

- Facilidad para el despliegue de equipos de respaldo tanto en centros de datos alternos, como en la nube.

Ventajas que se traducen en ahorro económico, al reducir la cantidad de servidores físicos, y en eficiencia a la hora de desplegar los recursos necesarios para cumplir con las demandas del negocio, dado que los despliegues requerirán de menos tiempo y esfuerzo por parte de los administradores.

Al igual que la virtualización ofreces estos notables beneficios, también es necesario indicar que su implementación incluyes unas pocas desventajas, como los son:

- La necesidad de un licenciamiento extra (es necesario adquirir las licencias del motor de virtualización)
- Al agregar una etapa de virtualización se está prácticamente agregando un punto más de falla la ecuación.
- Sacrificio de rendimiento a nivel de máquinas físicas: El hipervisor[4] del de la virtualización consume algo de procesamiento y memoria en procesos propios.
- Las fallas a nivel de hardware podrían afectar a más de una máquina.
- Los recursos son compartidos entre las máquinas que coexisten en la granja.

Aunque pese a estas desventajas, las ventajas que se tienen terminan siendo atractivas y más aún si existen limitaciones en el presupuesto económico para el desarrollo del proyecto asociado.

2.4.2.1. Principales proveedores de ambientes de virtualización y vulnerabilidades comunes.

Los analistas Thomas J. Bittman, Philip Dawson, y Michael Warrilow en su publicación del 3 de agosto de 2016 "Magic Quadrant for x86 Server Virtualization Infrastructure" (Gartner, Inc., 2016), Manifestaban que para esa época posiblemente alrededor del 80% de la infraestructura de servidores x86 utilizados se encontraban trabajando bajo ambientes virtualizados, realidad que en la actualidad, posiblemente no diste mucho de aquella época, la virtualización ya es cada vez más ofrecida como un servicio en internet y un plus en muchas plataformas de fabricantes de hardware. De hecho, la plataforma de la contraloría general de la

[4] Nombre con el que se le conoce al sistema sobre el cual corren las máquinas virtuales.

república cuenta con alrededor del 98% de sus servidores virtualizados, y los planes a futuro incluyen el contar con una plataforma 100% virtualizada con respaldo en la nube[5].

De esta forma, el prometedor uso masivo de esta tecnología ha provocado que cada vez sean más las empresas que le apuesten al desarrollo de la misma, ofreciendo desde hipervisores, hasta plataformas completas totalmente integradas, donde los clientes solo deben dedicarse a la administración de los servicios que corren sobre los servidores. Una muestra de ello se ve reflejada en la Figura 25 del cuadrante mágico de Gartner[6] referente a las plataformas de virtualización:

Figura 25. Cuadrante mágico para infraestructura de virtualización basada en x86. Tomado de https://www.gartner.com/doc/3400418/magic-quadrant-x-server-virtualization (Gartner, Inc., 2016)

Este cuadrante define a las compañías VMware y Microsoft como líderes del mercado, y a la compañía RedHat como visionaria, situación que siendo bastante ajustada a la realidad actual,

---

[5] plataforma de recursos informáticos distribuidas generalmente a lo largo de varios países con acceso mediante internet y administradas por operadores tanto públicos como privados.

[6] Representa gráficamente la situación del mercado con base en la visión y la capacidad de ejecución de las empresas fabricantes.

no desmerita en nada el trabajo realizado por compañías como Citrix, Oracle, Virtuozzo, Huawei y Sangfor que han realizado esfuerzos considerables por sostener su cuota en el mercado.

Se debe resaltar que más allá del el panorama expuesto y liderado por VMware , Microsoft y RedHat, alrededor de la virtualización existen un cúmulo de amenazas de seguridad que surgen día a día y normalmente son menguadas por los fabricantes mediante actualizaciones y parches de seguridad. Por lo que los administradores de las mismas, además de contar con el respectivo soporte, deben estar a la vanguardia de las noticias al respecto con el fin de aplicar los parches necesarios cuando esto sea posible.

2.4.2.2.Infraestructura de virtualización VMware.

La infraestructura de virtualización de VMware Vsphere® (Lowe, 2011) posiblemente es la marca más utilizada al momento de realizar un despliegue empresarial, esto debido a que VMware se constituyó en un pionero en el uso de estos sistemas, posicionándose en el mercado como un producto de excelente calidad y servicio. Su sistema básicamente se encuentra constituido por un hipervisor denominado ESXi (Elastic Sky X Integrated) y una herramienta de administración denominada Vcenter, desde el vcenter es posible administrar toda la plataforma e inclusive compartir sus recursos en la red LAN (Local Area Network) de la empresa (ver Figura 26).

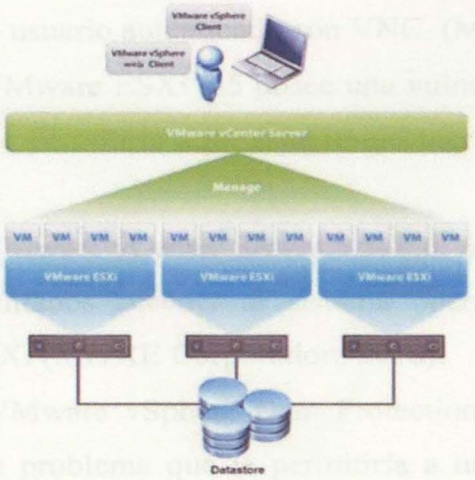

Figura 26. Infraestructura VMware vsphere. Tomado Virtualización de servidores con Vmware Vsphere 6 por David Peres Moriche (Moriche, 2016).

Modelo de Gestión de incidentes de seguridad CGR.

Adicional al Vcenter, VMware cuenta con un gran número de herramientas distribuidas como software adicional que permiten sacarle el provecho al máximo a la virtualización si las mismas son bien administradas. El hecho de que esta infraestructura se encuentre tan popularizada, también la hacen objeto de ataques, por lo que es común que cada cierto tiempo VMware publique actualizaciones de seguridad con el fin de contrarrestar posibles vulnerabilidades encontradas. Entre alguna de las vulnerabilidades más recientes tenemos:

- CVE-2017-4946: los Agentes de escritorio VMware V4H (Vrealize Operation for Horizon Desktop) y V4PA (Vrealize Operation for Published Aplication Desktop) permiten que un usuario con privilegios bajos pueda escalar a un usuario con privilegios del sistema. (MITRE Corporation, 2018)
- CVE-2018-6959: VMware vRealize Automation (vRA) anterior a la versión 7.4.0 contiene una vulnerabilidad en la administración del ID de las sesiones, lo que permitiría que un atacante se hiciera con la sesión de un usuario válido. (MITRE Corporation, 2018)
- CVE-2017-4943: VMware vCenter Server Appliance (vCSA) anterior a la version 6.5, permite el escalamiento de privilegios vía el plugin showlog. (MITRE Corporation, 2018)
- CVE-2017-4941: VMware ESXi 6.0 permite que VNC cause un desbordamiento de pila, lo que podría terminar con la ejecución de código remoto en la máquina virtual por parte del usuario autenticado con VNC. (MITRE Corporation, 2018).
- CVE-2017-4924: VMware ESXi 6.5 posee una vulnerabilidad en el componente de video SVGA que permitiría a un usuario ejecutar código en el host. (MITRE Corporation, 2018).
- CVE-2017-4919: VMware vCenter Server 5.5, 6.0, 6.5 le permitiría a un usuario con privilegios limitados acceder al sistema operativo sin estar autenticado mediante la API VIX. (MITRE Corporation, 2018).
- CVE-2017-4914: VMware vSphere Data Protection (VDP) 6.1.x, 6.0.x, 5.8.x, and 5.5.x posee un problema que le permitiría a un atacante remoto ejecutar comandos en la aplicación. (MITRE Corporation, 2018).

La Figura 27 ilustra el mapa de vulnerabilidades VMware.

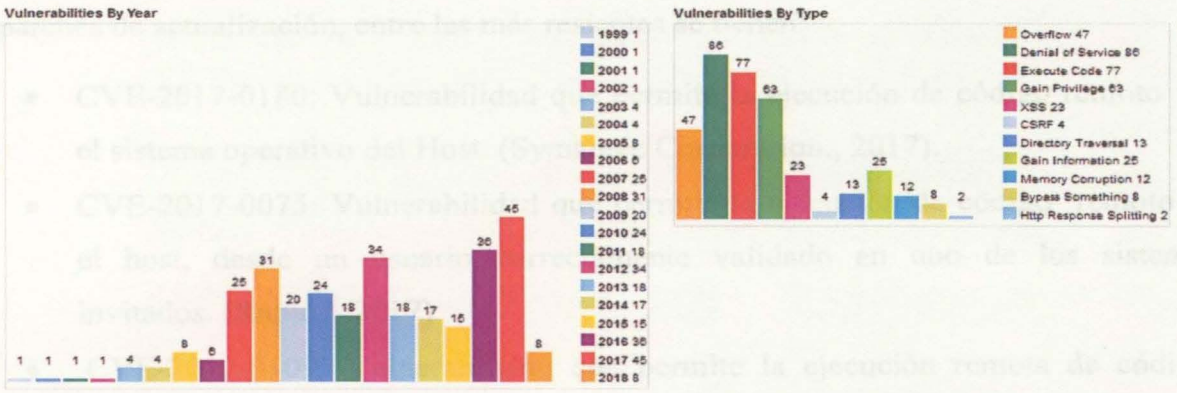

Figura 27. Mapa de vulnerabilidades VMware. Tomado de: www.cvedetails.com. (MITRE Corporation, 2018)

2.4.2.3.Infraestructura de virtualización Microsoft.

Microsoft, posee su infraestructura de virtualización basada en su hipervisor denominado Hyper V (ver Figura 28), el cual corre sobre Windows server 2012 y 2016 su sistema es mucho más económico que el VMware sobre todo si se adquiere en conjunto licencias de su sistema operativo, pero aún no capta la total confianza y aceptación de los usuarios que prefieren alternativas que les brinden más confianza al momento del uso. El impulso más grande a Hyper V se lo ha dado la solución en nube de Microsoft denominada Azure, la cual ha logrado cautivar a muchos usuarios con su simplicidad de uso, sus precios y la gran variedad de herramientas con las que cuenta. (Murugesan & Bojanova, 2016)

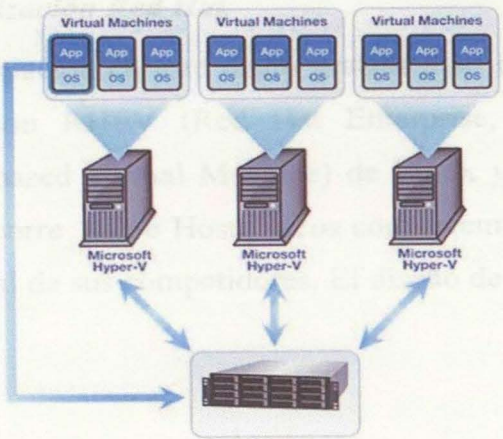

Figura 28. Infraestructura Hyper V de microsoft. Tomado de http://www.litsg.com. (LITSG, LLC, 2018)

Al igual que vsphere, cuenta con una gran lista de vulnerabilidades que han sido superadas mediante parches de actualización, entre las más resientes se tienen:

- CVE-2017-0180: Vulnerabilidad que permite la ejecución de código remoto en el sistema operativo del Host. (Symantec Corporation., 2017).
- CVE-2017-0075: Vulnerabilidad que permite la ejecución de código remoto en el host, desde un usuario correctamente validado en uno de los sistemas invitados. (Rapid7, 2017)
- CVE-2017-0109: Vulnerabilidad que permite la ejecución remota de código. (Symantec Corporation., 2017).
- CVE-2017-8664: Permite ejecutar código remoto en el sistema operativo del host. (Symantec Corporation, 2017).
- CVE-2017-8713: Hyper-V Information Disclosure Vulnerability, esta vulnerabilidad permite divulgar información cuando no valida correctamente el ingreso de usuarios autenticados a las máquinas virtuales. (MITRE Corporation, 2017).

Es de aclarar al Hyper-v correr sobre host con sistemas operativos Windows server 2012 y 2016, se ve igualmente afectado por las mismas vulnerabilidades que afectan a estos sistemas operativos y de las cuales más adelante se ilustrarán algunas.

2.4.2.4.Infraestructura de virtualización Red Hat.

Red Hat mantiene su participación en este nicho gracias a su infraestructura denominada Red Hat Enterprise Virtualization RHEV (Red Hat Enterprise, 2012). Siendo esta una integración entre KVM (Kernel-based Virtual Machine) de Linux y OpenStack[7]. RHEV con base en su hipervisor KVM que corre sobre Host físicos con sistema operativo Linux Red Hat promete un rendimiento superior al de sus competidores, El diseño de su infraestructura se puede ver en la Figura 29.

---

[7] Proyecto de código abierto que plantea que busca proveer infraestructura como servicio con base en la implementación de computación en la nube.

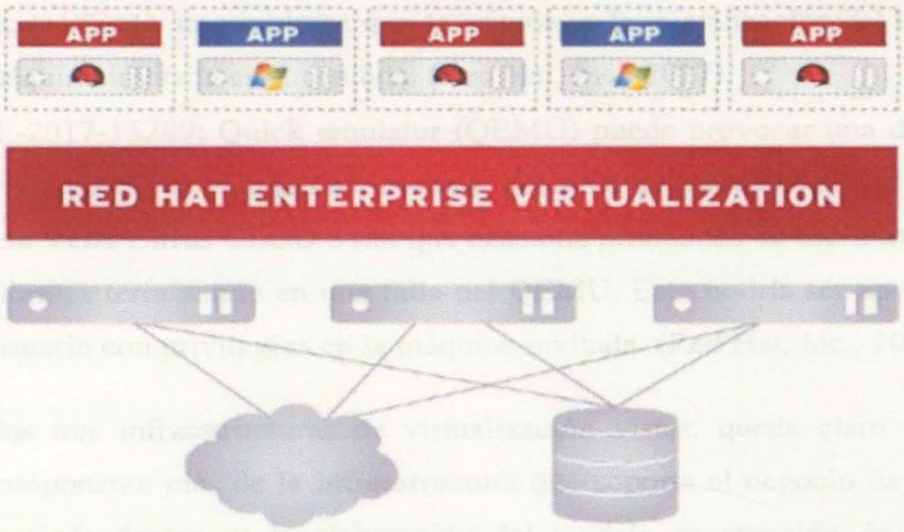

Figura 29. Infraestructura RHEV de Red Hat. Tomado de Technical update KVM and Red Hat Enterprise Virtualization (RHEV) (Red Hat Enterprise, 2012)

Igualmente no hay olvidar que como tal, esta infraestructura al igual que las anteriores ha poseído y poseerá vulnerabilidades que normalmente son remediadas mediante aplicación de parches y actualizaciones. Entre las vulnerabilidades más recientes se tienen:

- CVE-2016-4443: Afecta a Red Hat Enterprise Virtualization (RHEV) Manager 3.6 permitiendo a usuarios locales obtener llaves de encriptación, certificados e información confidencial mediante la lectura del log engine-setup. (MITRE Corporation, 2016).
- CVE-2017-5715: Un usuario con acceso local podría utilizar la ejecución especulativa que poseen algunos procesadores modernos para acceder a información privilegiada sin necesidad de una autorización. (Red Hat, Inc., 2018).
- CVE-2017-11334: Quick Emulator (QEMU) puede provocar una denegación de servicio (DoS) debido a un problema de acceso con lectura y escritura por fuera de límites, el cual puede ocurrir si un usuario con privilegios dentro de una maquina invitada (máquina virtual) ejecuta ciertas operaciones DMA (Direct Acces Memory). (Red Hat, Inc., 2017).
- CVE-2017-14167: Quick Emulator (QEMU) compilado con el PC system Emulator con soporte multiarranque permitiría a un usuario o proceso que se

ejecuta en una máquina invitada, realizar ejecución de código arbitrario en el Host, mediante un problema que se origina en la inicialización del kernel cuando la máquina invitada es encendida. (Red Hat, Inc., 2017).

- CVE-2017-15289: Quick emulator (QEMU) puede provocar una denegación de servicio (DoS) en la máquina invitada, debido a un problema con el soporte de la tarjeta VGA Cirrus CLGD 54xx que ocasiona problemas de escritura por fuera de los limites terminando en una falla del QEMU. Esto podría ser aprovechado por un usuario con privilegios en la máquina invitada (Red Hat, Inc., 2017) .

Con base en las tres infraestructuras de virtualización vistas, queda claro que al ser la virtualización un componente más de la infraestructura que soporta el negocio de la CGR, esta debe de ser contemplada dentro de la elaboración del modelo de atención de incidentes de seguridad, dado que la misma no está exenta de sufrir un incidente, pudiendo llegar a ser el talón de Aquiles del cual los atacantes claramente esperan sacar ventajas al momento de materializar un ataque.

2.4.3. Capa de Sistema operativo.

El autor Martín Silva, en su libro "sistemas operativos", describe el sistema operativo como un conjunto de elementos relacionados entre sí, que funcionan con un fin determinado, siendo este fin la operación y conducción del hardware (Silva, 2015). Esta afirmación si bien es cierta, en ocasiones se queda corta, dado que el sistema operativo tiene en sus manos la difícil tarea de gestionar todos los recursos existentes en una máquina, tanto software como hardware. Este decide cual aplicativo accede o tiene derecho a cual recurso, como interactúan entre ellos, los tiempos de ejecución, la interacción con los usuarios, etc. Motivo por el cual el sistema operativo es uno de los componentes más delicados y críticos al momento de la ocurrencia de un incidente de seguridad, y los mismos se configuran en los objetivos predilectos de los atacantes dado el nivel de daño que pueden causar y el poder que pueden adquirir si lo logran. De hecho, los sistemas operativos se han convertido en el centro de una guerra invisible entre Hackers, fabricantes y administradores de plataformas dado que la importancia de su papel es un punto indispensable en el funcionamiento y publicación de cualquier aplicación.

Lo que hace necesario que cualquier modelo de gestión de incidentes, inequívocamente contemple aquellas vulnerabilidades o debilidades existentes a nivel de sus sistemas operativos

con el fin de tener una estrategia que le permita actual ante un incidente que pueda comprometer el sistema donde corren sus servicios de forma que sean afectados lo menos posible.

La Contraloría General de la Republica en su plataforma de servidores cuenta principalmente con dos sistemas operativos en su granja de servidores:

- Linux Red Hat (en varias versiones)
- Microsoft Windows server (en sus 2 versiones más resientes)

Por lo que el análisis de vulnerabilidades se realizará basado en estos dos sistemas operativos, (Windows y Linux).

2.4.3.1. Sistema operativo Linux Red Hat.

Linux es un sistema operativo basado en UNIX y desarrollado por Linus Torvalds hacia la época de 1991 (Silberschatz, Baer Galvin, & Gagne, 2014), liberado bajo licencia GPL GNU[8] (General Public Licence GNU), lo que le permitió crecer con la ayuda de una amplia comunidad de desarrolladores y adeptos hasta convertirse en uno de los sistemas operativos más usados a nivel mundial. Linux actualmente se puede encontrar disponible en muchas distribuciones, teniendo las más comunes Red Hat, Opensuse, Ubuntu, Debian, Fedora, Etc.

Linux Red Hat conocido muchas veces como REHL, es una de las distribuciones de Linux más exitosas a nivel de servidores, gran parte debido a que no solo cuenta con una amplia comunidad de usuarios sino que igualmente se encuentra respaldado por una empresa bastante sólida encargada de brindar servicio de soporte y acompañamiento a los usuarios empresariales de esta versión, cosa que para la mayoría de las distribuciones es limitada a lo que se puede encontrar en foros y grupos de discusión.

Linux Red Hat se constituye en uno de los sistemas operativos favoritos al momento de desplegar servidores debido a sus costo reducido en comparación con competidores como Microsoft Windows (costo que puede ser relativo dado que el soporte es costoso), y más aún a su nivel de seguridad y confiabilidad, cosa difícil de conseguir para sistemas operativos de código cerrado, aunque, aun así existen vulnerabilidades en su gran mayoría atribuibles al factor

---

[8] Orientada hacia el software libre y el código abierto, que permite que cualquier usuario pueda usar, modificar y compartir libremente el software cubierto por esta licencia.

humano, y lógicamente, al igual que como ocurre con la infraestructura física y la virtualización, las que no lo son, pueden ser resueltas con la aplicación de los respectivos parches de actualización o el despliegue de nuevas versiones.

Además de los factores humanos, es lógico preguntarse ¿Por qué es necesario conocer un historial de vulnerabilidades que posiblemente ya han sido remediadas? La respuesta a esta pregunta se centra en que a pesar de que estas vulnerabilidades hayan sido remediadas o no, permitirán determinar posibles vectores de ataque, de forma tal, que se pueda actuar de manera predictiva ante cualquier amenaza futura, permitiendo tener un modelo de gestión de incidentes proactivo.

Entre las vulnerabilidades más comunes y de mayor impacto que pueden impactar esta distribución de Linux el MITRE nos describe las siguientes:

- CVE-2018-1083: Un usuario sin privilegios gracias a esta vulnerabilidad podría escalar de privilegios insertando código en una ruta de directorio creada especialmente para ello, el escalamiento ocurriría cuando un usuario con privilegios utilice la opción de autocompletar en la ruta de directorio creada ocasionando una situación de buffer overflow. (MITRE Corporation, 2018).
- CVE-2017-1000376: Un atacante podría ejecutar código arbitrario mediante el uso de la librería libffi, para ejecutar una pila que contenga este código peligroso. (MITRE Corporation, 2018).
- CVE-2017-15134: Una falla en el kernel con versión anterior a la 4.13.12 podría ocasionar una condición de denegación de servicio. (MITRE Corporation, 2018).
- CVE-2017-15116: un atacante podría causar denegación de servicio en versiones de Linux con kernel anterior a la versión 4.2 mediante el uso de la función rngapi_reset function ubicada en crypto/rng.c. (MITRE Corporation, 2018).
- CVE-2017-12197: Un usuario con una contraseña de una cuenta inactiva, podría saltarse restricciones de seguridad y acceder a información sensible. (MITRE Corporation, 2018).
- CVE-2016-4448: Una vulnerabilidad en la librería libxml2 anterior a la versión 2.9.4 permitiría a un atacante tener un impacto no determinado. (MITRE Corporation, 2018).

Modelo de Gestión de incidentes de seguridad CGR.

- CVE-2016-4123: Una vulnerabilidad en Adobe Flash player versión 21.0.0.242 o anterior podría presentar un impacto y un vector de ataque desconocido, lo que la hace muy peligrosa. (MITRE Corporation, 2018).
- CVE-2016-3471: Una vulnerabilidad en My SQL con versiones anteriores a 5.5.45 le permitirían a un usuario afectar la confidencialidad disponibilidad e integridad de la información. (MITRE Corporation, 2018).

En resumen hasta la fecha el MITRE reporta que Linux Red Hat ha tenido alrededor 453 vulnerabilidades descubiertas, de las cuales 16 se han descubierto en lo corrido del año 2018, perteneciendo en su gran mayoría a denegaciones de servicio (DoS) y ejecución de código como se puede observar en la Figura 30.

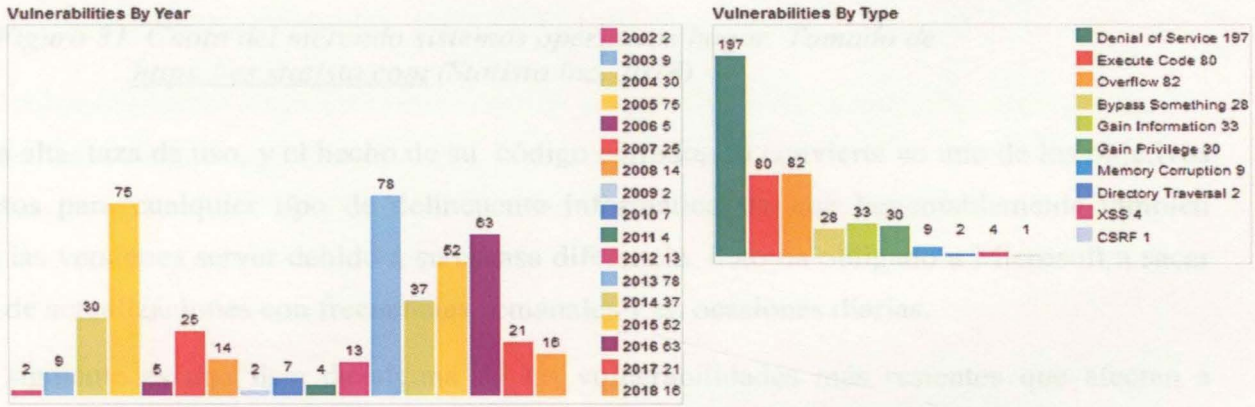

Figura 30. Mapa de vulnerabilidades Linux Red Hat Enterprise. Tomado de www.cvedetails.com. (MITRE Corporation, 2018).

2.4.3.2. Sistema operativo Microsoft Windows server

El sistema operativo Windows server en sus versiones server 2008 R2, server 2012 R2 y server 2016 (Rolandi, 2016), al igual que el Linux Red Hat se constituye en un sistema operativo bastante utilizado a nivel de la plataforma de servidores de la CGR, razón por la cual es necesario conocer algunas de sus vulnerabilidades más recientes y comunes con el fin de que el modelo de gestión de incidentes en desarrollo pueda quedar lo más ajustado posible a la realidad de la entidad. De hecho los sistemas operativos Microsoft en sus versiones para el hogar, son los más utilizados a nivel global como lo muestra la Figura 31, contando con una cuota mundial que rondaba alrededor del 88,5% para 2017 (Statista.inc, 2018).

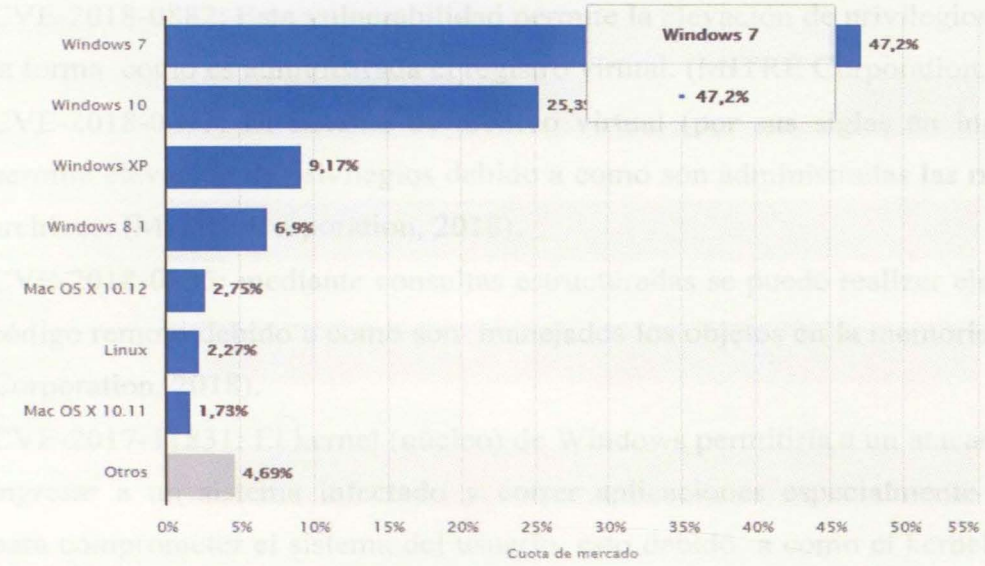

Figura 31. Cuota del mercado sistemas operativos hogar. Tomado de https://es.statista.com (Statista.inc, 2018)

Esta alta taza de uso, y el hecho de su código cerrado, lo convierte en uno de los objetivos predilectos para cualquier tipo de delincuente informático, lo que lamentablemente también afecta a las versiones server debido a su escasa diferencia. Esto ha obligado a Microsoft a sacar parches de actualizaciones con frecuencias semanales y en ocasiones diarias.

La siguiente es una lista de alguna de las vulnerabilidades más resientes que afectan a Windows server en todas sus versiones no actualizadas y reportadas por el MITRE:

- CVE-2018-0886: Afecta prácticamente a todas las versiones sin parches actualizados, permite la ejecución de código remoto debido a como el protocolo del proveedor de servicios de seguridad de credenciales (CredSSP) valida las solicitudes durante el proceso de autenticación. (MITRE Corporation, 2018).
- CVE-2018-0884: Esta vulnerabilidad en el Windows Scripting Host (WSH) Permite saltarse las características de seguridad a nivel de Windows server. (MITRE Corporation, 2018).
- CVE-2018-0883: El Shell de Windows de algunas versiones de Windows server permite la ejecución de código remoto debido a como se validan los destinos en la copia de archivos. (MITRE Corporation, 2018).

- CVE-2018-0882: Esta vulnerabilidad permite la elevación de privilegios debido a la forma como es administrada el registro virtual. (MITRE Corporation, 2018).
- CVE-2018-0877: El sistema de archivo virtual (por sus siglas en ingles VFS) permite elevación de privilegios debido a como son administradas las rutas de los archivos. (MITRE Corporation, 2018).
- CVE-2018-0825: mediante consultas estructuradas se puede realizar ejecución de código remoto debido a como son manejados los objetos en la memoria. (MITRE Corporation, 2018).
- CVE-2017-11831: El kernel (núcleo) de Windows permitiría a un atacante remoto ingresar a un sistema infectado y correr aplicaciones especialmente diseñadas para comprometer el sistema del usuario, esto debido a como el kernel inicializa la memoria del equipo. (MITRE Corporation, 2018).

Las vulnerabilidades expuestas anteriormente corresponden a una pequeña parte de todas las reportadas en la plataforma del MITRE, las cuales suman un total de 36 desde el 2009, perteneciendo 25 de estas al año 2018. Posiblemente muchas de las vulnerabilidades que se descubren día a día para versiones del hogar, podrían afectar también a los servidores. La Figura 32 resume la información reportada por el MITRE para estos servidores.

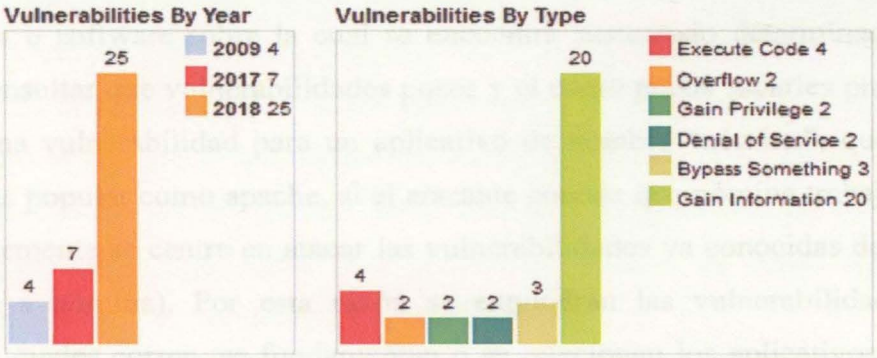

Figura 32. Mapa de vulnerabilidades para windows server. Tomado de www.cvedetails.com. (MITRE Corporation, 2018).

2.4.4. Capa aplicación.

La capa de aplicaciones hace referencia a los servicios que corren sobre cada uno de los servidores de la entidad, entre los cuales tenemos:

Modelo de Gestión de incidentes de seguridad CGR.

- Página web CGR
- Sitio de denuncias
- Boletín de responsables fiscales.
- Intranet.
- Directorio activo.
- Gestión Documental
- Nomina
- Inventario
- Sistema de aseguramiento electrónico
- Bases de datos Oracle y SQL

Si bien cada uno de estos servicios posee vulnerabilidades relacionadas con los distintos factores humanos que intervinieron en el momento de su desarrollo e implementación, estas vulnerabilidades no siempre son tan explotadas como aquellas que ya de antemano son conocidas por los atacantes, las mismas que generalmente vienen inmersas entre las distintas herramientas de desarrollo, producción o acceso a los servicios prestados, dentro de las cuales destacan las ya conocidas vulnerabilidades de día cero y aquellas vulnerabilidades que simplemente no han sido remediadas mediante los parches de actualización correspondientes. Estas vulnerabilidades representan un peligro latente dado que los atacantes solo necesitan conocer la herramienta o software sobre la cual se encuentra sustentado determinado servicio para posteriormente consultar que vulnerabilidades posee y el como puede sacarles provecho (no es lo mismo buscar una vulnerabilidad para un aplicativo de nombre "nómina", que para una herramienta de uso más popular como apache, si el atacante conoce que nómina trabaja sobre un servidor apache posiblemente se centre en atacar las vulnerabilidades ya conocidas del apache y así obtener el acceso a nómina). Por esta razón se expondrán las vulnerabilidades de las herramientas sobre las cuales corren, se fundamentan o se relacionan los aplicativos, dado que las mismas corresponden a casos generales que afectan la particularidad de cada uno de estos.

La Tabla 11 contiene el listado de algunas vulnerabilidades reportadas por el MITRE que en caso de no tenerse parchadas las herramientas podría tener efecto sobre los distintos aplicativos en la CGR:

Tabla 11
Vulnerabilidades a nivel de aplicaciones.

VULNERABILIDADES	DoS	Ejecución de código	Escalamiento de privilegios	XSS	Inyección de código SQL	Buffer overflow	Acceso a información no autorizada
Directorio activo	2	0	0	0	0	0	0
Servidor web apache	77	24	14	21	0	19	14
TomCat	28	6	7	22	0	5	32
Glassfish	8	2	0	3	0	2	4
Liferay	0	2	0	22	0	0	2
Java	32	15	1	1	0	5	7
Base de datos SQL	21	44	12	4	2	28	4
Base de datos Oracle	14	34	7	6	45	31	10

Nota. Tomado de MITRE Corporation. https://www.cvedetails.com/

2.4.5. Identificación del riesgo.

De acuerdo a las amenazas y el historial de vulnerabilidades reportadas por el MITRE (de las cuales solo un poco porcentaje se ha expuesto), es posible determinar en una manera aproximada aquellos riesgos a los que se encuentra expuesta la infraestructura informática de la contraloría General de la República, los cuales presentan un alto nivel de impacto si la entidad no cuenta con un plan de mejores prácticas que garanticen además de la aplicación de los parches de seguridad publicados por los fabricantes de los distintos componentes, un adecuado plan de capacitación y actualización tecnológica para el recurso humano de forma que sea posible garantizar una gestión del riesgo adecuada a las necesidades.

Con base en los reportes de vulnerabilidades obtenidos del Mitre es posibles determinar cuáles son los tipos de vulnerabilidades más frecuentes a nivel de cada una de las capas como lo muestra la Tabla 12 a continuación:

Tabla 12
Tipo de Vulnerabilidades más frecuentes.

	DoS	**Ejecución de código**	**Escalamiento de privilegios**	**XSS**	**Inyección de código SQL**	**Buffer overflow**	**Acceso a información no autorizada**
Capa Física	Alta	Alta	Media	Alta	Baja	Media	Media
Capa de Virtualización	Alta	Alta	Alta	Media	Baja	Media	Bajo
Capa de sistema operativo	Alta	Alta	Alta	Baja	Baja	Alta	Media
Capa de aplicación	Alta	Alta	Media	Alta	Alta	Alta	Alta

Nota. Elaboración propia.

La Tabla 13 representa los riesgos asociados a cada una de las amenazas identificadas.

Tabla 13
Identificación de riesgo.

AMENAZA / RIESGOS ASOCIADOS	**DoS**	**Ejecución de código**	**Escalamiento de privilegios**	**XSS**	**Inyección de código SQL**	**Buffer overflow**	**Acceso a información no autorizada**
Servicios fuera de línea	X	X	X	---	X	X	___
Lentitud en el acceso a los servicios	X	---	---	X	X	X	___
Bloqueo del sistema operativo	X	X	X	---	X	X	___
Perdida de información	---	X	X	X	X	---	X
Robo de información	---	X	X	X	X	X	X

clasificada									
Pedida de control en la información publicada	---	X	X	X	X	X	___		
Alteración de la información.	---	X	X	X	X	X	___		
Daño físico del equipo	---	X	-----	---	___	___	___		
Pérdida de administración	---	X	X	---	___	___	___		
Pérdida de Control del sistema operativo	---	X	X	---	___	___	___		

X: El riesgo se asocia con la amenaza.

---: El riesgo no está asociado con la amenaza.

Nota. Elaboración propia

Y la Tabla 14 refleja el impacto causado a las aplicaciones si estos riesgos llegaran a materializarse en un posterior incidente:

Tabla 14

Impacto de los incidentes en los aplicativos de la CGR.

Incidente / Aplicativo	**Servicios fuera de línea**	**Lentitud en el acceso a los servicios**	**Bloqueo del sistema operativo**	**Perdida de información**	**Robo de información clasificada**	**Pedida de control en la información publicada**	**Alteración de la información.**	**Daño físico del equipo**	**Pérdida de administración**	**Pérdida de Control del sistema operativo**
Página web CGR	Alto	Medio	Alto	Bajo	Medio	Alto	Alto	Alto	Alto	Alto
Sitio de denuncias	Alto	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
Boletín de responsables	Alto	Medio	Alto	Bajo	Alto	Alto	Alto	Alto	Alto	Alto

Fiscales										
Intranet	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Medio	Alto	Alto
Directorio activo	Alto	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
Gestión documental	Alto	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Medio	Alto
Nómina	Alto	Medio	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
Inventario	Medio	Medio	Medio	Alto	Alto	Alto	Alto	Medio	Alto	Alto
Sistema de aseguramiento electrónico	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
Base de datos	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto

Nota. Elaboración propia.

De acuerdo a la Tabla 14, es claro que cualquier incidente podría llegar a tener un alto grado de afectación sobre los aplicativos, lo que se traduciría en un impacto directo sobre el negocio, impacto que se puede apreciar en la Tabla 15.

Tabla 15
Impacto de los incidentes en el negocio.

Incidente	**Nivel de impacto**
Servicios fuera de línea	Alto
Lentitud en el acceso a los servicios	Media
Bloqueo del sistema operativo	Alto
Perdida de información	Alto
Robo de información clasificada	Alto
Pedida de control en la información publicada	Alto
Alteración de la información.	Alto
Daño físico del equipo	Alto
Pérdida de administración	Alto

Pérdida de Control del sistema operativo	Alto

Nota. Elaboración propia.

En resumen: Desde el punto de vista del riesgo, la adopción de un modelo de gestión de incidentes de seguridad en la entidad es una necesidad que puede considerarse prioritaria debido a la severidad del impacto que podría causar la ocurrencia de un incidente, por lo que la misma debe de estar no solo vigilante ante las amenazas existentes alrededor de su infraestructura, sino igualmente preparada ante cualquier incidente que pueda presentarse con el fin de sufrir la menor afectación posible.

2.5. Análisis de Impacto Sobre el Negocio BIA

El siguiente análisis tiene como base el análisis de impacto sobre el negocio realizado bajo el desarrollo del DRP (Contraloría General de la República, 2018), por lo que solo se utilizará información relevante con base en los fallos a nivel de la infraestructura de servidores. La finalidad del análisis es visibilizar la importancia de la infraestructura de servidores para la CGR y el consecuente efecto que podría producirse en caso de la falla de los servicios asociados, los cuales tienen efectos directos sobre los macroprocesos de la entidad.

El alcance del análisis se limita a las aplicaciones que se consideran más importantes para el negocio y su relación con los procesos de la entidad.

2.5.1. Criticidad de las aplicaciones.

La información de la criticidad de las aplicaciones en la Tabla 16 se determinó mediante la consulta directa a las personas y oficinas relacionadas con el proceso, al igual que mediante el análisis de la relación de los aplicativos con los objetivos institucionales, y la información tomada del plan de recuperación de desastres de la entidad.

Para la elaboración de la tabla se consideraron los siguientes Criterios para indicar la criticidad:

- **Alta:** El proceso se detiene o se interrumpe totalmente.

Modelo de Gestión de incidentes de seguridad CGR.

- **Media:** El proceso se ve afectado pero continua en operación o puede ser recuperado fácilmente.
- **Baja:** No afecta el proceso.

Tabla 16
Criticidad aplicaciones.

Aplicación	Proceso	Criticidad
SIRECI	Proceso Auditor	Alta
SIREF	Etapa pre-procesal, Etapa Procesal y Jurisdicción Coactiva	Alta
SIPAR	Desarrollar en el Control Fiscal Participativo	Alta
SIGEDOC	Gerenciar Talento Humano, Desarrollar el Control Fiscal Participativo, Etapa Procesal, jurisdicción coactiva, Proceso auditor y otros no identificados como críticos.	Alta
SIBOR	Etapa Procesal, Jurisdicción coactiva	Alta
KACTUS	Gerenciar el Talento Humano	Alta
PORTAL	Comunicar y Divulgar externamente	Alta
INTRANET	Todos	Media
INVENTARIOS	Administrar recursos fisicos	Media
SAE	Proceso Auditor, Etapa pre-procesal, Etapa Procesal y Jurisdicción Coactiva	Alta
DEUDA PÚBLICA	Evaluación de las finanzas públicas, Evaluación de políticas públicas, Estrategia y gobierno de ti	Media
PRORROGAS	Proceso Auditor	Baja

Nota. Tomado de DRP Contraloría General

2.5.2. Metodología de medición.

Para la medición del impacto si bien la contraloría general cuenta con una metodología de riesgos, se optó por utilizar una metodología propia lo más ajustada posible a la realidad y al

sujeto hacia el cual va dirigido el desarrollo del modelo, esto sin dejar de lado los lineamientos establecidos por la entidad. Los siguientes son los criterios sobre los cuales se fundamenta en análisis:

- Impacto a la ciudadanía.
- Impacto operativo.
- Impacto económico.

El levantamiento de información se realizó mediante entrevistas a los administradores de aplicaciones y algunos funcionarios seleccionados de forma puntual, dado que ellos cuentan con el mayor conocimiento de la aplicación y el cómo puede afectar al negocio un incidente de seguridad. En total se encuestaron 21 funcionarios, para lo que se utilizó el modelo de encuesta ilustrado en la Figura 48 en el apéndice A. El resultado de la misma se encuentra reflejado en el presente análisis.

2.5.2.1.Impacto a la ciudadanía.

Como entidad pública y de control, es necesario conocer el impacto sufrido directamente sobre la ciudadanía en caso de una falla parcial o total de la infraestructura, esto debido a que la misma se vería bastante afectada dado que además de quedar imposibilitados para radicar las respectivas denuncias relacionadas con su labor de fiscalizadores de lo público, tampoco podrían acceder a los distintos certificados que brinda la plataforma y que son útiles para cuando se desea conseguir un trabajo y obtener una visa. Es de notar que la página web de la CGR es un sitio bastante visitado; tan solo las estadísticas de la entidad indican alrededor de 10.000 visitas diarias al mismo.

El impacto se estima de acuerdo a la escala de la Tabla 17.

Tabla 17
Escala de impacto para la ciudadanía

Impacto sobre la ciudadanía	
Escala	**Descripción**
Catastrófico	Impacta totalmente la ciudadanía afectando procesos externos, la imagen de la entidad y/o otras entidades.

Mayor	Afectación de manera considerable la ciudadanía.
Moderado	Se afecta de forma moderada la ciudadanía.
Menor	Hay una afectación mínima a la ciudadanía.
Insignificante	No afecta a la ciudadanía.

Nota. Elaboración propia.

2.5.2.2.Impacto operativo.

Mide el impacto operativo de la entidad en caso de un incidente de seguridad que afecte la operatividad del negocio, considerándose la demora en los procesos, interrupciones momentáneas, perdidas de información y la falla completa de la infraestructura de acuerdo a la Tabla 18.

Tabla 18
Escala de impacto operativo.

Impacto sobre la operatividad	
Escala	**Descripción**
Catastrófico	Pérdida de información sensible de gran importancia, interrupción completa de procesos.
Mayor	Pérdida de información de importancia media-alta, afectación a procesos misionales.
Moderado	Pérdida de información de importancia media-alta. Lentitud tolerable en las aplicaciones, perdida de operatividad de procesos no misionales.
Menor	Bajo grado de afectación a los procesos perdida de información de importancia media, retrasos en procesos. Perdida de operatividad de procesos no misionales
Insignificante	No afecta a la operatividad, perdida de información de importancia baja

Nota. Elaboración propia.

2.5.2.3.Impacto económico.

Si bien el tema económico no tiene mucha relevancia en la entidad si se hace necesario contar con una aproximación económica en términos del impacto al negocio, la aproximación se realizará con base en la ejecución presupuestal de la contraloría general para el año 2017 con un total aproximado de $566.008.870.471,36[9]. Teniendo en cuenta un horario laboral de 5x8 y un periodo laboral de 243 días, el costo por hora de funcionamiento correspondería a $291.156.826. De esta forma se tiene la Tabla *19*.

Tabla 19
Escala de impacto económico.

Impacto económico	
Escala	**Descripción**
Catastrófico	Costos superiores a $ 2.329.254.608
Mayor	Costo inferior al valor de un día. $ 2.329.254.608
Moderado	Costo inferior al 100% del valor de una hora. $ 291.156.826
Menor	Costo inferior al 25% del valor de una hora. $ 72.789.207
Insignificante	Costo inferior al 10% del valor de una hora. $ 29.115.683

Nota. Elaboración propia.

2.5.2.4.Ponderaciones relativas a los impactos.

Debido a que no todos los tipos de impacto tienen el mismo peso para la entidad, se definieron estos en la Tabla 20.

Tabla 20
Ponderación impactos.

Impacto	Peso
Impacto a la ciudadanía	35%
Impacto operativo	40%

[9] Según reporte de ejecución presupuestal 2017 de la CGR. https://www.contraloria.gov.co /contraloria/planeacion -gestion-y-control/ gestion-presupuestal/presupuesto.

Impacto económico	25%

Nota. Elaboración propia.

2.5.2.5.Definición de términos.

- RPO: Punto objetivo de recuperación, punto en el cual la información debe de ser restaurada con el fin de permitir la reanudación de la operación.
- MAO: Tiempo máximo de interrupción soportable por el aplicativo o servicio.
- SDO: Objetivo de entrega de servicio, nivel mínimo de operación tecnológica aceptable por la entidad de forma que permita lograr sus objetivos durante la interrupción.
- RTO: Tiempo objetivo de recuperación requerido por cada una de las aplicaciones de acuerdo a su criticidad.

2.5.2.6.Escala de tiempo.

Para las valoraciones define la escala de tiempo de la Tabla 21 con base en el tiempo mínimo de 4 horas en el cual se considera ya un impacto importante sobre las operaciones del negocio y un tiempo máximo de 5 días hábiles donde los funcionarios consultados consideran que se generaría un impacto bastante fuerte sobre la entidad llegando a afectar completamente los procesos.

Tabla 21
Escala de tiempo.

TIEMPO					
0-4 horas	4-8 horas	8-24 horas	1 - 3 días	3 - 5 días	Más de 5 días

Nota. Elaboración propia.

2.5.3. Impacto a la ciudadanía.

La falla o afectación de los aplicativos contenidos en la Tabla 22 tendría impacto sobre la ciudadanía.

Tabla 22
Aplicativos que tienen impacto directo sobre la ciudadanía.

Nombre	**Descripción**
SIRECI	Sistema de rendición de Electrónica de la Cuenta e Informes. Que permite a los sujetos de control y entidades del estado presentar su rendición de cuentas e informes a la entidad.
SIREF	Sistema de información de responsabilidad fiscal. Proporciona un registro de todas las actuaciones relacionadas con la responsabilidad fiscal.
SIPAR	Sistema de información de participación ciudadana. Lleva un registro de las diferentes mecanismos de participación ciudadana, como las quejas, denuncias, solicitudes, etc.
SIBOR	Boletín de responsables fiscales. Expedición de certificados.
PORTAL	Portal institucional.
DEUDA PÚBLICA	Registro de la deuda pública estatal.
PRORROGAS	Gestión de prórrogas en el sistema de rendición de cuentas.
SAE	Sistema de aseguramiento electrónico de expedientes.

Nota. Elaboración propia.

Por consiguiente la Tabla 23 muestra el nivel de impacto a la ciudadanía producido por la indisponibilidad en cada uno de los aplicativos o servicios relacionados.

Tabla 23
Impacto a la ciudadanía.

Aplicativo, Servicio	**Macroproceso**	**Proceso**	**Impacto**					
			0-4 horas	4-8 horas	8-24 horas	1-3 días	3-5 días	Más de 5 días
Portal	Comunicación y Divulgación – CYD	Comunicar y divulgar externamente.	Mayor	mayor	Catastrófico	Catastrófico	Catastrófico	Catastrófico

SIBOR	Enlace con Cliente y Partes Interesadas – ECP.	.- Brindar apoyo técnico al congreso de la república. - Desarrollar el control fiscal participativo.	Moderado	Mayor	Mayor	Catastrófico	Catastrófico	Catastrófico
SIRECI	Control Fiscal Micro – CMI. Control Fiscal Macro – CMA	- Proceso auditor. -Actuaciones especiales de fiscalización. -Proceso administrativo sancionatorio. •Evaluación de finanzas públicas. •Evaluación de calidad y eficiencia del control fiscal interno para las entidades y organismos del estado.	Moderado	Mayor	Mayor	Catastrófico	Catastrófico	Catastrófico
SIPAR	Enlace con Cliente y Partes Interesadas – ECP	•Desarrollar el control fiscal participativo.	Menor	Moderado	Moderado	Mayor	Catastrófico	Catastrófico
SIREF	Responsabilidad Fiscal y Jurisdicción Coactiva – RFJ	• Etapa procesal. •Jurisdicción coactiva.	Insignificante	Menor	Menor	Moderado	Mayor	Catastrófico

Deuda pública	Control Fiscal Macro – CMA	Evaluación de finanzas públicas.	Insignificante	Insignificante	Insignificante	Menor	Menor	Moderado
SAE	Control Fiscal Micro – CMI.	•Proceso administrativo sancionatorio.	Insignificante	Menor	Menor	Moderado	Mayor	Mayor
	Control Fiscal Macro – CMA	• Proceso auditor.						
	Responsabilidad Fiscal y Jurisdicción	• Etapa procesal.						
		• Etapa preprocesal.						
	Coactiva – RFJ	•Jurisdicción coactiva.						

Nota. Elaboración propia.

2.5.4. Impacto operativo.

Los aplicativos de la Tabla 24 pueden impactar la operatividad del negocio de forma directa.

Tabla 24
Aplicativos que impactan la entidad a nivel operativo.

Nombre	**Descripción**
SIRECI	Sistema de rendición de Electrónica de la Cuenta e Informes. Que permite a los sujetos de control y entidades del estado presentar su rendición de cuentas e informes a la entidad.
SIREF	Sistema de información de responsabilidad fiscal. Proporciona un registro de todas las actuaciones relacionadas con la responsabilidad fiscal.
SIPAR	Sistema de información de participación ciudadana. Lleva un registro de los diferentes mecanismos de participación ciudadana, como las quejas, denuncias, solicitudes, etc. Su impacto a largo plazo dejaría sin insumos a la entidad y a los procesos que dependen de este aplicativo.
DEUDA PÚBLICA	Registro de la deuda pública estatal. Su impacto a largo plazo restaría competencias a la entidad para el desarrollo de sus investigaciones.

PRORROGAS	Gestión de prórrogas en el sistema de rendición de cuentas.
SAE	Sistema de aseguramiento electrónico de expedientes.
KACTUS	Administración de la nómina. Su impacto a largo plazo podría significar el cese de operaciones por parte de funcionarios y contratistas.
SIGEDOC	Sistema de gestión documental necesario para los procesos internos y externos de la entidad, su afectación genera pérdida de productividad al ocasionar represamientos de trámites y mensajería.
INTRANET	Portal interno de la entidad, mediante este los funcionarios se mantienen informados y acceden a los distintos aplicativos o aplicaciones.

Nota. Elaboración propia.

La Tabla 25 muestra el nivel de impacto a la operatividad de la entidad producido por la indisponibilidad en cada uno de los aplicativos o servicios relacionados.

Tabla 25
Impacto operativo.

Aplicativo, Servicio	**Macroproceso**	**Proceso**	**Impacto**					
			0-4 horas	4-8 horas	8-24 horas	1-3 días	3-5 días	Más de 5 días
SIRECI	Control Fiscal Micro – CMI. Control Fiscal Macro – CMA	- Proceso auditor. -Actuaciones especiales de fiscalización. -Proceso administrativo sancionatorio. •Evaluación de finanzas públicas. •Evaluación de calidad y eficiencia	Menor	Moderado	Mayor	Mayor	Mayor	Catastrófico

		del control fiscal interno para las entidades y organismos del estado.							
SIPAR	Enlace con Cliente y Partes Interesadas – ECP	•Desarrollar el control fiscal participativo.	Insignificante	Menor	Menor	Moderado	Mayor	Catastrófico	
SIREF	Responsabilidad Fiscal y Jurisdicción Coactiva – RFJ	• Etapa procesal. •Jurisdicción coactiva.	Insignificante	Menor	Menor	Moderado	Mayor	Catastrófico	
Deuda pública	Control Fiscal Macro – CMA	Evaluación de finanzas públicas.	Insignificante	Insignificante	Insignificante	Menor	Menor	Moderado	
SAE	Control Fiscal Micro – CMI. Control Fiscal Macro – CMA Responsabilidad Fiscal y Jurisdicción Coactiva – RFJ	•Proceso administrativo sancionatorio. • Proceso auditor. • Etapa procesal. • Etapa preprocesal. •Jurisdicción coactiva.	Insignificante	Menor	Menor	Mayor	Mayor	Catastrófico	
Kactus	Gestión del Talento Humano GTH	Gerenciar Talento Humano.	Insignificante	Insignificante	Insignificante	Menor	Mayor	Mayor	

SIGEDOC	Gestión del Talento Humano - GTH. Control Fiscal Micro – CMI. Control Fiscal Macro – CMA Responsabilidad Fiscal y Jurisdicción Coactiva – RFJ	Gerenciar talento humano. Desarrollar el control fiscal participativo. Etapa procesal. Jurisdicción coactiva. Proceso auditor	Moderado	Mayor	Mayor	Crítico	Crítico	Crítico
Intranet	Gestión del Talento Humano - GTH. Control Fiscal Micro – CMI. Control Fiscal Macro – CMA	Gerenciar talento humano. Desarrollar el control fiscal participativo.	Insignificante	Menor	Menor	Moderado	Moderado	Mayor

Nota. Elaboración propia

2.5.5. Impacto económico.

Los aplicativos listados en la Tabla 26 producen un impacto económico directo:

Tabla 26

Aplicativos que impactan la entidad económicamente.

Nombre	Descripción
KACTUS	Apalanca el proceso institucional de gerenciar talento humano a través de la administración de la nómina. Su costo en caso de un incidente estaría asociado a penalizaciones por no pagos o pagos tardíos a los funcionarios.
INVENTARIO	Apalanca los procesos administración de recursos físicos y administración de recursos informáticos pertenecientes al macroproceso gestión de los recursos de la entidad, se encarga de registrar los recursos físicos e informáticos que tienen la entidad, por lo que una

	afectación a este proceso podría causar pérdida de equipos, represamiento de recursos y ceses en los procesos de adquisiciones en la entidad.

Nota. Elaboración propia

El correspondiente nivel de impacto se visualiza en la Tabla 27.

Tabla 27
Impacto económico.

Aplicativo, Servicio	**Macroproceso**	**Proceso**	**Impacto**					
			0-4 horas	4-8 horas	8-24 horas	1-3 días	3-5 días	Más de 5 días
Kactus	Gestión del Talento Humano GTH	Gerenciar Talento Humano.	Insignificante	Menor	Menor	Moderado	Mayor	Catastrófico
Inventario	Gestión de los recursos de la entidad GRE	Administración de recursos físicos. Administración de recursos informáticos	Insignificante	Insignificante	Insignificante	Menor	Menor	Moderado

Nota. Elaboración propia.

2.5.6. Tiempo de recuperación de aplicaciones.

Los tiempos límites para la recuperación en caso de desastres para las aplicaciones, se encuentran definidos con base en el plan de copias de seguridad de la entidad, la criticidad de las aplicaciones y su nivel de impacto. El plan de recuperación de desastres de la entidad define de acuerdo a la Tabla 28 los objetivos de tiempo de recuperación (RTO), punto objetivo de recuperación (RPO) y periodo máximo tolerable de interrupción (MTPD) para las aplicaciones más críticas.

Tabla 28
Tiempos de recuperación aplicaciones.

APLICACIONES CRÍTICAS	RTO	RPO	MTPD
PORTAL	4 - 8 horas	2 días	2 días
SIBOR	4 - 8 horas	1 día	1 día
SIPAR	4 – 8 horas	1 día	1 día
SIGEDOC	1 – 2 días	1 día	2 días
SAE	1 – 2 días	1 día	5 días
SIREF	1 – 2 días	1 día	5 días
KACTUS	1 – 2 días	1 día	5 días
SIRECI	1 – 2 días	1 día	5 días

Nota. Adaptado de DRP Contraloría General de la república.

2.5.7. Tiempo de recuperación infraestructura.

Para el caso de fallas en la infraestructura tecnológica que soporta los servidores estos tiempos estarán marcados por los contratos de soporte vigente, al igual que por las aplicaciones que estos alojan, teniéndose los siguientes:

- Tiempo de respuesta máximo para infraestructura física de servidores y almacenamiento: 4 horas, con un día de solución.
- Tiempo de respuesta máximo para virtualización: 4 horas, con 8 horas de solución.

Por consiguiente se tiene la Tabla 29:

Tabla 29
Tiempos de recuperación infraestructura.

INFRAESTRUCTURA	RTO	RPO	MTPD
Servidores	4 - 8 horas	1 días	1 día
Almacenamiento	4 - 8 horas	1 día	1 día
Virtualización	4 – 8 horas	1 día	1 día

Nota. Elaboración propia.

En síntesis se tiene que para el caso de un desastre que ocurra sobre la infraestructura de servidores y almacenamiento y que impacte los servicios prestados por la entidad, la recuperación de la misma por ningún motivo debe superar un día puesto que esto podría afectar catastróficamente el negocio de la entidad.

3. Capítulo Tres – Planteamiento del Modelo: Procedimiento para la Atención de Incidentes. Definición de Recursos y Herramientas

Una vez identificadas las necesidades específicas del negocio respecto a la seguridad de la información y su infraestructura de servidores se hace necesario definir los procesos que permitirán poner en marcha el modelo, definiendo los respectivos procedimientos a ejecutar, equipos de respuesta y herramientas necesarias como formatos, escáneres de red y firewall que permitan la gestión del incidentes efectiva con la menor afectación posible.

3.1. Equipo de Respuesta a Incidentes de Seguridad CSIRT

El equipo de respuesta a incidentes CSIRT (Computer Security Incident Response Team) es el encargado de reaccionar ante cualquier eventualidad que pueda ocasionarse dentro de un incidente que afecte la infraestructura de servidores de la entidad. Como tal tiene entre sus funciones:

- Recomendar y promover políticas a la USATI en torno al uso seguro de las TICS en relación con la plataforma de servidores.
- Aplicar políticas de seguridad publicadas o recomendadas por la USATI.
- Analizar los datos del incidente.
- Calcular el impacto.
- Comunicarse con grupos de respuesta externos.
- Comunicar las respectivas alertas a la OSEI y USATI.
- Tomar o indicar las medidas necesarias para reducir el impacto del incidente.
- Elaborar los informes respectivos.
- Proponer el plan de actualizaciones si es necesario.

Para la conformación del equipo es necesario contar con personal que cuente con acceso de primera mano a los equipos y aplicativos y que además permitan comunicar decisiones y necesidades hacia los directivos, quienes al final son los que toman las decisiones de impacto en la entidad. Dadas las vulnerabilidades y vectores de ataque analizados con anterioridad también se hace necesario contar con personal que tenga los conocimientos necesarios en el análisis de logs de sistema operativo, uso de herramientas de análisis, escáneres de red, programación,

manejo de herramienta forense, etc. Se recomienda preferiblemente hacer uso de funcionarios de la unidad de seguridad y aseguramiento tecnológico e informático USATI, u la oficina a la cual le correspondan las labores relacionadas con la seguridad de la información de la entidad. El grupo debe contar con las facilidades de comunicación necesarias para comunicarse con grupos de apoyo representados por:

- Administrador de servidores.
- Administrador de aplicaciones.
- Administrador de equipos de seguridad y antivirus.
- Administrador de equipo de redes.

La Figura 33 corresponde al organigrama recomendado para el equipo de respuesta. Se recomiendan tres grupos de analistas conformados por lo menos 2 miembros cada uno, con el fin de que los mismos puedan dar respuestas de forma eficiente y ágil a las necesidades que se generen en relación con la seguridad y actividades de capacitación y cooperación.

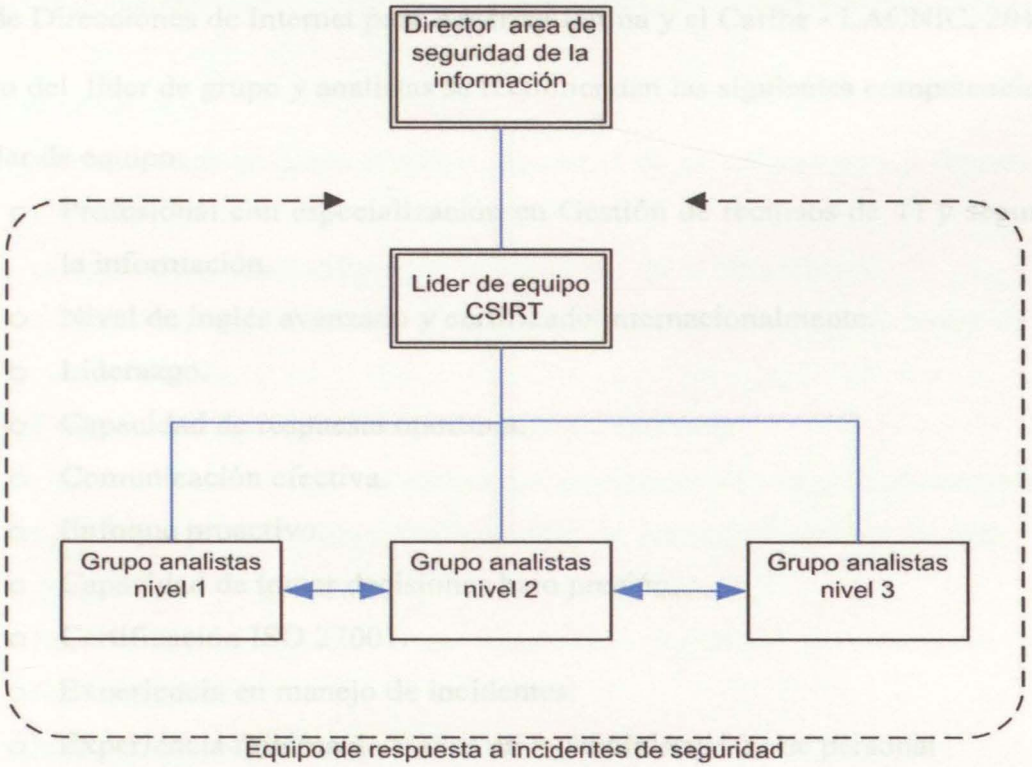

Figura 33. Equipo de respuesta a incidentes. Fuente: Elaboración propia.

Modelo de Gestión de incidentes de seguridad CGR.

3.1.1. Perfil profesional general para miembros del equipo de respuesta.

Funcionarios conexos la oficina encargada de mantener la seguridad de la información en la entidad, siendo la USATI para el caso de la contraloría general, con conocimientos en gestión de seguridad de la información y en cumplimiento con las competencias relacionadas.

Las características generales recomendadas por el Registro de Direcciones de Internet para America Latina y el Caribe LACNIC, mediante el proyecto AMPARO recomienda las siguientes habilidades para los miembros del equipo:

- Diversidad de conocimientos tecnológicos.
- Personalidad: habilidad de comunicación y relación personal.
- Personas dedicadas, innovadoras, detallistas, flexibles y metódicas.
- Experiencia en el área de seguridad de la información.
- Se maneje coherentemente con los valores personales y de la organización.
- Pueden asumir las funciones de: gerente, líder del equipo y/o supervisores.

(Registro de Direcciones de Internet para América Latina y el Caribe - LACNIC, 2011)

Para el caso del líder de grupo y analistas se recomiendan las siguientes competencias:

- Líder de equipo:
    - Profesional con especialización en Gestión de recursos de TI y seguridad de la información.
    - Nivel de inglés avanzado y certificado internacionalmente.
    - Liderazgo.
    - Capacidad de respuesta oportuna.
    - Comunicación efectiva.
    - Enfoque proactivo.
    - Capacidad de tomar decisiones bajo presión.
    - Certificación ISO 27001.
    - Experiencia en manejo de incidentes.
    - Experiencia mínima de 5 años en la administración de personal
    - Conocimiento CONPES 3854.

Modelo de Gestión de incidentes de seguridad CGR.

- Analistas nivel 1:
  - Profesionales en áreas afines a seguridad de la información o ingeniería de sistemas.
  - Conocimiento en utilización de equipos de uso en informática forense.
  - Experiencia de trabajo en ambientes virtualizados.
  - Experiencia en operación de equipos de seguridad perimetral (escáneres, firewalls, IDS).
  - Manejo, identificación y análisis de logs.
  - Capacidad para solucionar problemas.
  - Capacidad para trabajar bajo presión.
  - Conocimientos en sistemas operativos a nivel de administrador.
  - Protocolos de seguridad (IPSec).
  - Conocimiento en redes a nivel avanzado.
  - Conocimiento en criptografía.
  - Mecanismos de Seguridad (firmas digitales, certificados).

- Analistas nivel 2:
  - Profesionales en áreas afines a seguridad de la información o ingeniería de sistemas.
  - postgrado en áreas afines con la seguridad de la información.
  - Conocimiento avanzado y certificable en administración de bases de datos Oracle y SQL.
  - Experiencia superior a 3 años en trabajos similares.
  - Certificación en el uso de herramientas forenses y de seguridad perimetral.
  - Conocimiento en utilización de equipos de uso en informática forense.
  - Experiencia de trabajo en ambientes virtualizados.
  - Experiencia en operación de equipos de seguridad perimetral (escáneres, firewalls, IDS).
  - Manejo, identificación y análisis de logs.
  - Capacidad para solucionar problemas.
  - Capacidad para trabajar bajo presión.

Modelo de Gestión de incidentes de seguridad CGR.

- Conocimientos en sistemas operativos a nivel de administrador.
- Protocolos de seguridad (IPSec).
- Conocimiento en redes a nivel avanzado.
- Conocimiento en criptografía.
- Mecanismos de Seguridad (firmas digitales, certificados).

- Analistas nivel 3:
  - Profesionales en áreas afines a seguridad de la información o ingeniería de sistemas.
  - postgrado en áreas afines con la seguridad de la información.
  - Experiencia superior a 5 años en trabajos similares.
  - Conocimiento avanzado y certificable en hardware y plataformas de virtualización vmware, Hyper V y REHV.
  - Certificación en el uso de herramientas forenses y de seguridad perimetral.
  - Conocimiento en utilización de equipos de uso en informática forense.
  - Experiencia de trabajo en ambientes virtualizados.
  - Experiencia en operación de equipos de seguridad perimetral (escáneres, firewalls, IDS).
  - Manejo, identificación y análisis de logs.
  - Capacidad para solucionar problemas.
  - Capacidad para trabajar bajo presión.
  - Conocimientos en sistemas operativos a nivel de administrador.
  - Protocolos de seguridad (IPSec).
  - Conocimiento en redes a nivel avanzado (CCNP).
  - Conocimiento en criptografía.
  - Mecanismos de Seguridad (firmas digitales, certificados).

3.1.2. Escalado o asignación de incidentes de seguridad a analistas

Para el escalado o asignación de los incidentes a los grupos de analistas, se considerarán los distintos niveles de impacto contemplados en el capítulo 2, aplicándose los siguientes elementos de decisión:

Modelo de Gestión de incidentes de seguridad CGR.

3.1.2.1. Impacto sobre el negocio.

Se deberá medir el impacto sobre el negocio de acuerdo a lo establecido en el capítulo 2, los incidentes que tenga una afectación directa sobre los procesos o servicios misionales o estratégicos de la entidad, y posean un nivel de impacto bajo o medio, serán atendidos directamente por los analistas del nivel 2. Aquellos incidentes que sobrepasen nivel medio, serán atendidos por los analistas de nivel 3, debiéndose cumplir los tiempos establecidos en el capítulo 2.

Aquellos incidentes que afecten los procesos o servicios que son de apoyo o de evaluación, y posean un nivel de impacto bajo sobre los mismos, se asignarán a los analistas del nivel 1. Siendo escalados automáticamente a los analistas de nivel 2 si el nivel de impacto llegase a subir a medio, y siendo escalado a los analistas de nivel 3 si el nivel de impacto llegase a subir a alto; según lo dispuesto en el capítulo 2 en relación con la categorización del impacto sobre los distintos aplicativos.

3.1.2.2. Tiempo de duración del incidente.

Los incidentes bajo impacto, o que no tengan un impacto relevante sobre la operatividad del negocio serán asignados en principio a los analistas de nivel 1, donde se contará con un tiempo de vencimiento de los mismos, siendo este tiempo de 24 horas hábiles para el primer nivel y 8 horas hábiles para el segundo nivel. El incidente deberá de ser escalado en forma automática al siguiente nivel una vez vencidos estos tiempos, lo incidentes atendidos por los analistas de tercer nivel deben de ser resueltos en periodos que no deben superar las 4 horas hábiles.

3.1.2.3. Necesidades del servicio.

Aquellos incidentes que por necesidades del servicio sean catalogados como de alta prioridad por el personal de directivos de la entidad, serán asignados a los analistas del nivel 2 o en su defecto del nivel 3, a fin de dar solución a los mismos en tiempos no superiores a 4 horas hábiles.

3.1.3. Catálogo de servicios

La agencia de la unión europea para la seguridad de la red y la información, por sus siglas en inglés ENISA, Clasifica los servicios prestados por el CSIRT en 3 grupos a saber:

Modelo de Gestión de incidentes de seguridad CGR.

Servicios reactivos: Los que se prestan con el fin de contener un incidente ya ocurrido. Hacen parte de estos: Los reportes, El manejo del incidente, las alertas y advertencias, el manejo de las vulnerabilidades, etc. (ENISA, 2018).

Servicios Proactivos: Aquellos que se prestan con el fin de detectar y evitar futuros ataques. Clasifican dentro de estos servicios los siguientes: Anuncios, auditorías de seguridad, Desarrollo de herramientas, detección de intrusión, etc. (ENISA, 2018).

Servicios de gestión de calidad de la seguridad: Estos servicios normalmente son demandados a nivel de directivos y no tienen dependencia del tiempo. Entre estos tenemos: Análisis de riesgo, advertencias de seguridad, entrenamientos, etc. (ENISA, 2018).

Por otro lado el Foro de Respuesta a Incidentes y Equipos de Seguridad, por sus siglas en inglés FIRST, en su modelo para grupos de respuesta CSIRT, propone formar áreas de servicio clasificando los servicios de acuerdo a un aspecto que tengan en común, por lo que plantea las siguientes áreas:

- Área de servicio 1: gestión del incidente.
- Área de servicio 2: Análisis.
- Área de servicio 3: Aseguramiento de información.
- Área de servicio 4: Conciencia situacional.
- Área de servicio 5: Difusión, comunicaciones.
- Área de servicio 6: Desarrollo de capacidades.
- Área de servicio 7: Investigación y desarrollo.

  (Forum of Incident Response and Security Teams, 2018)

Si bien, ambas recomendaciones pueden ser tomadas en cuenta a la hora de presentar los servicios prestados por el CSIRT, para la propuesta de este marco se realizara una propuesta basada en las recomendaciones de ENISA, por tratarse de recomendaciones fáciles de entender e implementar, sin que lo mismo no signifique que las recomendaciones de FIRST y otros actores, no sean igual de valiosas.

Los servicios a prestar por el CSIRT son los siguientes:

3.1.3.1. Servicios reactivos:

- Alertas y advertencias de seguridad.
- Gestión de incidentes.
- Análisis del incidente.
- Calcular el impacto del incidente
- Coordinación de incidentes.
- Respuesta en sitio al incidente.
- Soporte en respuesta a incidentes.
- Manejo, análisis y mitigación de vulnerabilidades.

3.1.3.2. Servicios proactivos:

- Anuncios.
- Detección de intrusos
- Actividades de prevención y fortalecimiento de la infraestructura como la propuesta de planes de actualización.
- Configuración y mantenimiento de las herramientas de seguridad.
- Comunicar las respectivas alertas a la OSEI y USATI.

3.1.3.3.Servicios de gestión de calidad de la seguridad:

- Entrenamiento y capacitación.
- Análisis de riesgo.
- Consultoría en seguridad.
- Comunicación con otros grupos de respuesta a incidentes.

3.1.4. Comunicación con otros actores y prensa.

La comunicación con otros actores debe respetar las políticas y protocolos de la entidad emitidos principalmente por la oficina de comunicaciones en relación con la divulgación o publicación de información. Para el caso de la comunicación con otros grupos de respuesta a incidentes la misma se realizará mediante la USATI dadas sus funciones y responsabilidades en la entidad.

Modelo de Gestión de incidentes de seguridad CGR.

3.1.5. Capacitación y sensibilización.

Las actividades de capacitación y sensibilización a funcionarios y personal externo serán ejecutadas en coordinación con la oficina de capacitación de la entidad mediante la gestión realizada por el director de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático USATI o la oficina que realice las funciones correspondientes.

3.2. Ciclo de Vida del Modelo

Con base en los análisis realizados durante el desarrollo de este proyecto se plantea el ciclo de vida o de manejo del incidente contenido en la Figura 34 para el modelo de gestión de incidentes de seguridad aplicable a la infraestructura de servidores.

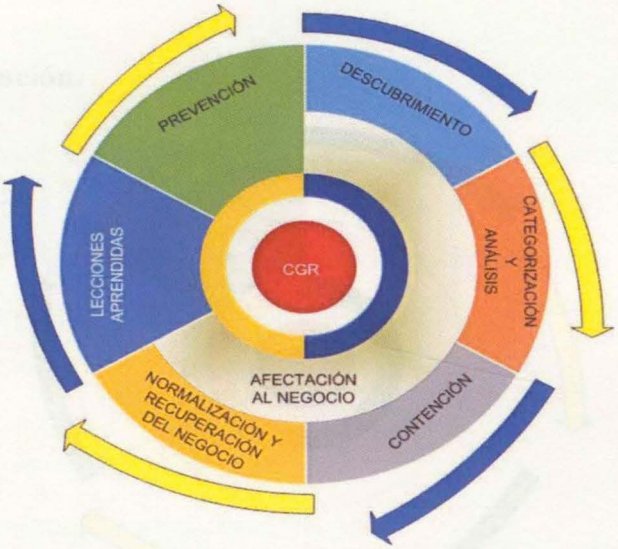

Figura 34. Ciclo de manejo del incidente del modelo CGR. Elaboración propia.

El diseño del modelo y en especial su ciclo de vida se fundamenta en la gestión del riesgo y el ciclo de mejoramiento continuo PHVA (planificar, hacer, verificar y actuar) por lo que se plantea un modelo de siete fases a saber:

1. Prevención
2. Descubrimiento
3. Categorización y análisis
4. Contención.
5. Normalización y recuperación del negocio.

Modelo de Gestión de incidentes de seguridad CGR.

6. Lecciones aprendidas
7. Afectación al negocio.

El modelo se encuentra fundamentado en la combinación de fases contenidas en el modelo NIST 800-61 y el modelo ISO 27035, siendo el modelo NIST el más utilizado por ser bastante didáctico, práctico y de mayor efectividad; mientras que el modelo ISO 27035, por ser más metódico y normalizado. Lo que permite al modelo propuesto alinearse en gran proporción con la norma ISO 27000 acogida por la entidad para el desarrollo de sus procesos institucionales.

La séptima fase corresponde a una fase transversal de afectación al negocio, con el fin de reflejar los efectos en el negocio que tiene el incidente y de esta forma priorizar y encaminar las acciones en pro de su mejoramiento.

3.2.1. Etapa de prevención.

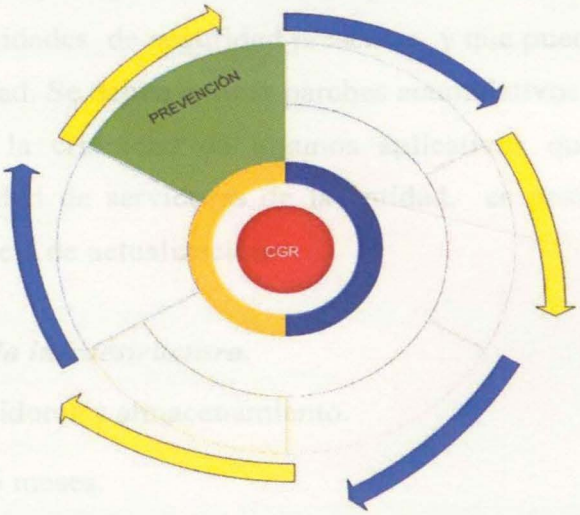

Figura 35. Etapa de prevención. Elaboración propia.

Orientada hacia la reducción del riesgo, la etapa de prevención (Figura 35) se consideraría la etapa más importante del modelo dado que de esta etapa depende mucho la ocurrencia de un incidente, es de recordar que "No hay mejor batalla que aquella que no se pelea" (Sun Tzu) por lo que cualquier incidente que se pueda evitar, termina resultando en la mejor opción. La etapa de prevención incluye las siguientes actividades:

Modelo de Gestión de incidentes de seguridad CGR.

3.2.1.1. Vigilancia tecnológica.

Responsable: USATI.

Periodicidad recomendada: Diaria.

La vigilancia tecnológica consiste en estar al tanto de las noticias y reportes a nivel de ciberataques que puedan afectar la plataforma de la entidad y con base en ello publicar políticas o recomendar a los administradores las medidas preventivas necesarias para mitigar las vulnerabilidades.

3.2.1.2. Actualización de sistemas operativos.

Responsable: Grupo de servidores y almacenamiento.

Periodicidad recomendada: 1 mes

La actualización de sistemas operativos es una tarea que se debe realizar con regularidad, con el fin de subsanar vulnerabilidades de seguridad presentes y que pueden ser un punto débil para la infraestructura de la entidad. Se deben aplicar parches acumulativos y de seguridad por lo menos una vez al mes. Dada la criticidad de algunos aplicativos que no pueden estarse reiniciando cada mes y la cantidad de servidores de la entidad, es posible que se presenten retrasos considerables la frecuencia de actualización.

3.2.1.3. Aplicación de parches a la infraestructura.

Responsable: Grupo de servidores y almacenamiento.

Periodicidad recomendada: 6 meses.

Aplicar parches de seguridad a nivel de hardware e hipervisor según las recomendaciones de los fabricantes o proveedores con el fin de subsanar vulnerabilidades en la plataforma y vigilar que los contratos de soporte y derecho a actualizaciones se mantengan vigentes.

3.2.1.4. Programación y realización de simulacros.

Responsable: USATI.

Periodicidad recomendada: anual.

Modelo de Gestión de incidentes de seguridad CGR.

En la etapa de prevención y la gestión del riesgo, es muy importante la realización de simulacros, dado que los mismos además de preparar la entidad para reaccionar en caso de un incidente, facultan a la misma para:

- Medir los distintos mecanismos de reacción.
- Automatizar y mejorar procesos.
- Conocer y fortalecer sus debilidades.
- Ubicar los fallos en el plan o modelo de gestión de incidentes revelando aquellos componentes que son críticos al momento de un evento.

Los simulacros deben incluir:

- Pruebas de recuperación de copias de seguridad.
- Pruebas de redundancia para servicios de clúster.
- Vmotion[10] tanto a nivel de almacenamiento como de host.
- Pruebas de redundancia a nivel de red.
- Pruebas de balanceo en equipos de seguridad.
- Ataques DoS controlados.
- Pruebas de penetración.

3.2.1.5.Actualización de firmware de plataforma de virtualización.

Responsable: Grupo de servidores y almacenamiento.

Periodicidad recomendada: anual.

Es necesario contar con actualizaciones de firmware mínimo una vez por año, dado que como se observó en páginas anteriores, en el año se publican decenas de vulnerabilidades que pueden afectar la plataforma.

3.2.1.6.Campañas de prevención.

Responsable: USATI

Periodicidad recomendada: anual.

---

[10] Movimiento de máquinas virtuales entre distintos host de un clúster o entre distintos volúmenes de almacenamiento.

Modelo de Gestión de incidentes de seguridad CGR.

La concientización juega un papel muy importante a nivel de prevención y la gestión del riesgo, esto debido a que un gran porcentaje ataques concluyen con éxito gracias al componente humano. Lo que hace necesario instruir a los funcionarios en políticas de ciberseguridad dentro y fuera de la entidad dado que cosas tan sencillas como recoger una memoria portátil en la calle pueden comprometer la seguridad y llegar fácilmente hasta la infraestructura de servidores.

3.2.1.7.Alistamiento de herramientas para el manejo del incidente.

Responsable: OSEI, USATI.

Es de importancia contar con las herramientas necesarias a nivel de la entidad con el fin de hacerle frente a los futuros incidentes de seguridad, para lo cual hay que disponer de por lo menos, las siguientes herramientas:

- Antivirus.
- Analizador y correlacionador de eventos.
- Firewall de red.
- Firewall de aplicaciones.
- Scanner de red.
- Sniffers de red.
- Acceso a hardware de repuesto.
- Soporte de fabricante de los distintos tipos de hardware.
- Herramientas para copias de seguridad.
- Software forense para el análisis de discos e imágenes.
- Computador portátil.
- Acceso alterno a internet.
- Software de encriptación.
- Información de contacto del equipo de incidentes.
- Analizador de logs.
- Soporte premium para los equipos hardware y software propietario.

3.2.2. Etapa de descubrimiento.

La etapa de descubrimiento (Figura 36) es una de las etapas más críticas al momento de concretarse un incidente, dado que la misma, de por si requiere que el personal a cargo de la

infraestructura, los equipos de monitoreo y las aplicaciones se encuentre atento a cualquier anormalidad en los equipos administrados. Por regla general las detecciones más tempranas siempre son las que menos daño causan, pero son las más difíciles de conseguir, dado que por lo general requiere de un trabajo mancomunado de las partes involucradas; al igual que de experiencia y de cierto grado de conocimiento acerca de lo que se desea encontrar. En la etapa de descubrimiento se debe recolectar toda la información necesaria que permita, en una posterior etapa de análisis, llegar a conclusiones que faciliten contrarrestar el ataque o la causa del incidente lo más rápido posible.

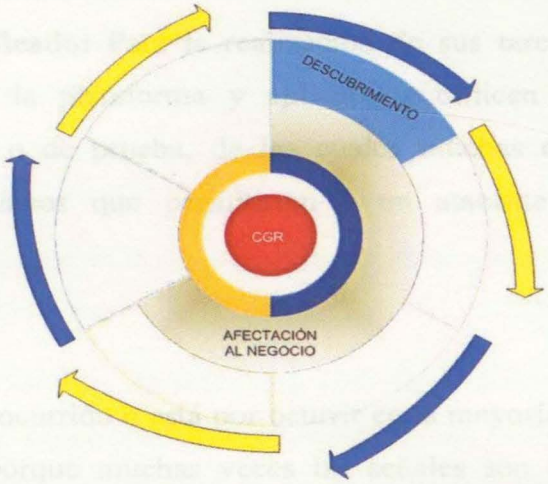

Figura 36. Estapa de descubrimiento. Elaboración propia.

3.2.2.1. Vectores de ataque.

Para el caso de servidores y almacenamiento los vectores de ataque son pocos, principalmente debido a que esta infraestructura permanece aislada de usuarios comunes, por lo que únicamente cuentan con acceso a ellos los administradores de la plataforma y de las aplicaciones.

En el ítem 4 del capítulo 2 se realizó un trabajo de identificación del riesgo basándose en las vulnerabilidades individuales de cada uno de los componentes de la infraestructura, por lo que los vectores de ataque más probables que podría utilizar un atacante son los siguientes:

- **Red:** Sin duda el mayor vector de ataque es la red, dado que gran cantidad de aplicativos y servidores cuentan con posibilidades de administración mediante

página web, o se encuentran conectados a la misma debido a las necesidades de los servicios que estos prestan.

- **Suplantación de identidad:** Un atacante valiéndose de ingeniería social podría suplantar la identidad de alguno de los usuarios con privilegios en el dominio, de forma tal, que esto le permitiera acceder a los servidores con la cuenta de un usuario autenticado.
- **Consola de administración:** El atacante podría conseguir acceso a los servidores o aplicaciones mediante pruebas de ensayo y error, o por medio del uso de diccionarios que permiten descifrar contraseñas débiles.
- **Software no verificado:** Para la realización de sus tareas es normal que los administradores de la plataforma y aplicativos utilicen algún sinnúmero de herramientas gratis o de prueba, de las cuales muchas de estas pueden estar infectadas por troyanos que permitirían a un atacante tener acceso a los servidores.

3.2.2.2.Indicios de un incidente.

Determinar si un incidente ha ocurrido o está por ocurrir en la mayoría de ocasiones resulta una tarea difícil, en gran parte porque muchas veces las señales son débiles y confusas, o simplemente los operadores no poseen la experiencia suficiente para para interpretarlas. En cualquiera de los casos es necesario contar con la ayuda extra que pueden brindar los distintos mecanismos de detección que de alguna forma u otra pueden ayudar a solventar las deficiencias humanas que posean los funcionarios que ejecutan dichas labores. Las siguientes representan algunos indicios comunes de los sistemas comprometidos en relación a la ocurrencia de incidentes de seguridad de la información:

- Reinicio inexplicado de los servidores y/o aplicaciones.
- Bloqueo de los servidores y/o aplicaciones.
- Recalentamiento excesivo del hardware.
- Alertas de uso excesivo de recursos.
- Logs de intentos de accesos fallido.
- Trafico de red anormal.
- Denegación de acceso al servidor.

- Aparición de usuarios no autorizados en las listas de acceso a los servidores.
- Pérdida de archivos o cifrado de los mismos.

3.2.2.3.Mecanismos de detección.

La detección de incidentes representa un componente indispensable para las distintas empresas que desean reforzar sus capacidades de gestión de incidentes, tanto así, que en el mercado prácticamente se ha consolidado un nicho propio donde inclusive es posible conseguir empresas que prestan estos servicios de manera externa, garantizando disponibilidades y labores de vigilancia continua de 7x24 . Para el caso de la CGR para la detección temprana de incidentes a nivel de su infraestructura debe centrar la solución en los vectores de ataque descritos, dado que ellos significan un mayor riego. Los siguientes son los mecanismos más comunes:

A. Herramientas para la detección temprana:

De acuerdo a los principales vectores de ataque se recomiendan las siguientes herramientas para la detección temprana del incidente:

- **Sistemas de prevención de intrusión IPS**: Herramienta de seguridad basado en red. Se ocupa del monitoreo de los sistemas o las redes en busca de actividades maliciosas con base en patrones de comportamiento alimentados principalmente por el fabricante de los dispositivos. El IPS puede interceptar y bloquear los paquetes maliciosos en la red, resetear el tráfico y enviar alarmas al equipo de respuesta o monitoreo.
- **Doble verificación de usuario:** Las herramientas de doble verificación de identidad para usuarios son las encargadas de confirmar que el usuario que accede a los sistemas si es quien dice ser, para lo que verifica dos o más veces la autenticación con el mismo; una primera parte mediante el uso de la contraseña propia el usuario y otra segunda parte mediante el envío de un código único a una cuenta registrada con anterioridad por el usuario. Para este caso el usuario debe confirmar el código único al igual que lo hizo con su contraseña.
- **Antivirus:** El antivirus conforma una de las herramientas más comunes utilizadas al momento de enfrentar un incidente de seguridad. Esto debido a que el antivirus puede realizar el escaneos de los archivos basándose en grandes bases de datos

contenidas a nivel de web y en análisis heurísticos, que lo convierten en la primera línea de defensa ante cualquier ataque.

- **Firewall:** El firewall se constituye en una potente herramienta al momento de detección de ataque dado que permite tener un informe de los puertos en los equipos que han sido objetos de ataque y que se han conseguido bloquear por medio de este. Ello hace posible determinar y detectar algunos tipos de ataque como por ejemplo el escaneo de puertos desde un equipo remoto.

B. Factor Humano.

Los procedimientos de detección temprana de incidentes indiscutiblemente requieren factores humanos que permitan determinar la ocurrencia de un incidente, ello debido a que el componente humano hasta el momento ha logrado definirse como un elemento irremplazable, pues puede reconocer patrones y comportamientos que las máquinas no. De hecho, en muchas ocasiones terminan siendo los usuarios de los aplicativos los primeros en darse cuenta que algo anda mal; procediendo con mucha frecuencia a dar aviso a los administradores de los aplicativos sobre su hallazgo. Por tal motivo es necesario que dentro de su gestión de incidentes la entidad cuente con distintos mecanismos que permitan dar relevancia al componente humano como un actor inalienable y principal en la gestión de incidentes. Implementando mecanismos tales como:

- Participación y acercamiento a los ciudadanos de forma que conozcan los procesos o procedimientos que les permitan reportar o comunicar fallas en la aplicación.
- Contar con personal especializado o capacitar los actuales de forma que puedan reconocer las anomalías en sus correspondientes aplicativos.
- Redes de cooperación entre los distintos actores y empresas.

3.2.3. Etapa de categorización y análisis.

Analizar y priorizar un incidente de seguridad requiere un trabajo conjunto del equipo de respuesta con los administradores de las aplicaciones afectadas, dado que esta persona, al ser la que más conoce de dicha aplicación puede contribuir con alternativas que afecten lo menos posible a los servicios prestados por la misma. En la etapa de categorización y análisis (Figura 37) deben asignarse categorías al tipo de incidente de seguridad de acuerdo al análisis que se

haga sobre el mismo, para ello el análisis debe tener como punto de partida los riesgos a los cuales se encuentre expuesta la infraestructura de acuerdo a los vectores de ataque, la cantidad de máquinas comprometidas, cantidad de máquinas vulnerables, información comprometida, etc. Igualmente debe tenerse en cuenta el componente de afectación al negocio procedente de la etapa transversal de afectación al negocio, dado que la misma es igualmente útil y permite determinar de forma más objetiva la resolución del incidente con base en las prioridades de la entidad.

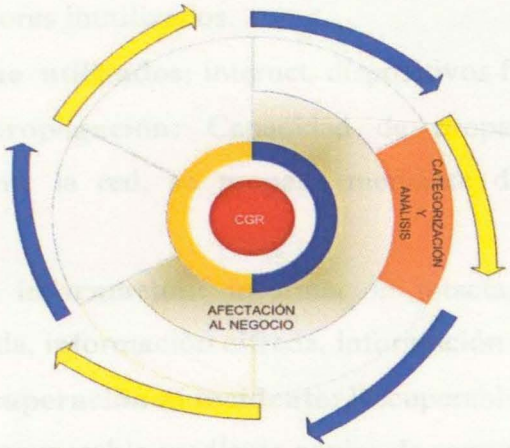

Figura 37. Etapa de categorización y análisis. Elaboración propia.

La etapa de análisis comprende las siguientes actividades:

- Se debe determinar la cantidad de máquinas, sistemas o equipos afectados.
- Verificar la existencia de datos históricos acerca de la violación de seguridad o el malware, que permitan determinar información clave para la etapa de contención.
- Realizar la recolección de datos arrojados por sniffers y programas de seguridad.
- Realizar búsquedas en internet relacionadas con el incidente, como puertos de ataque, información borrada, tipos de archivos atacados, servicios que corren en el servidor, etc.
- Contactar con los proveedores de las aplicaciones afectadas con el fin de obtener información que pueda ser necesaria para la documentación del incidente.
- Documentar el estado actual del incidente elaborando un resumen del mismo.
- Registrar las acciones tomadas hasta el momento.
- Reunir evidencias en relación con el incidente.

- Registrar la información de contacto del personal involucrado por si es necesario rendir descargos u obtener más información.

Una vez se ha recolectado la información suficiente se debe realizar una categorización o priorización del incidente, la cual debe de contemplar los siguientes parámetros, según sea necesario:

- **Nivel de daño sobre la infraestructura de servidores:** Servidores intactos, servidores sin acceso, servidores operados remotamente por personal no autorizado, servidores inutilizados.
- **Vectores de ataque utilizados:** internet, dispositivos físicos, ingeniería social.
- **Capacidad de propagación:** Capacidad de propagación nula, se propaga fácilmente mediante la red, se propaga mediante dispositivos físicos de uso compartido.
- **Efectos sobre la información:** información intacta, información modificada, información borrada, información cifrada, información en poder del atacante.
- **Capacidad de recuperación al incidente:** Recuperable a corto plazo, recuperable a mediano plazo, recuperable mediante copias de seguridad.
- **Afectación al negocio:** el negocio no sufre afectación, la afectación es leve, la afectación es moderada, se presentan graves efectos en el negocio.
- **Tipo de ataque:** DoS, Hombre en el medio, secuestro de información, infección por gusano, inutilización del sistema operativo, robo de contraseñas, etc.

Una vez se han contemplado los parámetros necesarios, se fija la priorización para el manejo del incidente de acuerdo a lo siguiente:

- **Prioridad baja:** No se afectan los servicios o se afectan servicios no esenciales, el incidente puede ser manejado localmente sin riesgo para los negocios de la entidad.
- **Prioridad media:** Se afectan algunos servicios no esenciales, con probabilidad de propagación, poco probable que se afecte al negocio.
- **Prioridad alta:** Se afectaron aplicativos misionales o servicios esenciales, alta probabilidad de propagación, riesgo de pérdida o secuestro de información, riesgo

de daño de equipos, información recuperable en tiempos superiores al periodo máximo tolerable de interrupción MTPD, existe afectación al negocio.

3.2.4. Etapa de afectación al negocio.

La etapa de afectación al negocio (Figura 38) es una etapa transversal que si bien parte paralela a la etapa de descubrimiento y finaliza en la etapa de normalización, su relevancia comienza a tener sentido a partir de la etapa de categorización y análisis, donde sus efectos comienzan a tenerse en cuenta sobre la resolución del incidente. Esta etapa tiene la finalidad de obtener indicaciones y priorizar procesos en relación con los efectos del incidente sobre el negocio de la CGR. Lo que permite centrarse en el objetivo de mantener los tiempos de recuperación del negocio dentro de los límites aceptables definidos por el estudio de necesidades de la entidad.

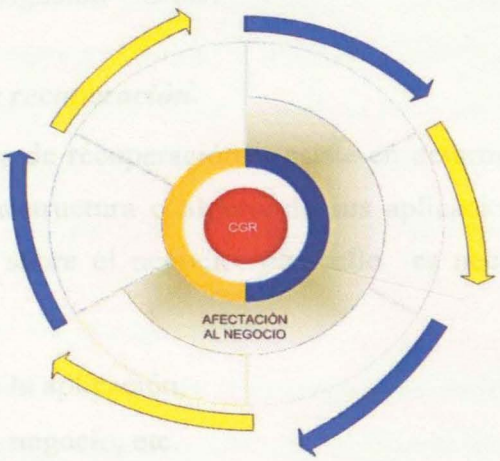

Figura 38. Etapa de afectación al negocio. Elaboración propia.

La etapa de afectación al negocio comprende las siguientes actividades:

3.2.4.1.Identificación de aplicaciones críticas.

Con el fin de establecer el impacto de los incidentes sobre el negocio, es necesario identificar aquellos aplicativos que tienen impacto directo sobre los distintos procesos y macroprocesos que puedan afectar los objetivos misionales de la entidad, para ello es necesario conocer el plan estratégico o el sistema de gestión de calidad de dicha empresa, dado que de ahí se podría obtener toda la información necesaria.

Modelo de Gestión de incidentes de seguridad CGR.

Para el caso la Contraloría General de la República, el análisis se realizó sobre los servidores de SIREF, SIRECI, SIPAR, SIGEDOC, SIBOR, PORTAL, INTRANET, KACTUS, SAE, DEUDA PÚBLICA Y PRORROGAS dado que los mismos son considerados críticos y con incidencia directa sobre los macroprocesos y procesos misionales y estratégicos de la entidad (Tabla 9, Tabla 10). Los cuales se encuentran relacionados en la Tabla 2 y la Figura 18.

Se identificaron los siguientes macroprocesos:

- Control Fiscal Micro – CMI.
- Control Fiscal Macro – CMA.
- Responsabilidad Fiscal y Jurisdicción Coactiva – RFJ.
- Enlace con Cliente y Partes Interesadas – ECP.
- Direccionamiento Estratégico y Arquitectura Empresarial– DET.
- Comunicación y divulgación – CYD.

3.2.4.2.Identificación de tiempos de recuperación.

La identificación de los tiempos de recuperación consiste en determinar los tiempos en los cuales es posible recuperar la infraestructura o alguna de sus aplicaciones críticas sin que se produzca un impacto considerable sobre el negocio, para ello es necesario conocer detalles como:

- El funcionamiento de la aplicación.
- Orientación: Cliente, negocio, etc.
- Frecuencia de copias de seguridad. (cantidad de información que se puede perder y pueda ser recuperada desde las copias de seguridad)
- Tiempo que el cliente está dispuesto a soportar sin el servicio.
- Coste económico.

Con base en esta información se deben calcular:

- El tiempo Objetivo de recuperación(RTO)
- Punto objetivo de recuperación (RPO)
- Periodo máximo tolerable de interrupción (MTPD).

Modelo de Gestión de incidentes de seguridad CGR.

Para el caso de la contraloría general estos tiempos de recuperación se encuentran contenidos en la Tabla 28 y Tabla 29 del presente documento, las cuales definen los siguientes tiempos de recuperación:

- Tiempo objetivo de recuperación (RTO): 4 a 8 horas.
- Punto objetivo de recuperación (RPO): 1 día.
- Periodo máximo tolerable de interrupción (MTPD): 1 día.

Por lo que supone que en caso de ser afectada la infraestructura de servidores, en la peor de las situaciones, la recuperación de esta no debería tardar más de 1 día, so pena de causar afectaciones gravísimas para la entidad según el aplicativo afectado.

3.2.4.3.Ajuste a la situación.

La actividad de ajuste a la situación es una actividad de empalme de la etapa de afectación al negocio, con las etapas de ´categorización y análisis´, contención, y normalización. Se controlan los tiempos de duración de estas etapas con el objetivo de que la suma del tiempo de duración de las tres etapas no supere el periodo máximo tolerable de interrupción MTPD.

MTPD > categorización y análisis + Contención + Normalización.

3.2.4.4.Estimación del impacto sobre el negocio.

La actividad de estimación del impacto es la encargada de estimar el grado de impacto al negocio de acuerdo a los procesos afectados y tiempo de afectación, para lo que el proceso de cálculo es realizado con base en los siguientes impactos:

- Impacto operativo.
- Impacto económico.
- Impacto al cliente (ciudadanía para el caso de entidades públicas).

Cada uno debe de ser calculado de acuerdo a parámetros internos de la entidad a la cual sea aplicado el modelo, categorizando los mismos en niveles que van desde impactos "insignificantes" hasta impactos "catastróficos", según la gravedad del mismo. El documento incluye todo un proceso de identificación del riesgo para la infraestructura de servidores de la CGR donde la Tabla 17, la Tabla 18 y la Tabla 19 ilustran los diferentes niveles de impacto de

acuerdo a su clasificación. Por ejemplo, para el caso del impacto económico causado por un incidente, valores por debajo de $29.115.683 son considerados como insignificantes, mientras que valores por encima de $329.254.608 son considerados como catastróficos, esto de acuerdo a un proceso de estimación realizado de acuerdo a las necesidades de la entidad.

3.2.5. Etapa de contención.

En la etapa de contención (Figura 39) se contienen y neutralizan los incidentes que lleguen a ocurrir de forma que se pueda limitar el daño producido a su mínimo posible. Ello implica que se deben tomar las medidas de contención necesarias para resolver el incidente con la mayor celeridad.

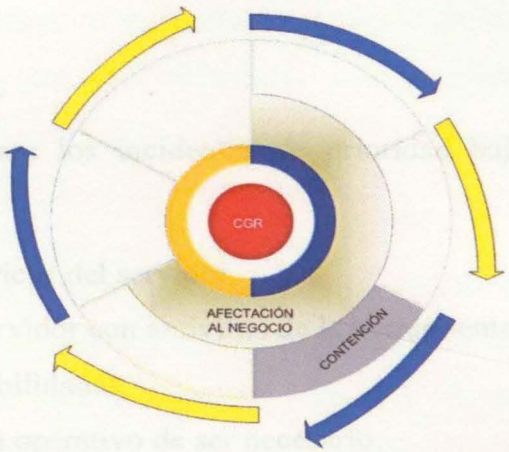

Figura 39. Etapa de contención. Elaboración propia.

Entre las medidas de contención se incluye acciones como:

- Aislamiento del equipo o máquina infectado.
- Apagado del equipo.
- Filtrado mediante red de los puertos de los quipos que se consideren infectados o con problemas de seguridad.
- Entrevista con los administradores directos de la aplicación.
- Consulta con proveedores.
- Monitoreo continuo de la red.
- Bloqueo de páginas o URL´s sospechosas.
- Elaboración de reportes para el los directivos de grupo.

Modelo de Gestión de incidentes de seguridad CGR.

- Emisión de boletines para los usuarios que acceden al aplicativo.
- Restricción de acceso a servicios conexos que puedan terminar afectados.
- Bloqueos de dominios.
- Remediación de vulnerabilidades.
- Instalación de reglas o políticas en el firewall orientadas a evitar que ocurra un nuevo ataque o incidente con características similares.

Cada una de estas medidas aplicadas de acuerdo a la prioridad del incidente, ya sea bajo, medio o alto, según se haya definido en la fase de categorización y análisis. Las siguientes son las medidas recomendadas para la infraestructura de servidores de la CGR de acuerdo a la prioridad:

3.2.5.1.Incidentes de prioridad baja.

Las medidas de contención para los incidentes de prioridad baja en la plataforma de servidores son las siguientes:

- Revisión de logs e históricos del servidor.
- Escaneo y vacuna del servidor con antivirus de la herramienta.
- Remediación de vulnerabilidades.
- Actualización de sistema operativo de ser necesario.
- Cambio de contraseñas
- Vigilancia con escáneres de red con el fin de estar al tanto del comportamiento.
- Apagado del servidor o servicios prestados.
- Reinstalación o recuperación de copias de seguridad si es necesario.
- Reporte de actividad del servidor a la USATI.
- Bloqueo de páginas sospechosas.

3.2.5.2.Incidentes de prioridad media.

Las medidas de contención para los incidentes de prioridad media en la plataforma de servidores son las siguientes:

- Aislamiento del servidor o grupo de servidores afectados.
- Revisión de logs e históricos del servidor.

- Escaneo y vacuna del servidor con antivirus de la herramienta.
- Remediación de vulnerabilidades.
- Actualización de sistema operativo de ser necesario.
- Cambio de contraseñas.
- Apagado del servidor o servicios prestados.
- Reinstalación o recuperación de copias de seguridad si es necesario.
- Reporte de actividad del servidor a la USATI.
- Reporte de la situación al director de la oficina con el fin de programar de alertar a directivos y programar medidas adicionales necesarias.
- Bloqueo de páginas sospechosas.
- Colaboración con equipos de respuesta externos a la entidad.
- Las demás medidas que sean necesarias para el efecto de la contención del incidente.

3.2.5.3.Incidentes de prioridad alta.

Estos incidentes de seguridad generan afectación al negocio de la CGR, y/o pueden afectar un gran número de servidores inclusive toda la infraestructura, por lo que la contención se constituye en un asunto prioritario para el grupo de respuesta y la entidad, por lo que se deben aplicar las siguientes medidas:

- Aislamiento de máquinas o servidores involucrados.
- Remediación de vulnerabilidades.
- Comunicación mediante informe a USATI y directivas de las distintas dependencias infectadas.
- Comunicados a la comunidad afectada, previa autorización del superior.
- Activación de canales de comunicación y alertas hacia otros grupos de respuesta y policía nacional.
- Bloqueo de páginas sospechosas.
- Cambio de contraseñas.
- Escaneo y vacuna del servidor con antivirus de la herramienta.
- Actualización de sistema operativo de ser necesario.

Modelo de Gestión de incidentes de seguridad CGR.

- Recuperación del servidor o servicios desde copias de seguridad.
- Activación del DRP.
- Elaboración de reportes e informes.
- Las demás medidas que sean necesarias para el efecto de la contención del incidente.

3.2.6. Etapa de normalización.

La etapa de normalización (Figura 40) corresponde a la última etapa transcurrida durante la ocurrencia del incidente, ello debido a que con la etapa de normalización involucra el hecho de que el incidente ya ha sido contenido y por consiguiente los servicios afectados están siendo normalizados o puestos en producción nuevamente.

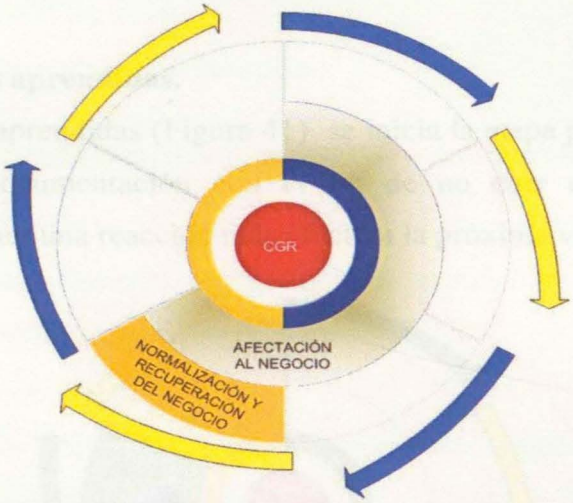

Figura 40. Etapa de normalización. Elaboración propia.

En la etapa de normalización se deben realizar las siguientes actividades.

- Recuperación de los servicios afectados.
- Restauración de copias de seguridad.
- Reconstrucción de bases de datos o archivos de sistema comprometidos.
- Remediación de vulnerabilidades a largo plazo.
- Verificación y vigilancia de servicios afectados y conexos con el fin de descartar contaminaciones o malos funcionamientos.

Modelo de Gestión de incidentes de seguridad CGR.

- Realizar un análisis del impacto real sufrido, verificando que los tiempos de reposición se encuentren dentro de los tiempos determinados o periodo máximo tolerable de interrupción MTPD contenido dentro de la fase de afectación al negocio.
- Emitir los correspondientes informes y avisos de normalización del servicio a superiores y comunidad en general de acuerdo a las normas de la entidad.

Es de notar que la etapa de normalización no siempre es inmediata, se debe procurar que los incidentes no se vuelvan a repetir, lo que en muchas circunstancias requiere de cambios de gran impacto que en gran parte llegan a durar semanas o meses. Este hecho por lo general afecta el restablecimiento total de los servicios, por lo que muchas de las tareas se realizan ya sea en forma paralela o escalonada, de acuerdo a la situación.

3.2.7. Etapa de lecciones aprendidas.

Con la etapa de lecciones aprendidas (Figura 41) se inicia la etapa post-incidente esta etapa tiene como fundamento la documentación con el fin de no caer en el mismo incidente nuevamente, o simplemente tener una reacción más efectiva la próxima vez que ocurra.

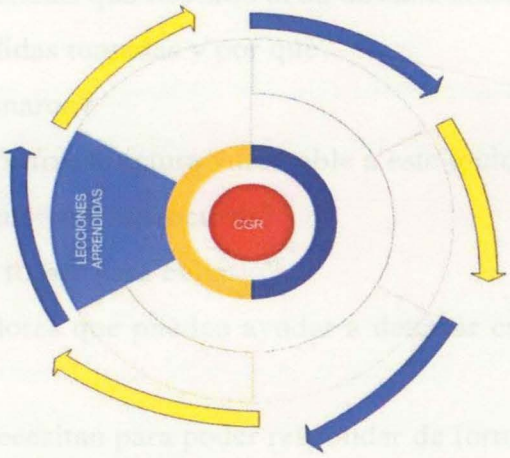

Figura 41. Etapa de lecciones aprendidas. Elaboración propia.

El éxito de esta etapa recae en el compromiso que tengan los administradores y el grupo de respuesta a incidentes con la gestión de documentar todas las medidas y contramedidas tomadas durante el incidente. Se debe realizar una bitácora que registre detalles como:

- Vectores de ataque.
- Tipo de equipo.

- Su sistema operativo.
- Aplicaciones que corre.
- Versión de parches que tenía el equipo al momento del incidente.
- Vulnerabilidades aprovechadas por el atacante.
- Fecha y hora de los eventos.
- Equipos afectados.
- Señales y evidencias del incidente.
- Acciones tomadas.
- Soluciones planteadas y aplicadas.
- Documentación de internet.
- Tiempo consumido por el incidente.
- Cualquier información relevante al incidente.

En resumen, se deben registrar acciones que ayuden a resolver los siguientes planteamientos:

- ¿Cómo inició el incidente?
- ¿Cuáles fueron las evidencias que llevaron al su descubrimiento?
- ¿Cuáles fueron las medidas tomadas y por qué?
- ¿Cuáles medidas funcionaron?
- ¿Qué hizo al servidor o infraestructura vulnerable a este incidente?
- ¿Existe posibilidad de que vuelva a ocurrir?
- ¿Qué medidas se deben tomar para evitarlo?
- ¿Cuáles son los indicadores que pueden ayudar a detectar este tipo de incidentes en el futuro?
- ¿Qué herramientas se necesitan para poder responder de forma más rápida y eficiente la próxima vez?
- ¿en caso de no contar con lo necesario para reaccionar, cuales son los grupos o personas externas a la entidad que pueden ayudar a solucionar el incidente?
- ¿Cuánto tiempo duró el incidente?

Como es de observar la etapa de lecciones aprendidas simplemente es una forma de preparar a la entidad o empresa para cuando ocurra nuevamente un incidente con condiciones similares al

incidente que se acaba de resolver, la entidad tenga el conocimiento y las herramientas adecuadas para reaccionar de forma más eficiente y rápida. Las lecciones aprendidas igualmente permitirán a la entidad autoevaluarse y mejorar su respuesta a incidentes permitiendo compartir sus conocimientos con otras entidades que posiblemente estén necesitando de esta ayuda, y sobretodo, establecer y mejorar sus políticas de seguridad, las cuales son dictaminadas actualmente por la USATI en el caso de la CGR.

Desde el punto de vista de negoció, las lecciones aprendidas contribuirán con la reducción del riesgo y el impacto que podrían generarle estos incidentes, lo que se traduce en una gestión más efectiva en pro de los objetivos misionales y estratégicos de la entidad.

3.3. Procedimiento para el Reporte de Incidentes al Grupo de Respuesta CSIRT.

El reporte de incidentes de seguridad por parte de los funcionarios administradores de plataforma y servidores es un componente muy importante en la gestión de incidentes, por lo que es necesario contar con procedimientos prestablecidos que indiquen el cómo actuar dado el caso, por esta razón a continuación se describen los procedimientos necesarios para el reporte de incidentes al grupo de respuesta a incidentes de seguridad.

3.3.1. Reporte de incidentes de seguridad por acceso no autorizado.

El siguiente corresponde al procedimiento a realizar por parte de administrador que detecte un acceso no autorizado al servidor:

1. Cambio de contraseñas de acceso al servidor.
2. Aplicación de parches a nivel de sistema operativo y distintos aplicativos.
3. Si el acceso al servidor continúa se debe aislar el servidor.
4. Realizar el reporte a USATI o al grupo de respuestas mediante el formulario de la Figura 44, indicando las medidas tomadas.
5. Si se tienen logs o algún elemento que evidencie el hecho, anexarlos al reporte.
6. El grupo de respuesta atenderá el caso de acuerdo a los protocolos, y procedimientos establecidos en el diagrama de procedimientos contenido en este documento.

Modelo de Gestión de incidentes de seguridad CGR.

3.3.2. Reporte de incidentes de seguridad por malware.

El siguiente corresponde al procedimiento a realizar por parte de administrador que detecte un malware en los servidores:

1. Aislar el servidor de la red.
2. Cambio de contraseñas de acceso al servidor.
3. Realizar copias de seguridad a la información importante.
4. Realizar el reporte a USATI o al grupo de respuestas mediante el formulario de la Figura 44, indicando las medidas tomadas.
5. El grupo de respuesta atenderá el caso de acuerdo a los protocolos y procedimientos establecidos en el diagrama de procedimientos contenido en este documento.

3.3.3. Reporte de incidentes de seguridad por secuestro o cifrado de información.

El siguiente corresponde al procedimiento a realizar por parte de administrador que detecte un secuestro o cifrado de información:

1. Aislar el servidor de la red.
2. Cambio de contraseñas de acceso al servidor.
3. Realizar copias de seguridad a la información importante.
4. Realizar el reporte a USATI o al grupo de respuestas mediante el formulario de la Figura 44, indicando las medidas tomadas.
5. El grupo de respuesta atenderá el caso de acuerdo a los protocolos y procedimientos establecidos en este documento.

3.3.4. Reporte de incidentes de seguridad por denegación de servicio DDOS.

El siguiente corresponde al procedimiento a realizar por parte de administrador que detecte intentos de ataques por denegación de servicio hacia el servidor:

1. Realizar el reporte a USATI o al grupo de respuestas mediante el formulario de la Figura 44, indicando las medidas tomadas.
2. El grupo de respuesta atenderá el caso de acuerdo a los protocolos y procedimientos establecidos en el diagrama de procedimientos contenido en este documento.

3.3.5. Reporte de incidentes de seguridad por intentos de acceso recurrentes y fallidos al servidor.

El siguiente corresponde al procedimiento a realizar por parte de administrador que detecte intentos de acceso fallidos y recurrentes al servidor:

1. Realizar el reporte al grupo de respuestas mediante el formulario de la Figura 44, indicando las medidas tomadas.
2. El grupo de respuesta atenderá el caso de acuerdo a los protocolos y procedimientos establecidos en el diagrama de procedimientos contenido en este documento.

3.3.6. Reporte de incidentes de seguridad por ataques desconocidos o no determinados al servidor.

El siguiente corresponde al procedimiento a realizar por parte de administrador que detecte ataques desconocidos al servidor:

1. Cambio de contraseñas de acceso al servidor.
2. Realizar Copias de seguridad a la información importante.
3. Realizar el reporte al grupo de respuestas mediante el formulario de la Figura 44, indicando las medidas tomadas.
4. El grupo de respuesta atenderá el caso de acuerdo a los protocolos, procedimientos establecidos en el diagrama de procedimientos contenido en este documento.

3.4. Diagrama de Procedimientos y Formatos Varios.

En concordancia complemento con el ciclo de vida del modelo referenciado con anterioridad la Figura 42 y la Figura 43 ilustran el correspondiente diagrama de procedimientos para la gestión de los incidentes, mientras que la Figura 44, la Figura 45, la Figura 46 y la Figura 47 contienen modelos de los distintos formatos necesarios para la apertura, informes, boletines y cierre de casos relacionados con incidentes de seguridad.

Modelo de Gestión de incidentes de seguridad CGR.

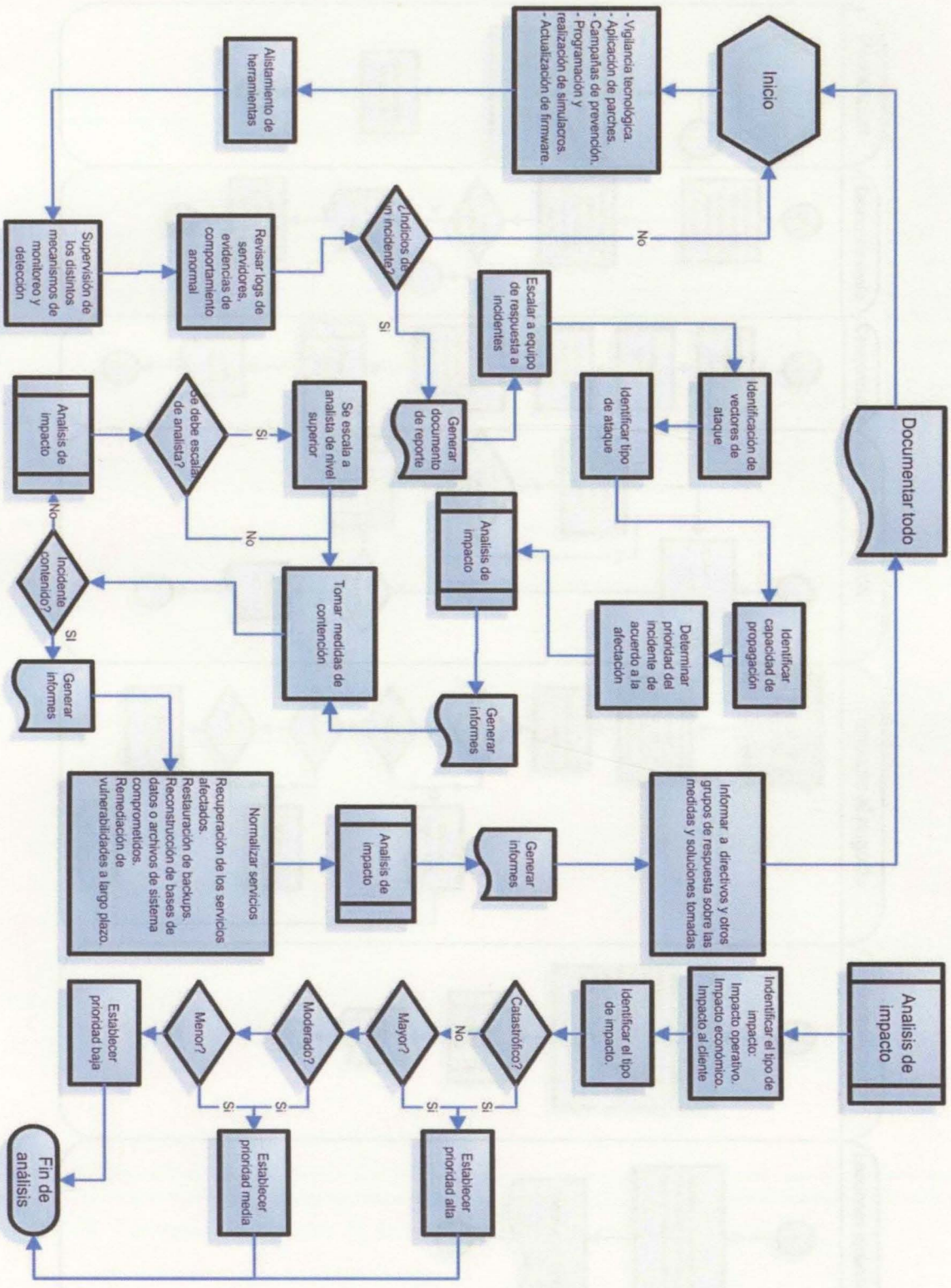

Figura 42. Diagrama de procedimientos. Fuente: Elaboración propia.

Modelo de Gestión de incidentes de seguridad CGR.

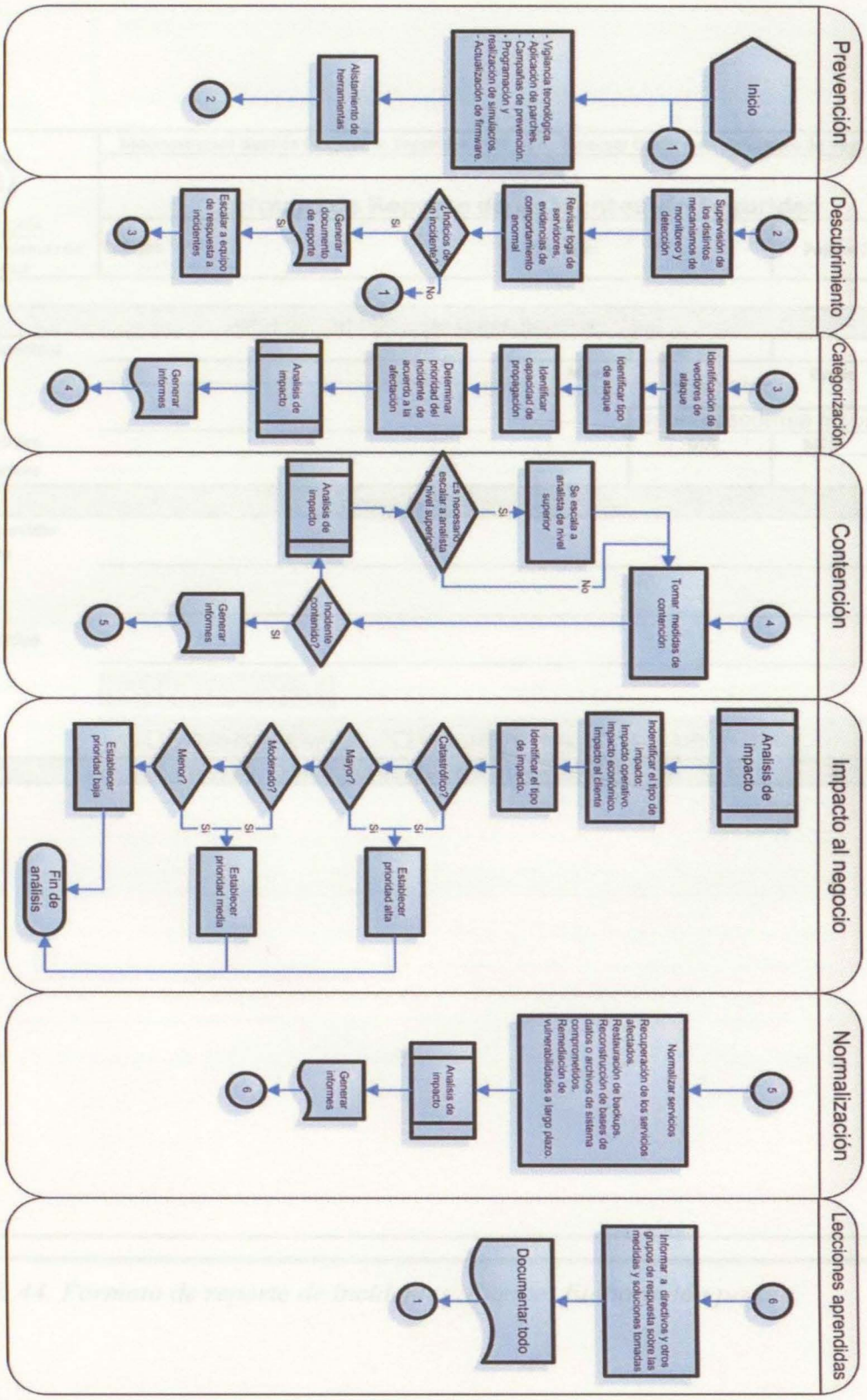

Figura 43. Diagrama de procedimientos por etapas. Fuente: Elaboración propia.

CONTRALORÍA GENERAL DE LA REPÚBLICA Gestion de Incidentes de Seguridad	Macroproceso: Gestión Integral de Seguridad -GIS	Proceso: Gestión de Incidentes de Seguridad	
	Formato de Reporte de Incidentes de Seguridad		
	Código:	Versión:	Página 1 de 1

Datos del Funcionaerio Quien Reporta				
Nombres y Apellidos		N° Ext.		
Cargo	Nivel		Grado	
Dependencia		FECHA DE SOLICITUD DEL USUARIO		
Correo electrónico		DIA	MES	AÑO
No. de caso anexo				

Datos del servidor	
Nombre del servidor comprometido	
Dirección IP	
Sistema operativo	
Prioridad	
Afectación	☐ ACCESIBLE COMPLETAMENTE ☐ OPERA LIMITADAMENTE ☐ TOTALMENTE INACCESIBLE

Eventos Anormales detectados

Figura 44. Formato de reporte de incidentes. Fuente: Elaboración propia.

Modelo de Gestión de incidentes de seguridad CGR.

CONTRALORÍA GENERAL DE LA REPÚBLICA Gestion de Incidentes de Seguridad	Macroproceso: Gestión Integral de Seguridad -GIS	Proceso: Gestión de Incidentes de Seguridad	
	Formato de Seguimiento a Incidentes de Seguridad		
	Código:	Versión:	Página 1 de 1
	Fecha:		
Información Grupo de Respuesta a Incidentes			
Nombres y Apellidos		Firma	
Nombres y Apellidos		Firma	
Nombres y Apellidos		Firma	
Nombres y Apellidos		Firma	
Nombres y Apellidos		Firma	
Nombres y Apellidos		Firma	
Datos del servidor			
Nombre del servidor comprometido			
Dirección IP			
Sistema operativo			
Prioridad			
Estado	☐ INFECTADO	☐ AISLADO	☐ BAJO ESTUDIO ☐ SANO
Bitácora			
Recomendaciones			

Figura 45. Formato de seguimiento a incidentes. Fuente: Elaboración propia.

Modelo de Gestión de incidentes de seguridad CGR.

CONTRALORÍA GENERAL DE LA REPÚBLICA Gestión de Incidentes de Seguridad	Macroproceso: Gestión Integral de Seguridad -GIS	Proceso: Gestión de Incidentes de Seguridad	
	Formato de Emisión de Boletines Durante Incidentes de Seguridad		
	Código:	Versión:	Página 1 de 1
Boletín Numero:	Fecha:		
Quien autoriza el boletín			
Nombres y Apellidos		Firma	
Nombres y Apellidos		Firma	
Detalles del incidente			
Servicios afectados			
Tiempo estimado de recuperación			
Medidas tomadas			
Prioridad			
Avance	☐ BAJO ESTUDIO	☐ CONTENIDO	☐ RESTAURADO
Recomendaciones e información adicional:			

Figura 46. Formato de emisión de boletines. Fuente: Elaboración propia.

CONTRALORÍA Gestion de Incidentes de Seguridad	Macroproceso: Gestión Integral de Seguridad -GIS		Proceso: Gestión de Incidentes de Seguridad	
	Formato de Informe Final para Incidentes de Seguridad			
	Código:		Versión:	Página 1 de 1
Número de caso:		Fecha:		
Información Grupo de Respuesta a Incidentes				
Nombres y Apellidos			Firma	
Nombres y Apellidos			Firma	
Nombres y Apellidos			Firma	
Nombres y Apellidos			Firma	
Nombres y Apellidos			Firma	
Nombres y Apellidos			Firma	
Datos del servidor				
Nombre del servidor comprometido				
Dirección IP				
Sistema operativo				
Prioridad				
Resumen				
Descripción de la solución				

Figura 47. Formato para informe final de incidentes. Fuente: elaboración propia.

Conclusiones

Los modelos o guías para la gestión de incidentes no son nada nuevo en el mercado. De hecho como se comprueba en la investigación realizada, existen numerosas guías o marcos en torno a este tema, guías que han sido realizadas con el fin de satisfacer necesidades de seguridad de la información tanto a nivel particular como general de algunos países o empresas ya sean estas de capital público o privado.

Igualmente, como se evidencia a través del documento, la seguridad de la información ha pasado a ser tema de interés global, tanto así que las grandes potencias no están escatimando esfuerzos en pro de asegurar sus recursos informáticos, o en su defecto, contar con un buen plan de gestión de incidentes que permita recuperarse de las afectaciones sufridas lo más rápido posible, aún más si dichos incidentes afectan de forma directa o indirecta sus infraestructuras críticas.

Hecho del cual, Colombia no es la excepción. Es claro que se han realizado grandes esfuerzos orientados hacia la seguridad de la información y más aún hacia la gestión de incidentes, tanto así que no solo se han sacado políticas nacionales mediante el Consejo Nacional de Política Económica y Social CONPES (como las actuales políticas con lineamientos para ciberseguridad y ciberdefensa CONPES 3701 y la política nacional de seguridad digital CONPES 3854), sino que también se han delegado funciones orientadas hacia la gestión de incidentes de seguridad, al ministerio de las tecnologías MINTIC, quien ha comenzado a liderar los procesos en relación, mediante la publicación de recomendaciones y guías aplicables a la gestión de incidentes no solo en las empresas e instituciones nacionales y de infraestructura crítica, sino también en aquellas privadas que consideren necesaria la implementación de medidas para evitar que su negocio se pueda ver afectado por la ocurrencia de un incidente informático.

Con respecto a la contraloría general se debe notar que si bien esta posee un plan de gestión de incidentes, el mismo corresponde a un modelo generalizado, enmarcado sobre la norma ISO 27000 la cual tiene como fuerte la estandarización, por lo que se centra poco en detalles específicos relacionados con seguridad de la información siendo menos selectivo que la norma NIST que recompila una serie de mejores prácticas en torno al tema, lo que provoca que esta sea

utilizada por una gran cantidad de entidades como es el caso del MINTIC quien lo utiliza como modelo para sus recomendaciones en relación con la gestión de incidentes de seguridad. De ahí que el trabajo propuesto, más que ser de gran utilidad, podrá representar un complemento y una gran fuente de insumo para futuras políticas y planes institucionales como lo es el caso del plan de recuperación de desastres de la entidad.

De este modo y con base en los modelos analizados el desarrollo de este proyecto propone el planteamiento de un modelo desarrollado en gran medida a partir del modelo NIST por tratarse de un modelo no solo ampliamente utilizado, sino también, recomendado por el MINTIC, que corresponde con los enfoques de seguridad de la información que se pretenden satisfacer a nivel de la entidad y en claro cumplimiento con la política nacional de seguridad digital establecida mediante CONPES 3854 de 2016. Ello sin dejar de lado algunas recomendaciones con base en la guía ISO 27035 que igualmente fueron tomadas dado su conocido referente como base para la estandarización de procesos.

En concordancia con lo anterior, es necesario contemplar las necesidades de la entidad desde el punto de la gestión del riesgo y la afectación al negocio, dado que como se observa a lo largo del capítulo 2 existe una gran variedad de amenazas que de forma indirecta pueden afectar la plataforma de la entidad, amenazas que sacan ventaja de vulnerabilidades contenidas en cada uno de los elementos que conforman la plataforma tanto a nivel físico, como en la virtualización, el sistema operativo y software aplicativo.

Si bien estas vulnerabilidades en su gran mayoría han sido remediadas mediante la publicación y aplicación de parches de seguridad, aún queda una gran incertidumbre al respecto de aquellas que no se conocen y que normalmente terminan siendo las que más daño causan.

En relación a esto cobra más relevancia contar en las entidades con una buena gestión de incidentes dado que permitirá reaccionar de forma adecuada ante estos eventos sin importar donde se originen los mismos.

El análisis del presentado a lo largo del capítulo 2 permitió realizar una aproximación al estado actual de infraestructura tecnológica de la CGR en relación con vulnerabilidades presentes que pueden ser explotadas mediante distintos vectores como la ingeniería social, la suplantación de identidad, el internet y el uso de software no autorizado, entre otros, que representan un peligro real, por lo que la propuesta contempla un modelo alineado con el negoció en relación

no solo con las políticas de las oficinas relacionadas en el proceso de seguridad de la información como lo son la Unidad de Seguridad y Aseguramiento Tecnológico e Informático USATI y la Oficina de Sistemas e Informática OSEI, sino igualmente con las políticas y objetivos institucionales en pro de su misión y plasmados en sus diferentes macroprocesos. Por lo que el modelo apoya tanto los objetivos de calidad, como misionales y estratégicos de la entidad fortaleciendo sus actividades de vigilancia y control fiscal mediante las garantías necesarias para dar continuidad a los servicios principales ante la ocurrencia de un incidente de seguridad en su infraestructura de servidores.

Así mismo, y en complemento con los capítulos 1 y 2, el documento en el capítulo 3 propone las herramientas, los recursos y los procedimientos necesarios para la gestión del incidente, planteando de forma clara el ciclo de vida del modelo, el cual permite mediante distintas etapas avanzar hacia la resolución de los posibles incidentes de manera gradual y facilitando igualmente que el modelo pueda ser implementado sin mayores dificultades en la entidad.

De la misma forma el modelo de gestión propuesto si bien se encuentra modelado para ser aplicado en la contraloría general, puede ser utilizado u adaptado para otras entidades sin mayor problema, debido a que en el mismo se utiliza terminología general y no propia de la entidad, permitiendo que este pueda ser adoptado fácilmente por entidades del estado y empresas privadas como alternativa a los modelos conocidos tradicionalmente.

Finalmente, y en concordancia con los objetivos del proyecto, el desarrollo del trabajo contiene el análisis centrado en la plataforma de servidores de la Contraloría General y su consecuente impacto sobre el negocio de la entidad, lo que permitió proponer un modelo de gestión de incidentes con las respectivas herramientas, procedimientos y recursos necesarios para su aplicación en la entidad, y en concordancia con los respectivos macroprocesos y procesos de gestión de calidad, seguridad de la información, y plan de recuperación de desastres desarrollados y en proceso de implementación por parte de la CGR.

Bibliografía

Agencia de Gobierno Electrónico y Sociedad de la Información. (2010). *Guia de procesos en gestión de incidentes.* Uruguay.

Almeida Galárraga, J. R. (2015). *Análisis y diseño de una Infraestructura convergente.* Quito: Pontificia Universidad Católica del Ecuador.

Barth, B. (2018). *Old version of HPE Lights-Out server management contains DoS vulnerability.* Obtenido de https://www.scmagazineuk.com/old-version-of-hpe-lights-out-server-management-contains-dos-vulnerability/article/748493/

Baud, J.-l. (2015). *Preparación para la certificación ITIL Foundation V3.* Barcelona: Ediciones ENI.

Best Management Practice. (2011). *ITIL Service Operation.* Norwich: TSO- The Stationery Office.

Beyond Security. (2018). *Finding and Fixing Vulnerability in HP StorageWorks MSA P2000 Hidden admin User Default Credentials , a High Risk Vulnerability.* Obtenido de https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_hp_storageworks_msa_p2000_hidden_admin_user_default_credentials

Consejo Nacional de Politica Económica y Social. (2011). *CONPES 3701 - Lineamientos de política para ciberseguridad y ciberdefensa.* Bogotá.

Consejo Nacional de Política Económica y Social. (2016). *CONPES 3854 - Política nacional de seguridad digital.* Bogotá.

Contraloría General de la República. (2012). *Resolución reglamentaria 205 de 2012. Por la cual se determina el funcionamiento interno de la Unidad de Seguridad y Aseguramiento Tecnológico e Informático y las Direcciones de Seguridad y Aseguramiento Tecnológico e Informático.* Bogotá: Contraloría General de la República.

Contraloría General de la República. (2013). *Política de seguridad de la información.* Bogotá.

Contraloría General de la República. (2014). *Resolución 70 de 2014.* Bogotá.

Modelo de Gestión de incidentes de seguridad CGR.

Contraloría General de la República. (2014). *SCIGC - Sistema de Control Interno y Gestión de Calidad.* Bogotá: Contraloría General de la República.

Contraloría General de la República. (2015). *Plan Estratégico 2014-2018.* Bogotá: Contraloría General de la República.

Contraloría General de la República. (2016). Manual de procedimiento para la gestiòn de incidentes. Bogotá.

Contraloría General de la República. (2016). *Programa de Fortalecimiento Institucional CGR.* Bogotá.

Contraloría General de la República. (2018). *Proyecto plan de recuperación de desastres DRP.* Bogotá: Contraloría General de la República.

CREST. (2013). *Ciber security incident response guide.* UK.

Dawn-Hiscox, T. (8 de Enero de 2018). *Critical vulnerabilities found in Dell EMC, VMware storage devices.* Obtenido de http://www.datacenterdynamics.com/content-tracks/security-risk/critical-vulnerabilities-found-in-dell-emc-vmware-storage-devices/99554.fullarticle

ENISA. (2018). *CSIRT Services.* Obtenido de https://www.enisa.europa.eu/topics/csirt-cert-services

Forum of Incident Response and Security Teams. (2018). *FIRST CSIRT Framework.* Obtenido de https://www.first.org/education/csirt_service-framework_v1.1

Gartner, Inc. (03 de Agosto de 2016). *Magic Quadrant for x86 Server Virtualization Infrastructure.* Obtenido de https://www.gartner.com/doc/3400418/magic-quadrant-x-server-virtualization

Goverment of Canada. (2013). *Ciber incident management framework for canada.* Canada.

Graz University of Technology. (2018). *Meltdown and spectre*. Obtenido de https://meltdownattack.com/

Huacanés Chávez, R. E. (Octubre de 2016). *Implementación de la norma ISO-IEC 27002:2013, sección "Control de acceso" para las aplicaciones informáticas de la Aseguradora del*

Modelo de Gestión de incidentes de seguridad CGR.

Sur. Quito, EEUU: Universidad de las Américas. Obtenido de http://iso27000.es/download/ControlesISO27002-2013.pdf

Hurtado Barrera, J. (2000). *Metodología de la investigación holística.* Caracas: Fundación Sypal.

International Organization for Standardization . (2013). *ISO/IEC 27001:2013(en).* Obtenido de https://www.iso.org/obp/ui/

International Organization for Standardization. (2016). *ISO/IEC 27035-2:2016(en).* Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-2:ed-1:v1:en

International Organization for Standardization and IEC. (2016). *ISO/IEC 27035-1: Principles of incident management.* Suiza: ISO.

International Organization for Standardization and IEC. (2016). *ISO/IEC 27035-2: Guidelines to plan and prepare for incident response.* Suiza.

iso27000.es. (Octubre de 2013). *iso27000.es- El portal del ISO 27001 en español.* Obtenido de http://iso27000.es/download/ControlesISO27002-2013.pdf

ISOTool Excellence. (2017). *Blog SGSI.* Obtenido de http://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/

LITSG, LLC. (2018). *Hyper-V Consulting.* Obtenido de http://www.litsg.com/technical-services/virtualization/hyper-v/

Lowe, S. (2011). *Mastering vmware vsphere 5.* sybex.

Microsoft Corporation. (2018). *¿Qué es Virtualización?* Obtenido de https://azure.microsoft.com/es-es/overview/what-is-virtualization/

Ministerio de Tecnologías de la Información y las Comunicaciones. (2017). *Modelo Nacional de Gestión del Riesgo de Seguridad Digital.* Bogota: Gobierno de Colombia.

Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC. (2015). *Decreto 1078 de 2015.* Bogotá.

MINTIC. (9 de 11 de 2016). Guía para la gestión y clasificación de incidentes de seguridad de la información. Bogotá, Cundinamarca, Colombia.

MITRE Corporation. (16 de Diciembre de 2016). *Vulnerability Details : CVE-2016-4443.* Obtenido de https://www.cvedetails.com/cve/CVE-2016-4443/

MITRE Corporation. (19 de Septiembre de 2017). *Vulnerability Details : CVE-2017-8713.* Obtenido de https://www.cvedetails.com/cve/CVE-2017-8713/

MITRE Corporation. (mayo de 2018). *CVE - Dell: products and vulneralities.* Obtenido de https://www.cvedetails.com/vendor/2234/Dell.html

MITRE Corporation. (2018). *CVE - HP: 3par Service Processor Sp-Vulnerability Statistics* . Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-10/product_id-32533/year-2015/opginf-1/HP-3par-Service-Processor-Sp.html

MITRE Corporation. (2018). *CVE- Vmware : Security Vulnerabilities.* Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-252/Vmware.html

MITRE Corporation. (05 de 2018). *CVE: Microsoft Windows Server - Security Vulnerabilities* . Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-10784/Microsoft-Windows-Server.html

MITRE Corporation. (2018). *CVE: Microsoft Windows Server - Vulnerability Statistics* . Obtenido de https://www.cvedetails.com/product/10784/Microsoft-Windows-Server.html?vendor_id=26

MITRE Corporation. (05 de 2018). *CVE: Redhat Enterprise Linux - Security Vulnerabilities* . Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-25/product_id-78/Redhat-Enterprise-Linux.html

MITRE Corporation. (2018). *CVE: Redhat- Enterprise Linux- Vulnerability Statistics* . Obtenido de https://www.cvedetails.com/product/78/Redhat-Enterprise-Linux.html?vendor_id=25

MITRE Corporation. (mayo de 2018). *CVE-Dell : Security Vulnerabilities* . Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-2234/Dell.html

MITRE Corporation. (2018). *HP : Security Vulnerabilities.* Obtenido de https://www.cvedetails.com/vulnerability-list/vendor_id-10/cvssscoremin-7/cvssscoremax-7.99/HP.html

Modelo de Gestión de incidentes de seguridad CGR.

MITRE Corporation. (2018). *HP : Vulnerability Statistics* . Obtenido de https://www.cvedetails.com/vendor/10/HP.html

MITRE Corporation. (2018). *Resumen de vulnerabilidades VMware.* Obtenido de https://www.cvedetails.com/vendor/252/Vmware.html

Moriche, D. P. (2016). *Virtualización de servidores con Vmware Vsphere 6.* España: Intitución Educativa Superior Castelar.

Murugesan, S., & Bojanova, I. (2016). *Encyclopedia of cloud computing.* Reino unido: Wiley.

National Institute of Standards and Technology. (2012). *NIST 800-61r2: Computer security incident handling guide.* EEUU.

National Institute of Standards and Technology. (2017). *Framework for improving critical infrastructure cybersecurity* . EEUU.

Nieves, A. C. (2017). *Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013.* Bogotá: IU Politécnico Grancolombiano.

Nutanix. (febrero de 2018). *gartner-magic-quadrant-for-hyperconverged-systems*. Obtenido de https://www.nutanix.com/go/gartner-magic-quadrant-for-hyperconverged-systems.php

Pardo Cuenca, M. G. (2015). *Modelo de Gestión de Seguridad de seguridad de la información para la universidad nacional de loja basado en la norma ISO/IEC 27001.* Loja-Ecuador: Universidad Nacional de Loja.

Pohorecki, G. (31 de Mayo de 2017). *Komunity Komand.* Obtenido de https://komunity.komand.com/learn/article/nist-sp-800-61-and-isoiec-27035-attempt-of-short-comparison/

Policía Nacional. (2017). *informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.* Bogotá: caivirtual.policia.gov.co.

Preittigun, A., Chantatub, W., & Vatanasakdakul, S. (Diciembre de 2012). A Comparison between IT Governance Research and Concepts in COBIT 5. *IRACST- International Journal of Research in Management & Technology (IJRMT)*, pág. 10.

Presidencia de la República. (2011). *Ley 1474 de 2011 - Estatuto anticorrupción.* Colombia.

Modelo de Gestión de incidentes de seguridad CGR.

Presidencia República de Colombia. (2000). *Decreto 267 de 2000. por el cual se dictan normas sobre organización y funcionamiento de la Contraloría General de la República, se establece su estructura orgánica, se fijan las funciones de sus dependencias y se dictan otras disposiciones.* Bogota: República de Colombia.

Rapid7. (14 de Marzo de 2017). *Microsoft CVE-2017-0075: Hyper-V Remote Code Execution Vulnerability*. Obtenido de https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0075

Red Hat Enterprise. (2012). *Technical update KVM and Red. Hat Enterprise Virtualization (RHEV).* Obtenido de https://www.slideshare.net/sshaaf/technical-update-kvm-and-red-hat-enterprise-virtualization-rhev

Red Hat, Inc. (13 de Julio de 2017). *CVE-2017-11334*. Obtenido de https://access.redhat.com/security/cve/cve-2017-11334

Red Hat, Inc. (05 de Septiembre de 2017). *CVE-2017-14167*. Obtenido de https://access.redhat.com/security/cve/cve-2017-14167

Red Hat, Inc. (11 de Octubre de 2017). *CVE-2017-15289*. Obtenido de https://access.redhat.com/security/cve/cve-2017-15289

Red Hat, Inc. (03 de Enero de 2018). *CVE-2017-5715*. Obtenido de https://access.redhat.com/security/cve/cve-2017-5715

Registro de Direcciones de Internet para América Latina y el Caribe - LACNIC. (2011). *Proyecto AMPARO - Manual de gestión de incidentes de seguridad informática.* LACNIC.

Rolandi, A. (12 de Octubre de 2016). *Windows Server - Introducción, Historia y Actualidad.* Obtenido de https://prezi.com/vetwcdobj6dk/windows-server-introduccion-historia-y-actualidad/

Sanchez Crespo, L. E. (2006). La gestión de la seguridad de los sistemas de información: pasado, presente y futuro. *Revista Base Informática.*

Silberschatz, A., Baer Galvin, P., & Gagne, G. (2014). *Operating System Concepts.* EEUU: Wiley.

Silva, M. (2015). *Sistemas operativos.* Buenos Aires: Alfaomega editores.

Statista.inc. (2018). *Cuota de mercado mundial de sistemas operativos según instalaciones a enero de 2017*. Obtenido de https://es.statista.com/estadisticas/576870/cuota-de-mercado-mundial-de-los-sistemas-operativos/

Sun Tzu. (2012). *El arte de la guerra.* (L. Droznes, Trad.) Bubok.

Symantec Corporation. (8 de Agosto de 2017). *Microsoft Windows Hyper-V CVE-2017-8664 Remote Code Execution Vulnerability*. Obtenido de https://www.symantec.com/security-center/vulnerabilities/writeup/100085

Symantec Corporation. (Marzo de 2017). Obtenido de Microsoft Windows Hyper-V CVE-2017-0109 Remote Code Execution Vulnerability: https://us.norton.com/online-threats/microsoftwindowshyper-vcve-2017-0109remotecodeexecution-96644-vulnerability.html

Symantec Corporation. (11 de Abril de 2017). *Microsoft Windows Hyper-V CVE-2017-0180 Remote Code Execution Vulnerability*. Obtenido de https://www.symantec.com/security-center/vulnerabilities/writeup/97444

Townsend, K. (14 de Febrero de 2018). *Nine Remotely Exploitable Vulnerabilities Found in Dell EMC Storage Platform.* Obtenido de https://www.securityweek.com/nine-remotely-exploitable-vulnerabilities-found-dell-emc-storage-platform

VmWare Inc. (2018). *¿Qué es la infraestructura hiperconvergente (HCI)?* Obtenido de https://www.vmware.com/co/products/hyper-converged-infrastructure.html

VMWare Inc. (2018). *Virtualización de VMWare*. Obtenido de https://www.vmware.com/co/solutions/virtualization.html

Apéndice A. Modelo Encuesta a Funcionarios de la CGR.

El siguiente corresponde al formulario de encuesta utilizado con el fin de determinar las aplicaciones de mayor criticidad en la entidad. Los resultados obtenidos conformaron la base para la elaboración del análisis realizado a la altura del capítulo 2.

Encuesta proyecto modelo de gestión de incidentes							
Nombre del servidor o aplicativo:					**Dirección IP:**		
Selecciones las respuestas de acuerdo a su perfil como administrador y al conocimiento que tiene sobre la aplicación.							**Notas**
¿Que tan importante es el aplicativo para el cumplimiento de la misión de la entidad?	poco importante		Importante		Muy importante		
¿Qué tan extenso sería el impacto por el fallo del servicio por más de 1 semana?	Local		Nacional		Internacional		
¿A qué usuarios les presta servicio esta servidor o aplicativo?	Internos		Externos				
¿Cuanto tiempo máximo considera que el servidor o aplicativo puede estar fuera de línea sin que se produzca una afectación grave?							
¿Con que frecuencia se realiza Backups de la información del servidor o aplicativo?							
¿Afectaría una falla en el servicio prestado por el servidor o aplicativo la imagen de la entidad?							
¿Cuántos usuarios diariamente acceden a la aplicación o servicio?							
Evalúe de 1 a 5 las siguientes situaciones, siendo 5 el valor de más relevancia o más grave.							
Pérdida de información correspondiente a 1 día							
Pérdida de información correspondiente a 3 días							
Pérdida de información correspondiente a 5 días o más							
Apropiación de información por parte de terceros							
Modificación de información por parte de terceros							
Notas adicionales:							

Figura 48. Encuesta sobre relevancia de aplicativos y/o servidores para la entidad. Fuente: Elaboración propia.

Apéndice B. Acuerdo de Confidencialidad.

El siguiente corresponde una adaptación del formato de acuerdo de confidencialidad utilizado por la contraloría general de la república.

ACUERDO DE CONFIDENCIALIDAD

El suscrito a saber: _____ domiciliado en **Bogotá**, identificado con _____quien obra en calidad de _____, manifiesta su voluntad de asumir, de manera unilateral, el presente compromiso, teniendo en cuenta las siguientes consideraciones:

PRIMERO: Que el funcionario Víctor Ferley Perea Asprilla adelanta sus estudios de maestría en Ciberseguridad y Ciberdefensa con la escuela Superior de guerra, para lo cual se requiere la elaboración de un "Proyecto de grado" como requisito para su graduación, lo cual puede generar acceso a información relevante y/o de reserva de la entidad.

SEGUNDO: Que se entiende que parte de la información a la cual tendrá acceso por causa o con ocasión de la ejecución de las actividades requeridas para adelantar el proyecto de grado, se encuentra sujeto a confidencialidad por tratarse de actividades relacionadas con el control fiscal.

CLÁUSULA PRIMERA. COMPROMISOS ASUMIDOS.

La Escuela Superior de Guerra, mediante suscripción del presente documento, asume los siguientes compromisos:

1. Mantener en confidencialidad y no divulgar LA INFORMACIÓN CONFIDENCIAL revelada por la CONTRALORIA GENERAL DE LA REPÚBLICA o por terceros formalmente designados para el efecto, que conozca o llegare a conocer en desarrollo y ejecución de las actividades que le competan por causa o con ocasión del proyecto de grado.

2. Mantener en confidencialidad y no divulgar ni utilizar, en provecho propio o de terceros y para fines distintos a los previstos, la información que le sea entregada directamente por

LA CONTRALORIA GENERAL DE LA REPÚBLICA y/o los funcionarios designados, prohibiéndose la divulgación inclusive para fines académicos.

3. Mantener en confidencialidad y no divulgar la información protegida por derechos de autor o por secreto industrial de acuerdo a la normatividad vigente y que haga parte de LA INFORMACIÓN CONFIDENCIAL.

4. Reconocer que el recibo de LA INFORMACIÓN CONFIDENCIAL no concede, ni expresa implícitamente, autorización, permiso o licencia de uso de marcas, patentes, derechos de autor, o de cualquier otro derecho de propiedad industrial o intelectual de LA CONTRALORIA GENERAL DE LA REPÚBLICA.

5. Suscribir, con antelación a la revelación de LA INFORMACIÓN CONFIDENCIAL, los Acuerdos de Confidencialidad que se ajustan a todo lo dispuesto en el presente Acuerdo con todos sus Docentes, empleados y/o familiares de los mismos, contratistas, subcontratistas, proveedores y demás personas naturales o jurídicas que haya involucrado, involucre o llegare a involucrar en la ejecución de las actividades que le correspondan para el cumplimiento del Proyecto de grado.

6. La escuela superior de Guerra mantendrá una lista de usuarios de LA INFORMACIÓN CONFIDENCIAL que le será entregada cuando ello lo amerite.

7. Utilizar única y exclusivamente LA INFORMACIÓN CONFIDENCIAL que conozca o llegare a conocer, en desarrollo y ejecución de lo que le competa en relación con el Proyecto de grado.

8. Adoptar y mantener mecanismos internos de seguridad adecuados para proteger la confidencialidad de toda la información que conozca o llegare a conocer en desarrollo del Proyecto de grado.

9. No usar LA INFORMACIÓN CONFIDENCIAL de modo que pueda ser de alguna manera, directa o indirectamente, perjudicial para los intereses de la CONTRALORIA GENERAL DE LA REPÚBLICA.

10. No acceder, copiar, reproducir, distribuir o transmitir por ningún medio conocido o por conocer LA INFORMACIÓN CONFIDENCIAL, en todo o en parte, sin previo y escrito consentimiento de LA CONTRALORIA GENERAL DE LA REPÚBLICA.

11. Cumplir con la confidencialidad en las mismas condiciones y formas, y con el mismo cuidado con que realiza la protección de la información confidencial.

Modelo de Gestión de incidentes de seguridad CGR.

Nota 1: Confidencialidad comprende toda la información divulgada por cualquiera de las partes ya sea en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otra forma tangible que le sea entregada al contratista.

Nota 2: el acuerdo de confidencialidad hace parte integral de las actividades requeridas para realizar el Proyecto de grado.

Nota 3: la realización del Proyecto de grado no obliga ni compromete a la LA CONTRALORIA GENERAL DE LA REPÚBLICA con la adquisición o pago de productos u honorarios de ninguna índole en la que incurra el suscrito por motivos de las actividades desarrolladas.

_____

ESDEGUE

Nombre:

Documento Identidad

Fecha

_____