Modelo de madurez de ciber-resiliencia organizacional

Gloria Patricia Arcila Arias

Trabajo de grado para optar al título profesional:

Maestría en Ciberseguridad y Ciberdefensa

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

2020

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

Modelo de madurez de ciber-resiliencia organizacional

Gloria Patricia Arcila Arias

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá - Colombia
2020

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

Modelo de madurez de ciber-resiliencia organizacional

Director

Dr. Carlos Alfonso Castañeda Marroquín

Maestría en Ciberseguridad y Ciberdefensa
Trabajo de grado
Bogotá - Colombia
2020

Nota de aceptación:

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá D.C., marzo de 2020

Agradecimientos

Agradezco primero que todo a Dios por ser esa luz que cada día ilumina mi camino con su sabiduría. A mi director de proyecto de grado, por regalarme espacios de su tiempo valioso para orientarme en el desarrollo de este trabajo. A mis compañeros y profesores de la Escuela Superior de Guerra, por todo el aprendizaje recibido. Al Ministerio de Tecnologías de la Información y Comunicaciones de Colombia por su patrocinio económico y finalmente, sin ser menos importante, a mi querida Empresas Públicas de Medellín (EPM), que me proporcionó el tiempo y el apoyo económico para poder desplazarme a Bogotá y participar de las sesiones de estudio durante los dos años que duró la maestría.

Dedicatoria

A mis hijas Sara Victoria, Susana Patricia y Sandra Isabel, y a mi nieta Violeta. Ellas son lo más lindo que la vida me ha regalado y la mayor motivación para seguir adelante con todos mis sueños.

Resumen

La ciber-resiliencia es el desarrollo de capacidades que le permiten a las organizaciones estar preparadas para afrontar ataques cibernéticos que puedan poner en riesgo la continuidad del negocio. Las capacidades clave que una organización debería desarrollar para ser ciber-resiliente son las de anticipar, resistir, recuperarse y evolucionar. Estas capacidades no se desarrollan de la noche a la mañana; por el contrario, su desarrollo requiere de la implementación de prácticas organizacionales que se fortalecen a medida que la organización va madurando.

En este trabajo se plantea el reto de identificar la forma como las capacidades organizacionales de ciber-resiliencia evolucionan de manera natural, así como las prácticas que se pueden evidenciar para determinar el nivel de madurez de ciber-resiliencia de una organización. Como resultado de este trabajo, se propone un modelo de madurez de ciber-resiliencia organizacional que tiene como fundamento técnico los principios de diseño de ciber-resiliencia definidos por la corporación MITRE (Massachusetts Institute of Technology Research & Engineering) (Deborah Bodeau & Graubart, 2017), y como referencia de estructuración del modelo, los niveles de madurez planteados en el modelo CMMI (Capability Maturity Model Integration) para desarrollo (SEI, 2010). Así mismo, el modelo comparativo se basó en el modelo de madurez de continuidad del negocio (BCMM, 2012).

Para validar el modelo de madurez de ciber-resiliencia organizacional propuesto, se elabora una herramienta de evaluación que es aplicada a cinco empresas del sector eléctrico. Una vez aplicada la herramienta de evaluación, se concluyó que el modelo es válido para evaluar rápidamente el estado de preparación de las organizaciones para afrontar ataques cibernéticos del tipo amenazas persistentes avanzadas.

Palabras clave: capacidades organizacionales, modelos de madurez, resiliencia, ciberseguridad, ciber-resiliencia, ataques cibernéticos, infraestructura crítica.

Abstract

Cyber-resilience is the development of capabilities that allow organizations to be prepared to face cyber-attacks that may jeopardize business continuity. The key capabilities that an organization should develop to be cyber-resilient are to anticipate, resist, recover and evolve. These capabilities do not develop overnight; on the contrary, their development requires the implementation of organizational practices that are evolving as the organization matures.

In the work carried out, the challenge of identifying the way in which the cyber-resilience organizational capacities evolve naturally, as well as the practices that can be evidenced to determine the level of cyber-resilience maturity of an organization and reflect it in a model. As a result of the work carried out, an organizational cyber-resilience maturity model was defined, whose technical basis is the cyber-resilience design principles defined by MITRE (Bodeau & Graubart, 2017) and as a model structuring reference, the Maturity levels set out in the CMMI model for development (SEI, 2010), likewise, the comparative model was based on the maturity model of business continuity (BCMM, 2012).

To validate the maturity model of organizational cyber-resilience, an evaluation tool is developed that applies to five companies in the electricity sector. Once the assessment tool was applied, it was concluded that the model is valid to quickly assess the organizations' readiness to face cyber-attacks of the type of persistent advanced threats.

Keywords: Organizational capacities, models of maturity, resilience, cybersecurity, cyber-resilience, cyber-attacks, critical infrastructure.

Tabla de contenido

Índice de tablas

Índice de figuras

Metodología

En este trabajo se utiliza un enfoque metodológico de investigación cualitativa con alcance descriptivo. En este tipo de enfoque, la revisión de la literatura se realiza no solo en la etapa inicial, sino en cualquier etapa del estudio, desde el planteamiento del problema hasta la elaboración del reporte de resultados. La literatura es útil para detectar conceptos clave que no se habían considerado en el planteamiento inicial del proyecto, así como para nutrirse de ideas en cuanto a los métodos de recolección de datos y análisis, para conocer cómo les han servido a otros (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2010).

Con el propósito de establecer el estado del arte se realizaron dos procesos generales: a) la búsqueda, selección, organización y disposición de fuentes de información para un tratamiento racional; b) la integración de la información a partir del análisis de los mensajes contenidos en las fuentes, que corresponde a la dimensión hermenéutica del proceso, y muestra los conceptos básicos unificadores (Londoño, Maldonado, & Calderón, 2014).

La selección de las capacidades clave a desarrollar para lograr la ciber-resiliencia organizacional se hace con base en la información recopilada en el estado del arte, donde se identifica que las capacidades de anticipar, resistir, recuperarse y evolucionar son las requeridas por las organizaciones para ser ciber-resilientes (Suárez, Gómez-Hidalgo, & Alvárez-Peláez, 2014). Estas capacidades se soportan en unos principios de diseño de ciber-resiliencia que son implementados en cuatro disciplinas clave: resistencia y supervivencia, ciberseguridad, amenazas persistentes avanzadas y evolución (Deborah Bodeau & Graubart, 2017).

La identificación de las prácticas que la organización implementa para ser ciber-resiliente se hizo teniendo en cuenta la definición de cada principio de diseño de ciber-resiliencia y recopilando información acerca de las diferentes metodologías y técnicas que permiten su implementación. Una vez identificadas las prácticas, se procedió a asociarlas a cada capacidad y disciplina de ciber-resiliencia.

Para la estructuración del modelo, se tomaron como referencia los niveles de madurez planteados por en el modelo CMM para desarrollo: 1-Inicial, 2-Gestionado, 3-Definido, 4-

Gestionado Cuantitativamente y 5-En Optimización (SEI, 2010). De igual manera, el modelo comparativo fue basado en el modelo de madurez de continuidad del negocio (BCMM, 2012), donde se pueden identificar tres estados en los cuales pueden estar las organizaciones: "En riesgo" para niveles de madurez 1 y 2, "Ejecutante competente" para niveles 3 y 4, y "El mejor de la clase" para nivel 5 de madurez. Finalmente, se diseñó una herramienta de evaluación que permitió validar el modelo.

Introducción

Las organizaciones en el mundo están expuestas a ataques cibernéticos que pueden poner en riesgo la continuidad del negocio, por lo que es necesario que se adapten a los nuevos cambios tecnológicos, a la protección de sus sistemas de información, de su infraestructura crítica y los servicios prestados por medio de las redes, y todo ello en un marco en constante evolución y revisión, características que incorpora y trabaja de forma específica la ciber-resiliencia (Suárez et al., 2014). La ciber-resiliencia es la capacidad de un proceso, negocio, organización o nación para anticipar, resistir, recuperarse y evolucionar para mejorar sus capacidades frente a condiciones adversas, estrés, o ataques a los recursos cibernéticos que se necesitan para funcionar (CERTSI, n.d.). Las capacidades representan un patrón de acción confiable, efectivo frente a variadas situaciones problemáticas, y reproducido en diferentes momentos en el tiempo (Dávila, 2013).

El desarrollo de la capacidad de ciber-resiliencia prepara a las organizaciones para dar respuestas rápidas a los ataques cibernéticos, evitando la interrupción prolongada de los servicios que prestan y el continuar ejecutando las funciones críticas para la misión organizacional, aun cuando se esté afrontando un ataque cibernético. Las capacidades organizacionales se pueden mejorar de forma incremental, por lo que se pueden identificar niveles o etapas que se caracterizan por las prácticas implementadas en los procesos organizacionales (SEI, 2010). Se plantea entonces el reto de identificar qué capacidades debe desarrollar una organización para ser ciber-resiliente, cómo evolucionan estas capacidades y qué prácticas evidencian el nivel de desarrollo de la capacidad de ciber-resiliencia organizacional.

El nivel de desarrollo de la capacidad de ciber-resiliencia organizacional puede evaluarse utilizando un modelo de madurez que permita identificar las diferentes etapas por las que una organización pasa cuando desarrolla sus capacidades, partiendo desde una etapa inicial, donde puede que apenas se haya comenzado a considerar la ciberseguridad, hasta un escenario dinámico, donde la organización es capaz de adaptarse rápidamente a los cambios en el panorama de la ciberseguridad en lo relativo a las amenazas, las vulnerabilidades, los riesgos, la estrategia económica o el cambio de las necesidades organizacionales (Rea-

Guaman, Sanchez-Garcia, Feliu, & Calvo-Manzano, 2017). Un modelo de madurez da a las organizaciones un punto de referencia con el que, además de evaluar el nivel de ciber-resiliencia en que se encuentran sus prácticas, procesos y métodos, se puede identificar la brecha existente entre el estado actual y el desarrollo deseado de su capacidad, así como un mapa de ruta de las prácticas a implementar para alcanzar el nivel de la capacidad de ciber-resiliencia organizacional deseado.

En el presente documento se tratan conceptos relacionados con las capacidades organizacionales y su evolución, los modelos de madurez organizacionales, la ciber-resiliencia como capacidad organizacional y los modelos de referencia para desarrollar las capacidades organizacionales de ciber-resiliencia. Una vez desarrollados estos conceptos, se plantean las bases para la definición del modelo de madurez, se identifican las capacidades clave de ciber-resiliencia y las prácticas que evidencian la evolución del desarrollo de estas capacidades. Finalmente, se plantea la propuesta de un modelo para evaluar el nivel de madurez de ciber-resiliencia organizacional.

En el desarrollo del trabajo se dio respuesta a los objetivos planteados al inicio de la investigación, donde se planteó como objetivo general: diseñar un modelo de madurez que oriente el desarrollo de las capacidades de ciber-resiliencia organizacional. Así mismo, se cumplieron los objetivos específicos de: analizar el estado actual de la ciber-resiliencia, identificar los elementos que apoyan el desarrollo de las capacidades de ciber-resiliencia, analizar la forma como las capacidades de ciber-resiliencia evolucionan en las organizaciones y definir una propuesta de un modelo de madurez de ciber-resiliencia organizacional.

Pregunta de investigación

La ciber-resiliencia requiere del fortalecimiento las capacidades organizacionales, mediante la implementación de buenas prácticas que preparen a las organizaciones para afrontar ataques cibernéticos, sin afectar la continuidad del negocio. Se plantea entonces el reto de identificar cuáles capacidades deben desarrollar las organizaciones para fortalecer la ciber-resiliencia, qué prácticas soportan estas capacidades y cómo contar con un patrón que les sirva de guía para evaluar y mejorar su nivel de ciber-resiliencia organizacional. Con el

propósito de plantear una alternativa para las organizaciones, se formula la pregunta de investigación: ¿Cómo estructurar una propuesta de un modelo de madurez que oriente a las organizaciones en el desarrollo de las capacidades de ciber-resiliencia?

Objetivos de la investigación

Objetivo general

Diseñar un modelo de madurez que oriente el desarrollo de las capacidades que apoyan la ciber-resiliencia organizacional.

Objetivos específicos

a) Analizar el estado actual de la ciber-resiliencia.
b) Identificar los elementos que apoyan el desarrollo de las capacidades de ciber-resiliencia.
c) Analizar la forma como las capacidades de ciber-resiliencia evolucionan en las organizaciones.
d) Definir una propuesta de un modelo de madurez de ciber-resiliencia organizacional.

1. Capacidad de ciber-resiliencia

1.1 Capacidades organizacionales y su evolución

Las capacidades organizacionales son la base para que una organización desarrolle la habilidad de realizar una actividad particular de manera confiable, o al menos mínimamente satisfactoria. Se caracterizan por ser una forma de solucionar problemas complejos, ejercidas habitualmente de manera efectiva, son confiables y mediante un proceso de aprendizaje, evolucionan en el tiempo. Las capacidades pueden también ser interpretadas como un patrón de acción confiable que muestra ser efectivo frente a variadas situaciones problemáticas, y es reproducido en diferentes momentos en el tiempo. Una capacidad organizacional no será constituida hasta que un conjunto de prácticas confiables haya tomado forma a lo largo del tiempo (Dávila, 2013).

Las capacidades evolucionan con el tiempo y dan referencia del estado de madurez de los procesos organizacionales. El estado de madurez de una organización puede medirse evaluando la evolución de sus capacidades organizacionales. El Software Engineering Institute (SEI) en su modelo CMMI (SEI, 2010), considera niveles de capacidad organizacional que permiten identificar la forma como los procesos pueden mejorar de forma incremental, planteando cuatro niveles de capacidad: 0.-Incompleto, 1.-Realizado, 2-Gestionado y 3-Definido.

El nivel de capacidad "0- Incompleto", hace referencia a un proceso que, o bien no se realiza, o se realiza parcialmente. El nivel de capacidad "1-Realizado" es un proceso que lleva a cabo el trabajo necesario para producir productos de trabajo. El nivel de capacidad "2-Gestionado" corresponde a un proceso que se planifica y ejecuta de acuerdo con la política; emplea personal cualificado que tiene los recursos adecuados para producir resultados controlados; involucra las partes interesadas relevantes; se monitorea, controla y revisa; y se evalúa la adherencia frente a la descripción del proceso. El nivel de capacidad "3-Definido" es un proceso gestionado que se adapta a partir de un conjunto de procesos estándar de la organización de acuerdo con las guías de adaptación de la organización, tiene una descripción de proceso que se mantiene y que contribuye a los activos de proceso de la organización con experiencias relativas a procesos (SEI, 2010).

1.2 Ciber-resiliencia como capacidad organizacional

La resiliencia puede definirse como una cualidad intrínseca, una característica propia de una organización que le permite enfrentarse de forma exitosa a los cambios y a los eventos tanto internos como externos. La resiliencia implica adaptación que se ha de realizar en el mínimo intervalo de tiempo, a la máxima velocidad, incluso en tiempo real, garantizando así la continuidad de las funciones esenciales y la menor pérdida de capacidades. Por lo tanto, una organización resiliente es aquella con capacidad de toma rápida de decisiones, y también la capacidad del sistema para implementar dichas decisiones. La resiliencia supone admitir que se producirán fallos, errores, y que se tienen los medios para restaurar la operación normal y asegurar los bienes y reputaciones, por lo que una forma de medir el grado de resiliencia organizacional es su capacidad de anticiparse a las crisis (Carrasco, 2015).

Las definiciones de resiliencia difieren dependiendo del alcance. La resiliencia de la infraestructura es la capacidad de reducir la magnitud y la duración de los eventos disruptivos; la efectividad de una infraestructura o empresa resiliente depende de su capacidad para anticipar, asimilar, adaptarse y recuperarse rápidamente de un evento potencialmente perjudicial. En el ámbito organizacional, la resiliencia se define como la capacidad de adaptarse al riesgo que afecta sus capacidades operativas básicas, siendo la resiliencia operacional una capacidad emergente de la gestión efectiva del riesgo operacional que es respaldada y habilitada por actividades como la seguridad y la continuidad del negocio. En el ciberespacio, la resiliencia se define como la capacidad de adaptarse a las condiciones cambiantes y prepararse para resistir y recuperarse rápidamente de una interrupción (Deborah Bodeau, Graubart, Picciotto, & McQuaid, 2011).

En el ciberespacio, la resiliencia es llamada "ciber-resiliencia", y se puede también definir como la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes (Suárez et al., 2014). La ciber-resiliencia involucra potenciar las capacidades de identificación, detección, prevención, contención, recuperación, cooperación y mejora continua, frente a las distintas ciber amenazas. Para conseguir la ciber-resiliencia, partiendo de unos objetivos, capacidades y técnicas, debemos ser capaces de medirla, de una manera eficiente, coordinada y metodológica, con el fin de garantizar que las organizaciones tienen

adoptadas unas medidas razonables que garanticen la protección de sus datos, sistemas y equipos (Suárez et al., 2014).

Para lograr la ciber-resiliencia organizacional se debe alcanzar un conocimiento real y profundo de la organización y su entorno. La gestión del riesgo, del cambio y la implementación de medidas preventivas y correctivas, incluyendo planes de continuidad del negocio y de recuperación de desastres, son herramientas que también aumentan la ciber-resiliencia organizacional. El cambio debe ser incorporado en la organización como uno de sus principios de funcionamiento. El factor humano también hace que una organización sea ciber-resiliente, partiendo de una dirección integrada a la organización, realmente informada de cada uno de los procesos que se ejecutan y con una visión global. Se hace necesario contar con un responsable de la ciber-resiliencia con voz a nivel directivo. La concienciación del personal también es un aspecto clave para lograr el compromiso de las personas. La capacidad de anticiparse a la crisis es también fundamental para lograr la ciber-resiliencia, lo que le da relevancia a los CERT y a la necesidad de potenciarlos en su capacidad proactiva y anticipatoria de amenazas, mediante labores de inteligencia. Otro aspecto destacado a considerar es la reducción de dependencias externas e internas, lo que implica que la organización ha de implementar redundancia en sus sistemas, en su personal y en sus procesos (Carrasco, 2015).

Teniendo en cuenta que los ataques cibernéticos son cada vez más sofisticados y se ha pasado de explotar vulnerabilidades conocidas a descubrir o crear nuevas vulnerabilidades, una organización ciber-resiliente debe estar preparada para afrontar amenazas persistentes avanzadas, donde el atacante es sigiloso, estratégico, evoluciona y es capaz de descubrir nuevas vulnerabilidades, desarrollando tácticas, técnicas y procedimientos para explotar las vulnerabilidades imprevistas (Deborah Bodeau & Graubart, 2017). Una Amenaza Persistente Avanzada (APT) es capaz de superar las defensas perimetrales, el control de acceso y los mecanismos de gestión de privilegios, y la detección de intrusiones, haciendo posible que el atacante mantenga su presencia a largo plazo en los sistemas objetivo del ataque. Si bien algunas fuentes restringen el término APT a los adversarios que buscan filtrar datos, el término es cada vez más utilizado para incluir adversarios avanzados que buscan la

interrupción y el debilitamiento de la efectividad de la misión de una organización (Department Of Defense United States Of America, 2013).

1.3 Modelos de madurez para medir las capacidades organizacionales

Para evaluar el nivel actual de capacidad de sus prácticas, procesos, métodos, así como para establecer objetivos y prioridades para la mejora, las organizaciones pueden apoyarse en modelos de madurez. Un modelo de madurez puede definirse como un conjunto de características, atributos, indicadores o patrones que representan la capacidad y progresión de una disciplina en particular (Rea-Guaman et al., 2017). Así mismo, un modelo de madurez puede orientar a la organización en la implementación de buenas prácticas, ofreciendo un punto de partida y un camino de mejoramiento evolutivo que permite pasar de procesos inconsistentes a procesos maduros (Pérez-Mergarejo, Pérez-Vergara, & Rodríguez-Ruíz, 2014).

Según el SEI, un nivel de madurez es una plataforma evolutiva definida para la mejora de los procesos de la organización y consta de prácticas específicas que diferencian un proceso de otro y prácticas genéricas que aplican a varios procesos organizacionales, la implementación de estas prácticas permite mejorar el rendimiento global de la organización. Cada nivel de madurez desarrolla un subconjunto importante de procesos de la organización, preparándola para pasar al siguiente nivel de madurez. Cada nivel de madurez específico se mide mediante el logro de metas específicas y genéricas que dan cuenta de la implementación de las prácticas que aplican al proceso. El SEI en su modelo CMMI (Capability Maturity Model Integration) contempla cinco niveles de madurez de los procesos: 1-Inicial, 2-Gestionado, 3-Definido, 4-Gestionado Cuantitativamente, y 5-En Optimización (SEI, 2010).

En el nivel de madurez "1-Inicial", el SEI indica que los procesos son generalmente *ad hoc* y caóticos, sin que la organización proporcione un entorno estable para dar soporte a los procesos. En el nivel de madurez "2-Gestionado" se empieza a evidenciar la planificación y ejecución de acuerdo con las políticas, el empleo de personal cualificado y recursos adecuados para producir resultados controlados; involucra a las partes interesadas relevantes;

se monitorea, controla y revisa; se evalúa la adherencia a la descripción del proceso. En el nivel de madurez "3-Definido", los procesos están caracterizados, comprendidos y se describen en estándares, procedimientos, herramientas y métodos. En comparación con el nivel 2, el nivel 3 describe el proceso más rigurosamente, se establece claramente el propósito, entradas, criterios de entradas, actividades, roles, medidas, etapas de verificación, salidas y criterios de salidas. En el nivel de madurez "4-Gestionado Cuantitativamente", se establecen objetivos cuantitativos para la calidad y el rendimiento del proceso, utilizados como criterios para la gestión. Estos objetivos se basan en las necesidades del cliente, usuarios finales, organización e implementación del proceso. En el nivel de madurez "5-En Optimización", la organización mejora continuamente sus procesos basándose en una comprensión cuantitativa de sus objetivos de negocio y las necesidades de rendimiento (SEI, 2010).

En este capítulo hemos identificado aspectos clave relacionados con la capacidad de ciber-resiliencia y los modelos de madurez. Para la definición de una propuesta de un modelo de madurez de ciber-resiliencia organizacional, resulta imperativo realizar una revisión de la literatura relacionada con modelos de referencia que sirvan como base para identificar los elementos clave a tener en cuenta para la definición del modelo.

2. Modelos de referencia para desarrollar las capacidades de ciber-resiliencia organizacional

2.1 Marco de ingeniería de ciber-resiliencia

El marco de ingeniería de ciber-resiliencia fue propuesto por MITRE (Massachusetts Institute of Technology Research & Engineering), organización sin ánimo de lucro que provee ingeniería de sistemas, investigación y desarrollo, y soporte sobre tecnologías de la información al gobierno de los Estados Unidos de América. En su marco, el MITRE identifica las metas, objetivos y prácticas de ciber-resiliencia; un modelo de amenazas; capas o dominios de arquitectura a los que se podrían aplicar prácticas de ciber-resiliencia; aspectos del costo a considerar como parte del análisis de la compensación de la estrategias e implementación de alternativas. Las metas consideradas en el marco son: anticipar, resistir, recuperar y evolucionar. La meta de anticipar busca mantener un estado de preparación informada con el fin de evitar compromiso de las funciones críticas del negocio cuando se presente un ataque cibernético. La meta de resistir implica que continúen ejecutándose las funciones esenciales del negocio, a pesar de la ejecución exitosa de un ataque por un adversario. La meta de recuperar es restaurar las funciones críticas del negocio en la mayor medida de lo posible luego de un ataque cibernético. La meta de evolucionar es la implementación de cambios que permitan minimizar los impactos adversos de los ataques reales o previstos (Deborah Bodeau et al., 2011).

Para lograr las metas de ciber-resiliencia, el marco establece ocho objetivos: entender, preparar, prevenir, continuar, restringir, reconstituir, transformar y rediseñar. En la tabla 1 podemos observar la relación entre las metas de ciber-resiliencia y los objetivos del marco.

Tabla 1

Metas de Ciber-resiliencia y objetivos

Meta	Objetivos
Anticipar	Entender, Preparar, Prevenir
Resistir	Entender, Continuar, Restringir
Recuperar	Entender, Continuar, Reconstituir
Evolucionar	Entender, Transformar, Rediseñar

Fuente: Deborah Bodeau et al. (2011). Traducción propia.

El objetivo de entender busca conocer al adversario y las técnicas de ataques que puede utilizar para atacar, así mismo conocer en detalle el comportamiento normal de los recursos cibernéticos, de tal forma que se puedan detectar cambios que indiquen un ataque en curso. El objetivo de preparar consiste en definir un conjunto de acciones a realizar para enfrentar ataques cibernéticos previstos, considerando tanto los recursos cibernéticos, como la capacitación y entrenamiento del personal. El objetivo de prevenir es evitar la ejecución exitosa de un ataque mediante la aplicación de principios y prácticas de ingeniería de seguridad de sistemas de información para implementar controles de seguridad. El objetivo de continuar es permitir que las funciones críticas del negocio tengan un grado aceptable de disponibilidad durante un ataque. El objetivo de restringir es limitar el daño que un ataque pueda hacer a los recursos cibernéticos con acciones como el aislamiento de los recursos comprometidos. El objetivo de reconstituir es volver a desplegar los recursos cibernéticos que fueron afectados por un ataque, de tal forma que las funciones críticas del negocio continúen. El objetivo de transformar es cambiar aspectos del comportamiento organizacional en respuesta a ataques cibernéticos anteriores, actuales o potenciales, minimizando la exposición de los recursos cibernéticos. El objetivo de rediseñar es modificar la arquitectura empresarial para aplicar prácticas de ciber-resiliencia para abordar los cambios previstos a largo plazo en las capacidades, la intención o la orientación del

adversario, e incorporar tecnologías emergentes en formas que mejoren la ciber-resiliencia (Bodeau et al., 2011).

Otro componente del marco son las prácticas de ciber-resiliencia que permiten lograr los objetivos, las cuales se aplican en la organización en la arquitectura, en el diseño de las funciones críticas del negocio y los recursos cibernéticos. En la tabla 2, se resumen las prácticas de ciber-resiliencia.

Tabla 2

Prácticas de ciber-resiliencia

Práctica	Descripción
Respuesta adaptativa	Tomar acciones en respuesta a un ataque según las características de este.
Monitoreo analítico	Recopilar y analizar datos de manera continua y de manera coordinada para identificar posibles vulnerabilidades, actividades adversas y daños.
Defensa coordinada	Administrar de manera adaptativa y coordinada múltiples mecanismos distintos para defender los recursos críticos contra actividades adversas.
Engaño	Uso de técnicas como ofuscamiento y desinformación para confundir al adversario.
Diversidad	Usar un conjunto heterogéneo de tecnologías (hardware, software, firmware, protocolos) para minimizar el impacto de los ataques y forzar a los adversarios a atacar múltiples tipos de tecnologías.
Posicionamiento dinámico	Utilizar el procesamiento distribuido y la reubicación dinámica de activos y sensores críticos, impidiendo la capacidad del adversario para localizar, eliminar o corromper los activos críticos del negocio y requiriendo que el adversario dedique más tiempo y esfuerzo para encontrar los activos críticos.
Representación dinámica	Una representación es dinámica si puede reflejar cambios en el estado o el comportamiento. Las representaciones dinámicas apoyan la conciencia situacional y, por lo tanto, informan la respuesta adaptativa y la defensa coordinada.
No persistencia	Retener la información, los servicios y la conectividad por un tiempo limitado, reduciendo así la oportunidad de un adversario de explotar vulnerabilidades y establecer un punto de apoyo persistente.

Práctica	Descripción
Restricción de privilegios	Restringir los privilegios requeridos para usar los recursos cibernéticos, y los privilegios asignados a los usuarios y entidades cibernéticas, según el tipo (s) y el grado (s) de criticidad y confianza respectivamente, para minimizar las posibles consecuencias de las actividades adversas.
Reordenación	Alinear los recursos cibernéticos con los aspectos centrales de las funciones críticas del negocio, reduciendo así la superficie de ataque.
Redundancia	Mantener múltiples instancias protegidas de recursos críticos (información y servicios), que sirven como copias de seguridad en el caso de daños localizados en un recurso y brindan soporte contra sobretensiones cuando sea necesario para soportar cargas pico, fallas y conmutaciones por error inesperadas.
Segmentación	Separar (lógica o físicamente) componentes basados en su tipo o criticidad, para limitar la propagación o daño de explotaciones exitosas, reduciendo la superficie de ataque y permitiendo la colocación de defensas más rentables en función de la criticidad de los recursos.
Integridad demostrada	Asegurarse de que los servicios críticos, los almacenes de información, los flujos de información y los componentes no hayan sido corrompidos por un adversario.
Imprevisibilidad	Hacer cambios con frecuencia y al azar, no solo en respuesta a las acciones del adversario, haciendo más difícil para un adversario predecir el comportamiento y aumentando la posibilidad de que se detecten acciones adversas.

Fuente: Deborah Bodeau et al.(2011).

2.2 Principios de diseño de ciber-resiliencia

Según el MITRE, un diseño organizacional ciber-resiliente necesariamente debe considerar unos principios que apalanquen el logro de esta capacidad. Los principios de diseño de ciber-resiliencia son la sumatoria de principios de diseño relacionados con la seguridad, la resiliencia, la adaptación y evolución y la supervivencia. Un principio de diseño de ciber-resiliencia puede guiar los requisitos, la arquitectura, la elección de soluciones técnicas específicas, la forma como una solución es implementada o integrada, así como la definición de procesos y procedimientos. Los principios de diseño pueden caracterizarse como: 1)

estratégicos para ser aplicados en el proceso de ingeniería de sistemas para guiar la dirección de los análisis de ingeniería, y 2) estructurales, que afectan directamente la arquitectura y el diseño (Ricci, Rhodes, & Ross, 2014).

Los principios de diseño estratégicos de ciber-resiliencia se describen a continuación:

- ***Centrarse en los activos críticos comunes***. La estrategia de centrarse primero en los activos que son críticos y comunes; luego en los críticos o comunes. El enfoque en los activos críticos, los recursos valorados por su importancia para el cumplimiento de la misión, ha sido durante mucho tiempo fundamental para la planificación de contingencias, la continuidad de las operaciones y la resiliencia operacional, así como para el análisis de la seguridad operacional. Los activos que son comunes a múltiples misiones o funciones de negocios son objetivos potenciales de alto valor para los ciber atacantes, ya sea porque esos activos son críticos o porque su compromiso aumenta las opciones de movimiento lateral o persistencia de los atacantes (Deborah Bodeau & Graubart, 2017).
- ***Soportar agilidad y diseñar para adaptarse.*** El panorama de amenazas no solo cambia a medida que los adversarios evolucionan, también lo hacen las tecnologías y las formas en que los individuos y las organizaciones las usan. De ahí la necesidad tanto de la agilidad como de la adaptabilidad como parte de la estrategia de gestión de riesgos, en respuesta al supuesto de estructura de riesgo de que se producirán cambios imprevistos en el entorno de amenazas, técnico y operacional a lo largo de la vida útil de un sistema (Deborah Bodeau & Graubart, 2017).
- ***Reducción de la superficie de ataque***. Una gran superficie de ataque es difícil de defender y requiere un esfuerzo continuo para monitorear, analizar y responder ante anomalías. La reducción de las superficies de ataque permite que los recursos o entornos puedan ser monitoreados y defendidos de manera más efectiva. La superficie de ataque también puede incluir los entornos operativos, desarrollo y mantenimiento que un adversario puede alcanzar y que podrían ser vulnerables. Adicionalmente, la superficie de ataque puede incluir las personas y procesos, así como la cadena de suministro (Deborah Bodeau & Graubart, 2017).

- ***Dudar de la fiabilidad de todos los recursos técnicos***. Los sistemas y sus componentes, que van desde chips hasta módulos de software y servicios en ejecución, pueden verse comprometidos por períodos prolongados sin detección. De hecho, es posible que nunca se detecten algunos compromisos. Por lo tanto, la suposición de que algunos recursos del sistema se han comprometido es prudente. Este principio de diseño implica la necesidad de analizar cómo la arquitectura del sistema reduce las posibles consecuencias de un compromiso exitoso, en particular, la duración y el grado de interrupción causada por el adversario, así como la velocidad y el alcance de la propagación de malware (Deborah Bodeau & Graubart, 2017).
- ***Espere que los adversarios evolucionen***. Los adversarios cibernéticos avanzados invierten tiempo, esfuerzo y recopilación de inteligencia para mejorar y desarrollar las tácticas, técnicas y procedimientos (TTP) que les permiten evolucionar sus estrategias de ataque en respuesta a las oportunidades que ofrecen las nuevas tecnologías o los usos de la tecnología, así como al conocimiento que obtienen sobre las TTP de los defensores. En tiempo (cada vez más corto), las herramientas desarrolladas por adversarios avanzados están disponibles para adversarios menos sofisticados; por lo tanto, los sistemas y las misiones deben ser resilientes frente a ataques inesperados. Este principio de diseño, por lo tanto, respalda una estrategia de administración de riesgos que debe ir más allá de la práctica común de buscar remediar vulnerabilidades conocidas (Deborah Bodeau & Graubart, 2017).

Los principios de diseño estructurales de ciber-resiliencia apoyan los principios de diseño estratégico y se describen a continuación:

- ***Limitar la confianza por defecto***. Limitar el número de elementos del sistema que son de confianza, reduce el nivel de esfuerzo necesario para el aseguramiento, la protección y el monitoreo. Requiere la definición de procesos y procedimientos para determinar los aspectos necesarios de confiabilidad, identificar los elementos del sistema para los que dichos aspectos son necesarios y para reducir el tamaño del conjunto de elementos del sistema de confianza (Deborah Bodeau & Graubart, 2017).

- ***Limitación de la visibilidad***. Controlar que puede ser descubierto, observado y usado, incrementa el esfuerzo necesario por los adversarios para expandir su posición o aumentar los impactos sobre los recursos cibernéticos. La visibilidad de los datos puede ser controlada por mecanismos como el cifrado, el ocultamiento o la ofuscación de datos. Para limitar la visibilidad o controlar el uso, el acceso a los recursos del sistema se puede controlar desde perspectivas de múltiples disciplinas de seguridad, incluyendo controles de acceso físico y lógico (Deborah Bodeau & Graubart, 2017).
- ***Contención y exclusión de comportamientos anómalos.*** La limitación de qué se puede hacer y dónde estas acciones pueden ser realizadas, reduce la posibilidad o el grado de difusión de compromisos o interrupciones en los componentes o servicios. El comportamiento de un elemento del sistema como los recursos que utiliza, con qué elementos del sistema interactúa o cuándo realiza una acción determinada, puede variar según muchas circunstancias legítimas. El análisis del proceso de negocio permite identificar comportamientos inaceptables, así como comportamientos que son aceptables solo en circunstancias específicas. Excluir comportamientos evita que tales comportamientos tengan consecuencias indeseables. Los comportamientos se pueden excluir a priori con diversos grados de seguridad, desde la eliminación de la funcionalidad hasta la restricción de esta o su uso, balanceando la seguridad y la flexibilidad (Deborah Bodeau & Graubart, 2017).
- ***Defensa en profundidad (capas) y segmentación de los medios***. La combinación de defensa en profundidad y el particionamiento, aumentan el esfuerzo que el atacante requiere para superar las múltiples defensas. Las capas de defensa restringen el movimiento del adversario verticalmente en una arquitectura en capas; una defensa en una capa evita que se propague un compromiso en una capa adyacente. El particionamiento separa los conjuntos de recursos en sistemas efectivamente separados con interfaces controladas (Deborah Bodeau & Graubart, 2017).
- ***Planifica y gestiona la diversidad***. La diversidad es una técnica de resiliencia reconocida que elimina puntos de ataque o falla. La implementación de este principio debe tener en cuenta el costo y la capacidad de administración para evitar la introducción de nuevos riesgos. La diversidad ofrece el beneficio de proporcionar

formas alternativas para entregar la funcionalidad requerida, de modo que si un componente se ve comprometido, se pueden usar uno o más componentes alternativos que brindan la misma funcionalidad (Deborah Bodeau & Graubart, 2017).

- ***Mantener redundancia.*** La redundancia es clave para muchas estrategias de resiliencia, pero puede degradarse con el tiempo, a medida que se actualizan las configuraciones o cambia la conectividad. La implementación considera aspectos como duplicidad de recursos en múltiples ubicaciones, manteniéndolos sincronizados; así mismo, puede considerar el contar con capacidades adicionales de almacenamiento de información, procesamiento y comunicaciones, para ser utilizadas en contingencias (Deborah Bodeau & Graubart, 2017).
- ***Hacer que la localización de los recursos sea versátil***. Un recurso vinculado a una única ubicación puede convertirse en un único punto de falla y un objetivo de alto valor para un atacante. La aplicación de este principio implica el uso de posicionamiento dinámico, a menudo en combinación con redundancia o diversidad (Deborah Bodeau & Graubart, 2017).
- ***Aprovechamiento de la información de los indicadores de ciberseguridad.*** La salud y el estado del dato puede ser útil para soportar la conciencia situacional, indicando comportamientos potencialmente sospechosos y prediciendo la necesidad de adaptación con motivo de los cambios de requerimientos operacionales. Implica el monitoreo de indicadores de comportamiento anormal, y la correlación del monitoreo de datos de múltiples capas o tipos de componentes en la arquitectura para poder identificar problemas potenciales de forma temprana para que puedan ser evitados o contenidos (Deborah Bodeau & Graubart, 2017).
- ***Mantener la conciencia situacional.*** La conciencia situacional permite conocer las posibles tendencias de rendimiento y la aparición de anomalías, informando sobre ellas para tomar acciones que garanticen que el cumplimiento de la misión organizacional no se vea afectado. Abarca el conocimiento del sistema, las amenazas y la dependencia que las funciones críticas del negocio tienen de los elementos del sistema. Requiere de la utilización de inteligencia de amenazas, teniendo en cuenta la constante evolución de los adversarios (Deborah Bodeau & Graubart, 2017).

- ***Gestionar riesgos adaptativamente***. Respalda la agilidad, proporcionando una mitigación de riesgos complementaria en todas las operaciones críticas, a pesar de las interrupciones o cortes de los componentes (Deborah Bodeau & Graubart, 2017).
- ***Maximizar la transitoriedad; minimizar la persistencia***. El uso de elementos transitorios del sistema minimiza la duración de la exposición a actividades adversas, mientras que el refrescamiento periódico a un buen estado conocido puede eliminar el malware o los datos dañados (Deborah Bodeau & Graubart, 2017).
- ***Validación periódica o continua de la integridad.*** La validación periódica o continua de la integridad o corrección de los datos o el software puede aumentar el esfuerzo del adversario para modificar o fabricar datos o funciones. Así mismo, el análisis periódico o continuo del comportamiento de usuarios individuales, componentes del sistema y servicios puede aumentar la sospecha, generando acciones como monitoreos más cercanos, privilegios más restrictivos o cuarentena (Deborah Bodeau & Graubart, 2017).
- ***Cambiar o interrumpir la superficie de ataque***. Interrumpir la superficie de ataque puede causar que el adversario desperdicie recursos, haga suposiciones incorrectas sobre el sistema, lance ataques o revele información de forma prematura (Deborah Bodeau & Graubart, 2017).
- ***Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario***. Permite aumentar la incertidumbre de los adversarios sobre la estructura y el comportamiento del sistema. Considera técnicas como el ofuscamiento, que aumenta el esfuerzo que necesita el adversario y puede ocultar actividades críticas el tiempo suficiente para que se completen sin interrupción del adversario (Deborah Bodeau & Graubart, 2017).

2.3 Modelo de gestión de resiliencia CERT

El CERT-RMM es un modelo de madurez de la capacidad para administrar la resiliencia operativa que fue definido por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon. Este modelo tiene dos objetivos principales: establecer la convergencia de

las actividades de gestión de riesgo operacional y resiliencia (planeación y gestión de la seguridad, continuidad del negocio y las operaciones de TI y la prestación de los servicios); y aplicar un enfoque de mejora de procesos para la gestión de la resiliencia operativa definiendo y aplicando una escala de capacidad que exprese niveles crecientes de madurez del proceso (Partridge & Young, 2011).

El modelo CERT-RMM proporciona una definición de proceso expresada en 26 áreas de proceso en cuatro categorías: gestión empresarial, ingeniería, operaciones y administración de procesos. Este modelo se centra en la recuperación de cuatro activos operativos esenciales: personas, información, tecnología, e instalaciones. Incluye procesos y prácticas que definen una escala de cuatro niveles de capacidad para cada área de proceso: incompleta, realizada, gestionada y definida (Partridge & Young, 2011).

CERT-RMM tiene varios componentes clave. El "área de proceso" constituye el principal elemento estructural. En el modelo, cada área de proceso tiene una serie de componentes descriptivos y abarca un área funcional de competencia. En conjunto, las 26 áreas de proceso definen el sistema de gestión de la resiliencia operacional.

Cada área de proceso tiene un conjunto de metas. Las metas son elementos obligatorios del área de proceso y definen el logro de los objetivos del proceso que es reflejado por el área de proceso (Partridge & Young, 2011).

A continuación, se describen las áreas de proceso que conforman el modelo:

- ***Área de proceso de definición y gestión de activos (ADM)***. El propósito de esta área de proceso es identificar, documentar y administrar los activos de la organización durante su ciclo de vida para asegurar la sostenibilidad de la producción y así soportar los servicios organizacionales (Caralli, Allen, Curtis, White, & Young, 2016)
- ***Área de proceso de gestión de acceso (AM).*** El propósito de esta área de proceso es garantizar que el acceso otorgado a los activos de la organización sea acorde con sus requisitos comerciales y de resiliencia. Los controles de acceso son un elemento clave de la protección provista a un activo y forman una parte sustancial de la estrategia de protección de la organización para activos y servicios. Debido a que el entorno

operativo está cambiando constantemente, es difícil para una organización mantener controles de acceso actualizados y que reflejen los requisitos reales de negocio y resiliencia (Caralli et al., 2016, p. 58).

- ***Área de proceso de comunicaciones (COMM).*** El propósito de las comunicaciones es desarrollar, entregar y administrar comunicaciones internas y externas para respaldar las actividades y procesos de resiliencia. Desde una perspectiva de resiliencia, la comunicación es una función esencial, ya que une partes dispares de la organización que colectivamente tienen un gran interés en proteger activos y servicios de alto valor y mantener activos y servicios durante y después de un evento perturbador. Las comunicaciones efectivas son un factor crítico de éxito para garantizar la ejecución exitosa de los planes de continuidad del servicio, transmitir los requisitos de resiliencia a partes externas y gestionar las interrupciones, especialmente durante una crisis o desastre (Caralli et al., 2016, p. 58).
- ***Área de proceso de cumplimiento (COMP).*** El propósito de esta área es garantizar conciencia y cumplimiento con un conjunto establecido de directrices, normas, prácticas, políticas, regulaciones y legislación relevantes, internas y externas, y otras obligaciones (como contratos y acuerdos de nivel de servicio) relacionadas con la gestión de la resiliencia operativa (Caralli et al., 2016, p. 88).
- ***Área de proceso gestión de controles (CTRL)***. El propósito de esta área de proceso es establecer, monitorear, analizar y administrar un sistema de control interno que garantice la efectividad y eficiencia de las operaciones al asegurar el éxito de la misión de los servicios críticos y los activos que los respaldan (Caralli et al., 2016, p. 120).
- ***Área de proceso de control ambiental (CE).*** El propósito del control ambiental es establecer y administrar un nivel adecuado de controles físicos, ambientales y geográficos para respaldar las operaciones de servicios resilientes en las instalaciones de la organización. El área de proceso de control ambiental aborda la importancia de las instalaciones en la resiliencia operativa de los servicios, así como los problemas únicos que los activos de las instalaciones heredan debido a su ubicación geográfica y el entorno en el que operan (Caralli et al., 2016, p. 149).

- ***Área de proceso de enfoque empresarial (EF).*** El objetivo de esta área de proceso es establecer patrocinio, planificación estratégica y gobierno sobre el sistema de gestión de resiliencia organizacional (Caralli et al., 2016, p. 184).
- ***Área de proceso gestión de dependencias externas (EXD)***. El propósito del área de proceso de administración de dependencias externas es establecer y administrar un nivel apropiado de controles para asegurar la capacidad de recuperación de los servicios y activos que dependen de las acciones de las entidades externas (Caralli et al., 2016, p. 216).
- ***Área de proceso gestión de recursos financieros (FRM).*** El propósito de esta área de proceso es solicitar, recibir, administrar y aplicar recursos financieros para apoyar los objetivos y requisitos de resiliencia. La gestión de recursos financieros se centra en mejorar la capacidad de la organización para aplicar recursos financieros en actividades de resiliencia, al tiempo que ayuda a la organización a gestionar activamente el costo y el retorno de la inversión de estas actividades (Caralli et al., 2016, p. 256).
- ***Área de proceso gestión de recursos humanos (HRM).*** El propósito de esta área de proceso es administrar el ciclo de vida laboral y el desempeño del personal de una manera que contribuya a la capacidad de la organización para administrar la resiliencia operativa. La gestión de recursos humanos también trata de garantizar que los recursos humanos de la organización no supongan un riesgo operativo adicional para la organización cuando un empleo se interrumpe voluntaria o involuntariamente (Caralli et al., 2016, p. 287).
- ***Área de proceso gestión de identidad (ID).*** El propósito de esta área de proceso es crear, mantener y desactivar identidades que puedan necesitar algún nivel de acceso confiable a los activos de la organización y administrar los atributos asociados de las identidades. En la gestión de identidades, las identidades de personas, objetos y entidades se crean para que se den a conocer a la organización y puedan gestionarse a lo largo de su vida útil. En el caso de las personas, estas identidades generalmente representan usuarios de información, sistemas e instalaciones que tienen nombres de identificación únicos (como una identificación de usuario) y para los cuales se conoce

información sobre sus roles y responsabilidades en la organización (Caralli et al., 2016, p. 323).

- ***Área de proceso de gestión y control de incidentes (IMC).*** El propósito de esta área de proceso es establecer procesos para identificar y analizar eventos, detectar incidentes y determinar una respuesta organizacional adecuada (Caralli et al., 2016, p. 349).
- ***Área de proceso de gestión del conocimiento e información (KIM).*** El propósito de la gestión de conocimiento e información es establecer y administrar un nivel apropiado de controles para respaldar la confidencialidad, integridad y disponibilidad de la información de la organización, registros vitales y propiedad intelectual (Caralli et al., 2016, p. 389).
- ***Área de proceso de medición y análisis (MA).*** El propósito de esta área de proceso es desarrollar y mantener una capacidad de medición que es usada para soportar las necesidades de gestión de información del sistema de gestión de resiliencia operacional. Las mediciones consistentes, oportunas y precisas son retroalimentación importante para administrar cualquier actividad (Caralli et al., 2016, p. 425).
- ***Área de proceso de monitoreo (MON).*** El propósito de esta área de proceso es recopilar, registrar y distribuir información sobre el sistema de gestión de resiliencia operacional para la organización. El monitoreo es una actividad de toda la empresa que la organización utiliza para "tomar el pulso" de sus operaciones diarias y, en particular, sus procesos de gestión de resiliencia operativa. El descubrimiento y análisis proactivos de los datos relacionados con las actividades operacionales aseguran que las partes interesadas tengan la información necesaria para tomar decisiones antes, durante o después de que ocurra una interrupción. El monitoreo proporciona la información que la organización necesita para determinar si está sujeta a amenazas y vulnerabilidades que requieren acciones para evitar el impacto organizacional (Caralli et al., 2016, p. 451).
- ***Área de proceso de definición del proceso organizacional (OPD).*** El propósito de esta área de proceso es establecer y mantener un conjunto utilizable de activos de procesos organizacionales y estándares de entorno de trabajo para la resiliencia operativa (Caralli et al., 2016, p. 480).

- ***Área de proceso enfoque del proceso organizacional (OPF)***. El propósito de esta área de proceso es planificar, implementar y desplegar mejoras de procesos organizacionales basadas en una comprensión profunda de las fortalezas y debilidades actuales de los procesos de resiliencia operacional de la organización y los activos de procesos. La mejora del proceso se produce en el contexto de las necesidades de la organización y se utiliza para abordar los objetivos de la organización (Caralli et al., 2016, p. 502).
- ***Área de proceso formación y sensibilización organizacional (OTA).*** El propósito de la capacitación y concientización organizacional es promover la concientización y desarrollar habilidades y conocimientos de las personas en apoyo de sus roles para lograr y mantener la resiliencia operativa. La capacitación y concientización organizacional es un área de proceso empresarial que busca asegurar que el personal de la organización esté al tanto de las necesidades e inquietudes de la resiliencia y que se comporte de una manera coherente con los requisitos y objetivos operacionales de resiliencia de la organización. Esto requiere que se les informe sobre los planes y programas de resiliencia de la organización y que comprendan su papel en estos planes y programas (Caralli et al., 2016, p. 527).
- ***Área de proceso gestión de personas (PM).*** El propósito de la gestión de personas es establecer y administrar las contribuciones y la disponibilidad de las personas para respaldar el funcionamiento resiliente de los servicios de la organización (Caralli et al., 2016, p. 559).
- ***Área de proceso gestión de riesgos (RISK).***El propósito de la gestión de riesgos es identificar, analizar y responder a los riesgos de los activos de la organización que podrían afectar negativamente la operación y la prestación de servicios. La gestión del riesgo operacional influye significativamente en la resiliencia operacional. El riesgo de interrupción de cualquier activo hace que los servicios asociados no puedan cumplir su misión, lo que reduce la resiliencia operativa (Caralli et al., 2016, p. 590).
- ***Área de proceso de desarrollo de requisitos de resiliencia (RRD).*** El propósito del desarrollo de requisitos de resiliencia es identificar, documentar y analizar los requisitos de resiliencia operacional para servicios de alto valor y activos relacionados.

Los requisitos de resiliencia proporcionan la base para proteger los activos de las amenazas y mantenerlos en la medida de lo posible para que puedan desempeñarse según lo previsto en el soporte de los servicios (Caralli et al., 2016, p. 620).

- ***Área de proceso gestión de requisitos de resiliencia (RRM).*** El propósito de esta área de proceso es administrar los requisitos de resiliencia de los servicios de alto valor y los activos asociados e identificar inconsistencias entre estos requisitos y las actividades que realiza la organización para cumplir con los requisitos. Junto con el área de proceso de "Desarrollo de requisitos de resiliencia", el área de proceso de "Gestión de requisitos de resiliencia" busca definir el ciclo de vida de los requisitos de resiliencia, desde el inicio, el desarrollo o la adquisición hasta la aplicación, el monitoreo y la medición, y la gestión de cambios (Caralli et al., 2016, p. 643).
- ***Área de proceso de ingeniería de soluciones técnicas resilientes (RTSE).*** El propósito de la ingeniería de soluciones técnicas resilientes es garantizar que el software y los sistemas se desarrollen para satisfacer sus requisitos de resiliencia. El software y los sistemas resilientes no pueden sobrevivir y resistir a amenazas sin un compromiso organizacional para abordar la resiliencia a lo largo del proceso de desarrollo (Caralli et al., 2016, p. 665).
- ***Área de proceso de continuidad del servicio (SC).*** El propósito de la continuidad del servicio es garantizar la continuidad de las operaciones esenciales de los servicios y sus activos asociados si se produce una interrupción como resultado de un incidente, desastre u otro evento perturbador. La continuidad de la prestación de servicios de una organización es una preocupación primordial en las actividades de resiliencia operativa de la organización (Caralli et al., 2016, p. 703).
- ***Área de proceso de gestión de la tecnología (TM).*** El propósito de la administración de tecnología es establecer y administrar un nivel apropiado de controles relacionados con la integridad y disponibilidad de los activos de tecnología para respaldar las operaciones resilientes de los servicios de la organización (Caralli et al., 2016, p. 740).
- ***Área de proceso análisis y resolución de vulnerabilidad (VAR).*** El propósito del análisis y resolución de vulnerabilidades es identificar, analizar y gestionar vulnerabilidades en el entorno operativo de una organización. El análisis y la resolución

de vulnerabilidades informa a la organización de las amenazas que deben analizarse en el proceso de gestión de riesgos para determinar si representan un riesgo tangible para la organización en función de sus factores de riesgo, apetito y tolerancia únicos. A su vez, el proceso de gestión de riesgos informa los procesos de análisis y resolución de vulnerabilidades para centrar la atención en los activos y servicios más críticos para cumplir con los objetivos estratégicos (Caralli et al., 2016, p. 786).

2.4 Modelo de indicadores para la mejora de la ciber-resiliencia (IMC)

Este modelo fue publicado por el CERT de seguridad e industria "CERTSI" del gobierno de España y plantea indicadores para la mejora de la ciber-resiliencia (IMC) en organizaciones y empresas de sectores industriales e infraestructuras críticas industriales. El modelo de indicadores de ciber-resiliencia está compuesto por una metodología de evaluación de indicadores, diccionario de indicadores y una plantilla de autoevaluación. Este modelo parte de la definición de un conjunto de metas de alto nivel, unos objetivos generales y específicos, y por último define las preguntas necesarias para contestar o conseguir dichos objetivos. Los indicadores de ciber-resiliencia son una representación estadística de los datos de una característica de ciber-resiliencia relevante, con el fin de permitir comparaciones significativas, y representan el grado de satisfacción de las métricas de ciber-resiliencia (CERTSI, n.d.).

El modelo de indicadores para la mejora de la ciber-resiliencia está soportado en un marco de trabajo conformado por cuatro metas y catorce dominios funcionales agrupados por meta, los cuales se resumen en la figura 1.

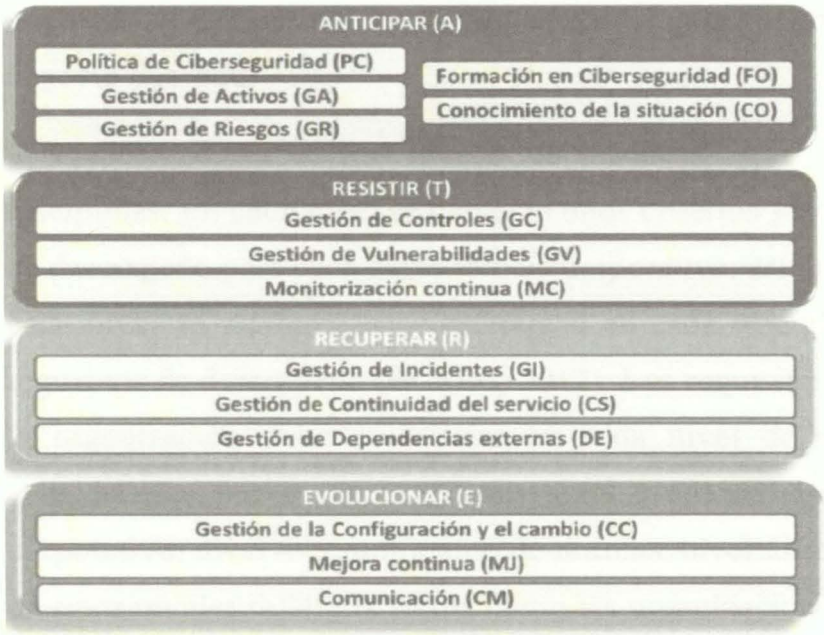


Figura 1. Marco de trabajo de ciber-resiliencia
Fuente: (CERTSI, n.d.).

Para alimentar este marco de trabajo, se definió un conjunto de métricas de ciber-resiliencia agrupadas por dominio funcional y un conjunto de indicadores de ciber-resiliencia, basados principalmente en indicadores clave de rendimiento (KPI), y en la posible definición de KRI o KGI.

2.5 Modelo de madurez de continuidad del negocio (BCMM)

El modelo de la madurez de la continuidad del negocio (BCMM), fue definido por Virtual Corporation para dirigir la necesidad de organizaciones de valorar y mejorar su programa de continuidad de negocio (BCMM, 2012). Este modelo permite a las organizaciones contar con una herramienta de diagnóstico para evaluar objetivamente la efectividad del programa de continuidad del negocio organizacional, apoyando a la alta dirección de las organizaciones para responder las preguntas relacionadas con el nivel actual de madurez de continuidad del negocio, el nivel de madurez que debería plantearse la organización como objetivo y las

prácticas que se deben implementar para lograr el nivel de madurez de continuidad del negocio deseado.

El modelo consta de seis niveles de madurez, ocho competencias corporativas y cuatro disciplinas. En cada nivel se manejan unos criterios y descriptores, así como unos requisitos de desempeño para cada competencia corporativa; así mismo, el contenido del programa por cada nivel de madurez hace referencia en cada disciplina a unos conceptos clave y unos requisitos de desempeño (BCMM, 2012). Los requisitos de desempeño son las prácticas que la organización debe evidenciar en cada nivel de madurez. Los niveles de madurez considerados por el BCMM son: nivel 1-autodirigido, nivel 2-departamental, nivel 3-corporativo, nivel 4-cumplimento de normas, nivel 5-integrado, nivel 6-sinérgico. Cada uno de estos niveles refleja la forma como las organizaciones abordan la gestión de continuidad del negocio, partiendo de esfuerzos individuales de las áreas organizacionales, hasta ser parte de la organización e integrar a las partes interesadas. Cada nivel, a su vez, refleja el grado de preparación que tiene la organización para recuperarse de eventos que pueden poner en riesgo su continuidad.

A continuación, se describen las competencias corporativas que considera el modelo:

- ***Liderazgo***: corresponde al compromiso y entendimiento demostrado por la alta dirección con respecto a la implementación del programa corporativo global de continuidad del negocio, así como la articulación y entendimiento por parte del comité ejecutivo del caso de negocio para implementar continuidad del negocio (BCMM, 2012).
- ***Conciencia de empleados***: constituye la amplitud y profundidad de conocimiento conceptual de continuidad del negocio en todos los niveles jerárquicos de la organización, incluyendo las consideraciones para la calidad y sostenibilidad de los programas de entrenamiento y de creación de conciencia (BCMM, 2012).
- ***Estructura del programa de CN***: comprende la dimensión y relevancia del programa de CN en la organización. El grado en que el programa de CN cumple con el caso de negocio (BCMM, 2012).

- ***Interiorización del programa***: mide el nivel de coordinación de continuidad del negocio entre los diferentes departamentos, funciones y unidades de negocio a lo largo de toda la organización. El grado en que las consideraciones de continuidad del negocio han sido incorporadas en otras iniciativas, programas o procesos de negocio (BCMM, 2012).
- ***Métricas:*** constituyen el desarrollo y monitoreo de las mediciones apropiadas del desempeño del Programa de Continuidad del Negocio. El establecimiento de una línea base y su permanente seguimiento a las metas establecidas para alcanzar las competencias necesarias de la continuidad del negocio (BCMM, 2012).
- ***Compromiso de recursos***: busca la disponibilidad de suficientes recursos humanos (bien entrenados y respaldados por la organización), financieros y otros recursos requeridos para el programa de continuidad del negocio (BCMM, 2012).
- ***Coordinación externa***: coordinación de asuntos y requerimientos de continuidad del negocio con la comunidad externa, incluyendo clientes, proveedores, bancos, gobierno, acreedores, aseguradoras, etc., garantizando que los eslabones críticos de la cadena de suministros tienen planes de CN adecuados en sus propias organizaciones (BCMM, 2012).
- ***Contenido del programa de CN***: se refiere a cómo la organización implementa las cuatro disciplinas centrales de la continuidad del negocio (BCMM, 2012).

Las disciplinas que apoyan la gestión de continuidad del negocio se describen a continuación:

- ***Administración de incidentes***: se asegura de que todos los aspectos de respuesta a la emergencia, manejo de crisis, y cualquier otra actividad involucrada en el comando, control y comunicación durante una contingencia organizacional y/o desastre, sean manejados adecuadamente (BCMM, 2012).
- ***Administración de la seguridad***: asegura que la seguridad física (inmuebles), informática y cualquier otra actividad asociada con proteger la integridad específica de personas, bienes o información, estén apropiadamente enfocadas (BCMM, 2012).

- ***Recuperación tecnológica***: asegura que el hardware, software, redes y aplicaciones críticas de la organización son recuperados de manera adecuada dentro de los tiempos objetivos de recuperación (BCMM, 2012).
- ***Recuperación de negocios***: asegura que las funciones, procesos y recursos críticos del negocio, son recuperables de manera adecuada dentro de los tiempos objetivos de recuperación (BCMM, 2012).

2.6 Modelo de madurez de la comunidad de ciberseguridad (CCSMM)

Este modelo fue desarrollado por el CIAS (Center for Infrastructure Assurance and Security) de la Universidad de Texas, para abordar las necesidades de los Estados y las comunidades para desarrollar un programa de ciberseguridad viable y sostenible. El modelo identifica las características de las comunidades y los Estados, mediante la evaluación de aspectos tales como la concienciación sobre la ciberseguridad, el intercambio de información dentro y entre las organizaciones, el desarrollo y la implementación de procesos y procedimientos de seguridad, y la integración de la seguridad informática en la comunidad, el Estado, planes de continuidad de las operaciones y la respuesta a incidentes (White, 2011).

El modelo de madurez de la comunidad de ciberseguridad considera cinco niveles de madurez:

- ***El nivel 1-Inicial,*** donde se tiene poco o ningún conocimiento, análisis y evaluaciones de ciberseguridad, así como poca inclusión de las amenazas y problemas cibernéticos en los planes de continuidad de las operaciones.
- ***El nivel 2-Establecido*** es caracterizado porque existe una conciencia de las amenazas cibernéticas y la necesidad de implementar la ciberseguridad. Así mismo, es consciente de la necesidad de capacitación y entrenamiento cooperativo en ciberseguridad.
- ***El nivel 3-Autoevaluado***, donde se evidencia que los líderes dentro de las organizaciones, comunidades y Estados promueven activamente la concienciación sobre la ciberseguridad y cooperan con otros para establecer programas de capacitación

y educación. En este nivel, la ciberseguridad se incluye en los planes de continuidad de operaciones y esos planes se prueban y evalúan mediante ejercicios.

- ***El nivel 4-Integrado*** incorpora la ciberseguridad como parte del proceso de planificación. En este nivel, el intercambio de información se formaliza y hay una fusión de información cibernética.
- ***En el nivel 5-Vanguardia***, la ciberseguridad es un imperativo comercial para las organizaciones, comunidades y Estados. Se ha integrado tan a fondo en los procesos que no se considera una disciplina separada. Las entidades en este nivel son capaces de enseñar y guiar a otros (White, 2011).

2.7 Marco para la mejora de la ciberseguridad en infraestructuras críticas

Este marco fue desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) y se presenta como una forma flexible de abordar la ciberseguridad en las dimensiones físicas, cibernéticas y de personas. El marco es aplicable a tecnología de información (TI), sistemas de control industrial (ICS), sistemas ciber físicos (CPS) o dispositivos conectados en general, incluido el internet de las cosas (IoT). El marco es una metodología con un enfoque para reducir el riesgo vinculado a las amenazas cibernéticas que puedan comprometer la seguridad de la información, y está compuesto por tres partes: el núcleo del marco, los niveles de implementación y los perfiles del marco. Cada componente del marco refuerza la conexión entre los impulsores empresariales o de misión y las actividades de ciberseguridad (NIST, 2018).

- ***Núcleo del marco.*** Proporciona un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. Consta de cuatro elementos: funciones, categorías, subcategorías y referencias informativas (NIST, 2018). En la tabla 3 se describen las funciones y categorías del marco.
- ***Niveles de implementación del marco.*** Proporcionan un contexto sobre cómo una organización considera el riesgo de ciberseguridad y los procesos establecidos para gestionar dicho riesgo. Los Niveles Parcial (Nivel 1) a Adaptable (Nivel 4) describen

un grado cada vez mayor de rigor y sofisticación en las prácticas de gestión de riesgos de ciberseguridad. Cada nivel describe el estado de implementación del proceso de gestión de riesgos, del programa integrado de gestión de riesgos y la participación externa (NIST, 2018).

- ***Perfil del marco.*** Corresponde a la alineación de las funciones, categorías y subcategorías con los requisitos empresariales, la tolerancia al riesgo y los recursos de la organización, permitiendo a la organización establecer una hoja de ruta para reducir el riesgo de ciberseguridad, alineada con los objetivos organizacionales y sectoriales. Considera los requisitos legales o reglamentarios y las mejores prácticas de la industria, y refleja las prioridades de gestión de riesgos (NIST, 2018).

Tabla 3

Identificadores únicos de función y categoría

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Fuente: National Institute of Standars and Technology (2018).

2.8 Modelo de madurez de la capacidad de ciberseguridad (C2M2)

El C2M2 (Cybersecurity Capability Maturity Model) nació como resultado de un programa de ciberseguridad realizado con colaboración público-privada en Estados Unidos (la Casa Blanca, copatrocinado por el DOE, Department of Energy, y el DHS, Department of Homeland Security) para mejorar las capacidades de ciberseguridad subsector electricidad, y para comprender la postura de ciberseguridad de la red. El programa C2M2 consta de tres modelos de madurez de capacidad de ciberseguridad: el modelo de madurez de capacidad de ciberseguridad (C2M2); el modelo de madurez de la capacidad de ciberseguridad del subsector de electricidad (ES-C2M2), y el modelo de madurez de capacidad de ciberseguridad del subsector de petróleo y gas natural (ONG-C2M2) (Curtis & Mehravari, 2015).

El modelo está compuesto por diez dominios que contienen un conjunto estructurado de prácticas, que permiten evaluar la evolución de la capacidad y madurez en cada dominio, usando niveles denominados milésimas de pulgadas (MIL) que van desde 0 a 3. Las prácticas dentro de cada dominio se organizan en objetivos, que representan logros en el dominio. Cada dominio tiene una declaración del propósito del dominio que representa su intención; adicionalmente, cuenta con unas notas de introducción que son un contexto del dominio e introducen sus prácticas (Christopher et al., 2014).

Los dominios que conforman el modelo C2M2 se describen a continuación:

- ***Gestión del riesgo (RM)***. Tiene como objetivo establecer, operar y mantener un programa de gestión de riesgos de seguridad cibernética que cubra tanto la organización como sus unidades de negocio, filiales, la interconexión de infraestructuras relacionadas y las partes interesadas (Christopher et al., 2014).
- ***Gestión de activos, cambios y configuración (ACM).*** Tiene como finalidad gestionar los activos de tecnología de información (TI) y tecnología de operación (TO) de la organización, incluyendo hardware y software, acorde con el riesgo de la infraestructura crítica y los objetivos organizacionales. Este dominio considera cuatro objetivos: manejo del inventario de activos, la gestión de la configuración de los

activos, manejo de cambios en los activos y actividades de gestión (Christopher et al., 2014).

- ***El dominio gestión de identidad y acceso (IAM).*** Tiene como objetivo crear y administrar las identidades de las entidades a las que puede concederse acceso lógico o físico a los activos de la organización. Este dominio comprende tres objetivos: establecer y mantener identidades; control de acceso, y actividades de gestión (Christopher et al., 2014).
- ***Gestión de amenazas y vulnerabilidades (TVM).*** Tiene como propósito establecer y mantener los planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas de seguridad cibernética y a las vulnerabilidades asociadas con el riesgo de la infraestructura de la organización y los objetivos de la organización. Este dominio considera tres objetivos: identificar y responder a las amenazas; reducir las vulnerabilidades de ciberseguridad; actividades de gestión (Christopher et al., 2014).
- ***Conciencia situacional (SA).*** Tiene como objetivo establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y utilizar información operativa y de ciberseguridad, incluyendo el estado y resumen de los otros dominios modelo, formando una imagen operativa común (COP). Este dominio considera cuatro objetivos: realizar registro; realizar monitoreo; establecer y mantener una imagen operativa común, y actividades de gestión (Christopher et al., 2014).
- ***Intercambio de información y comunicaciones (ISC***). Tiene como finalidad establecer y mantener relaciones con entidades internas y externas para recoger y proporcionar información sobre seguridad cibernética, así como las amenazas y las vulnerabilidades, para reducir los riesgos y aumentar la capacidad de recuperación operativa en concordancia con el riesgo de la infraestructura crítica y los objetivos organizacionales. Este dominio considera dos objetivos: compartir información sobre seguridad cibernética y actividades de gestión (Christopher et al., 2014).
- ***Eventos y respuesta a incidentes, continuidad de operaciones (IR).*** Busca establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de seguridad cibernética y para sostener las operaciones a lo largo de un evento

de seguridad cibernética, acorde con el riesgo de la infraestructura crítica y objetivos organizacionales. Este dominio considera cinco objetivos: detectar eventos de seguridad cibernética; escalar eventos de ciberseguridad y declarar incidentes; responder a incidentes de seguridad cibernética y escalado de eventos; plan de continuidad, y actividades de gestión (Christopher et al., 2014).

- ***Cadena de suministro y gestión de dependencias externas (EDM).*** Tiene como propósito establecer y mantener controles para gestionar los riesgos de seguridad cibernética asociados a los servicios y bienes que son dependientes de entidades externas, acorde con el riesgo a la infraestructura crítica y objetivos de la organización. Este dominio considera tres objetivos: identificar las dependencias; manejo de riesgo de dependencia, y actividades de gestión (Christopher et al., 2014).
- ***Administración de personal (WM).*** Tiene como propósito establecer y mantener los planes, procedimientos, tecnologías y controles para crear una cultura de seguridad cibernética y para asegurar la educación continua y la competencia del personal, acorde con el riesgo a la infraestructura crítica y los objetivos organizacionales. Este dominio considera cinco objetivos: asignar responsabilidades de seguridad cibernética; controlar el ciclo de vida de la fuerza laboral; desarrollar ciberseguridad de la fuerza de trabajo; aumentar la conciencia de la seguridad cibernética y actividades de gestión (Christopher et al., 2014).
- ***Programa de gestión de seguridad cibernética (CPM).*** Tiene el propósito de establecer y mantener un programa de seguridad cibernética de la empresa que provea el gobierno, la planificación estratégica, y el patrocinio de las actividades de seguridad cibernética de la organización de manera que alinea los objetivos de seguridad cibernética con los objetivos estratégicos de la organización y el riesgo a la infraestructura crítica. Este dominio considera cinco objetivos: establecer la estrategia del programa de seguridad cibernética, patrocinador del programa de seguridad cibernética, establecer y mantener la arquitectura de seguridad cibernética, realizar desarrollo de software seguro y actividades de gestión (Christopher et al., 2014).

2.9 Controles de ciberseguridad del CIS

Estos controles fueron propuestos por el "Center for Internet Security" CIS y son un conjunto de acciones priorizadas que colectivamente forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes. Según el CIS, los cinco principios fundamentales de un sistema efectivo de defensa cibernética son:

- ***La ofensa informa a la defensa***: basado en utilizar el conocimiento adquirido de ataques reales para aprender continuamente de estos eventos y construir defensas efectivas y prácticas, incluyendo solo controles demostrados para detener ataques conocidos del mundo real.
- ***Priorización***: implica invertir primero en los controles que proporcionarán mayor reducción de riesgos y protección contra los actores más peligrosos y que tienen mayor viabilidad de implementación.
- ***Mediciones y métricas***: establecer un lenguaje común que sea entendido por los diferentes niveles organizacionales para medir la efectividad de las medidas de seguridad de tal forma que los ajustes necesarios se identifiquen e implementen rápidamente.
- ***Diagnóstico y mitigación continuos***: comprende la validación continua de la efectividad de las medidas de seguridad para ayudar a dirigir la prioridad de los siguientes pasos.
- ***Automatización***: la automatización de las defensas ayuda a lograr mediciones confiables, escalables y continuas de la adhesión a los controles y las métricas relacionadas

(CIS, 2019).

El CIS considera en total 20 controles de ciberseguridad a implementar, los cuales se describen en la tabla 4.

Tabla 4

Controles ciberseguridad CIS

Control CIS	Descripción
1- Inventario de dispositivos autorizados y no autorizados	Gestión activa de todo el dispositivo hardware en la red para que solo los dispositivos autorizados obtengan acceso y se detecte y prevenga el acceso de dispositivos no autorizados.
2- Inventario de software autorizados y no autorizados	Gestión activa de todo software en la red de tal forma que solo software autorizado esté instalado, se detecte el software no autorizado y se prevenga su instalación y ejecución.
3- Gestión continua de vulnerabilidades	Adquirir, evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.
4- Uso controlado de privilegios administrativos	Los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.
5- Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	Establezca, implemente y gestione activamente (rastree, informe, corrija) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.
6- Mantenimiento, monitoreo y análisis de logs de auditoría	Reúna, administre y analice registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.
7- Protección de correo electrónico y navegador web	Minimizar la superficie de ataque y la oportunidad para atacantes de manipular el comportamiento humano a través de su interacción con navegadores web y sistemas de correo electrónico.
8- Defensa contra malware	Controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar el uso de automatización para permitir la actualización

Control CIS	Descripción
	rápida de la defensa, la recopilación de datos y la acción correctiva.
9- Limitación y control de puertos de red, protocolos y servicios	Administrar (rastrear/controlar/corregir) el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.
10: Capacidad de recuperación de datos	Los procesos y herramientas utilizadas para respaldar adecuadamente la información crítica con una metodología comprobada para la recuperación oportuna de la misma.
11- Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	Establecer, implementar y gestionar activamente (rastrear, reportar, corregir) la configuración de seguridad de la infraestructura de red utilizando un proceso de gestión de configuración y control de cambios riguroso para prevenir que los atacantes exploten servicios y configuraciones vulnerables.
12- Defensa de borde	Detectar/prevenir/corregir el flujo de información que transfieren redes de diferentes niveles de confianza con un enfoque en datos que dañan la seguridad.
13- Protección de datos	Los procesos y herramientas utilizadas para prevenir la exfiltración de datos, mitigar el efecto de la exfiltración de datos y asegurar la privacidad e integridad de la información sensible.
14- Control de acceso basado en la necesidad de conocer	Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen una necesidad y derecho a acceder a estos activos críticos basado en una clasificación aprobada.
15- Control de acceso inalámbrico	Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el uso seguro de las redes de área local inalámbricas (WLAN), puntos de acceso y sistemas de clientes inalámbricos.

Control CIS	Descripción
16- Monitoreo y control de cuentas	Gestione activamente el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen.
17- Implementar un programa de concienciación y entrenamiento de seguridad	Para todos los roles funcionales en la organización (priorizando aquellos que son misionales para la organización y su seguridad), identificar los conocimientos, habilidades y capacidades específicos necesarios para soportar la defensa de la empresa; desarrollar y ejecutar un plan integral para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concienciación.
18- Seguridad del software de aplicación	Gestione el ciclo de vida de seguridad de todo el software interno desarrollado y adquirido para prevenir, detectar y corregir las debilidades de seguridad.
19- Respuesta y manejo de incidentes	Proteger la información de la organización, así como su reputación, desarrollando e implementando una infraestructura de respuesta a incidentes (por ejemplo, planes, funciones definidas, capacitación, comunicaciones, supervisión de la gestión) para descubrir rápidamente un ataque y luego contener de manera efectiva el daño, erradicando la presencia del atacante y restaurando la integridad de la red y los sistemas.
20- Pruebas de penetración y ejercicios de equipo rojo	Probar la fortaleza general de la defensa de una organización (la tecnología, los procesos y las personas) simulando los objetivos y las acciones de un atacante.

Fuente: CIS (2019).

2.10 Análisis de la literatura revisada

Tabla 5

Análisis literatura revisada

Modelo de referencia	Aporte para el diseño del modelo de ciber-resiliencia organizacional
Marco de Ingeniería de Ciber-resiliencia (Deborah Bodeau et al., 2011).	Plantea en detalle las metas y los objetivos que deben apalancar la ciber-resiliencia en las organizaciones y la forma en que los objetivos están respaldados en un conjunto de prácticas de resiliencia cibernética. El marco se enfoca en estrategias y prácticas arquitectónicas, enfatizando en los sistemas de información. Este marco permite entender en detalle el concepto de ciber-resiliencia y aporta al modelo de madurez de ciber-resiliencia las metas de anticipar, resistir, recuperarse y evolucionar, así como prácticas clave que las organizaciones deben implementar. Este modelo tiene un enfoque muy marcado hacia tecnología de información, siendo necesario complementarlo para que consideren todos los activos y ciberactivos críticos para la misión organizacional.
Principios de diseño de ciber-resiliencia (Deborah Bodeau & Graubart, 2017)	Este documento presenta un conjunto representativo de principios de diseño para la ciber-resiliencia que se puede aplicar en una variedad de entornos. Estos principios están definidos por disciplinas de ingeniería especializadas y son una declaración concisa o una frase que identifica un concepto clave y la descripción de cómo se aplica este concepto al diseño de un sistema que considera no sólo la tecnología, sino los procesos y procedimientos operativos. El contenido del documento facilita en gran medida el entendimiento de la ciber-resiliencia, las disciplinas que la apoyan, los principios y prácticas que puede implementar una organización. La completitud de esta referencia radica en los principios hacen que se tenga una visión integral de la organización en la protección de los activos y ciberactivos críticos para la misión organizacional, independiente que se trate de tecnología de información o tecnología de operación o internet de las cosas IoT. Este documento da una orientación a las organizaciones para focalizar sus esfuerzos, por lo que los principios

Modelo de referencia	Aporte para el diseño del modelo de ciber-resiliencia organizacional
	representativos de diseño de ciber-resiliencia y sus disciplinas asociadas, deben ser tomados como referencia para la formulación del modelo de madurez de ciber-resiliencia organizacional.
Modelo de gestión de resiliencia CERT (Caralli et al., 2016)	Este modelo de madurez de la capacidad para administrar la resiliencia operativa permite a la organización aplicar un enfoque de mejora de procesos para la gestión de la resiliencia operativa. Sus 26 áreas de proceso describen en detalle los objetivos y prácticas que la organización debe implementar para administrar la resiliencia operativa. Para el diseño del modelo de madurez de ciber-resiliencia organizacional este documento puede aportar con las prácticas contenidas en algunas de sus áreas de proceso.
Modelo de indicadores para la mejora de la ciber-resiliencia (IMC) (CERTSI, n.d.)	El modelo presenta un conjunto de indicadores que permiten a la organización medir su nivel de madurez en cuanto a la ciber-resiliencia. Para el diseño del modelo de madurez de ciber-resiliencia este documento aporta en la identificación de la forma como evolucionan las competencias organizacionales de ciber-resiliencia.
Modelo de madurez de continuidad del negocio (BCMM, 2012).	Este modelo apoya a las organizaciones en la definición de un programa de continuidad del negocio. La estructuración del modelo en lo que respecta a el "Modelo Comparativo" y los descriptores de los niveles de madurez, sirven como referencia para la estructuración del modelo de madurez de ciber-resiliencia organizacional.
Modelo de madurez de la comunidad de ciberseguridad (CCSMM) (White, 2011).	Este modelo esta focalizado en evaluar la madurez de la ciberseguridad en los estados o comunidades. Para el caso del diseño del modelo de madurez de ciber-resiliencia, no se tomará este documento como referencia.
Marco para la mejora de la ciberseguridad en infraestructuras críticas (NIST, 2018)	El marco está enfocado en reducir el riesgo vinculado a las amenazas cibernéticas. Este marco tiene como foco la ciberseguridad por lo que su aporte al modelo de ciber-

Modelo de referencia	Aporte para el diseño del modelo de ciber-resiliencia organizacional
	resiliencia está relacionado con las prácticas asociadas a esta disciplina.
Modelo de madurez de la capacidad de ciberseguridad C2M2 (Christopher et al., 2014)	Este modelo de madurez tiene como foco la mejora de las capacidades de ciberseguridad. Las prácticas de sus dominios pueden ser consideradas en el modelo de madurez de ciber-resiliencia organizacional.
Controles de Ciberseguridad del CIS (CIS, 2019)	El documento contiene un conjunto de prácticas de defensa que mitigan los ataques más comunes contra sistema y redes. En lo que respecta al modelo, de este documento se pueden tomar prácticas para incluir en el modelo de madurez de ciber-resiliencia organizacional.

Fuente: elaboración propia.

De la literatura revisada, es de gran aporte para la definición de la propuesta de modelo de madurez de ciber-resiliencia organizacional, el documento de principios de diseño de ciber-resiliencia (Deborah Bodeau & Graubart, 2017). Este documento considera unas disciplinas de ciber-resiliencia y así mismo, describe en detalle unos principios de diseño de ciber-resiliencia que pueden orientar a las organizaciones en la implementación de prácticas que apoyen el desarrollo de las capacidades de ciber-resiliencia. Los niveles de madurez planteados en el modelo CMMI para desarrollo (SEI, 2010) sirven para orientar la estructuración de los niveles de madurez del modelo a proponer. Así mismo, el modelo de madurez de continuidad del negocio (BCMM, 2012) puede orientar la definición de un modelo comparativo y descriptores de cada nivel de madurez.

3. Bases para la definición de la propuesta de un modelo de madurez de ciber-resiliencia organizacional

3.1 ¿Por qué formular una propuesta de un modelo de madurez de ciber-resiliencia organizacional?

Los modelos de evaluación de la madurez de ciber-resiliencia organizacional identificados en las fuentes de información consultadas, hacen referencia a una ciber-resiliencia que tiene un fuerte énfasis en la implementación efectiva de buenas prácticas de ciberseguridad para afrontar ataques cibernéticos tradicionales realizados por atacantes convencionales. Los ataques tradicionales son comúnmente perpetrados por un solo atacante, con múltiples objetivos que incluyen personas o entidades, con el propósito de obtener beneficios financieros o reconocimientos, con ejecución de un ataque comúnmente en un solo intento y por un breve período de tiempo (Cortés Novoa, 2017).

Sin desconocer el valor del enfoque de los modelos consultados, es importante señalar la importancia de que la ciber-resiliencia sea abordada en la organización, desde el diseño de la arquitectura tecnológica que soporta las funciones críticas, de tal forma que se prepare para afrontar tanto ataques convencionales, como ataques tipo amenazas persistentes avanzadas. Esta visión permitirá a la organización actuar en concordancia con la realidad actual, donde se ve que los ataques están siendo perpetrados por grupos organizados con alta disponibilidad de recursos y patrocinio, cuyo objetivo de ataque son organizaciones específicas con información relevante de propiedad intelectual, gubernamental y de seguridad nacional o que operan infraestructuras críticas. Este tipo de atacantes tienen como propósito el espionaje, obtener avances competitivos o beneficios estratégicos o inclusive apoyar una guerra, con una ejecución de ataques que se hace en múltiples intentos dentro de un largo período de tiempo (Cortés Novoa, 2017).

Cuando una organización aborda la ciber-resiliencia desde el diseño, tiene un enfoque más preventivo, que le permite adelantarse a las situaciones que puedan ocurrir y en ese sentido, plantear acciones que mejoren la respuesta a la situación prevista, para evitar que una interrupción prologada de una función crítica, ponga en riesgo la continuidad del negocio. Incluir como parte de la propuesta de un modelo de madurez de ciber-resiliencia unos

principios de diseño, permite recopilar la experiencia que la organización puede utilizar para guiar decisiones de análisis y diseño. Un principio toma forma de una declaración concisa o una frase que identifica un concepto clave que orienta la organización en el diseño de sus sistemas, incluidos sus procesos y procedimientos operativos. Un principio de diseño puede, además de guiar las decisiones de diseño, guiar el análisis de cómo y con qué eficacia un determinado diseño o el sistema implementado aplica el principio (Deborah Bodeau & Graubart, 2017). Los principios de diseño generalmente están definidos por unas disciplinas de ingeniería especializadas, que en el caso de la ciber-resiliencia, son las disciplinas de ciberseguridad, resistencia y supervivencia, amenazas persistentes avanzadas y evolución.

3.2 Mapa conceptual de las bases para la definición del modelo

El siguiente mapa resume los conceptos clave que se deben considerar para la definición de la propuesta del modelo de madurez de ciber-resiliencia organizacional.

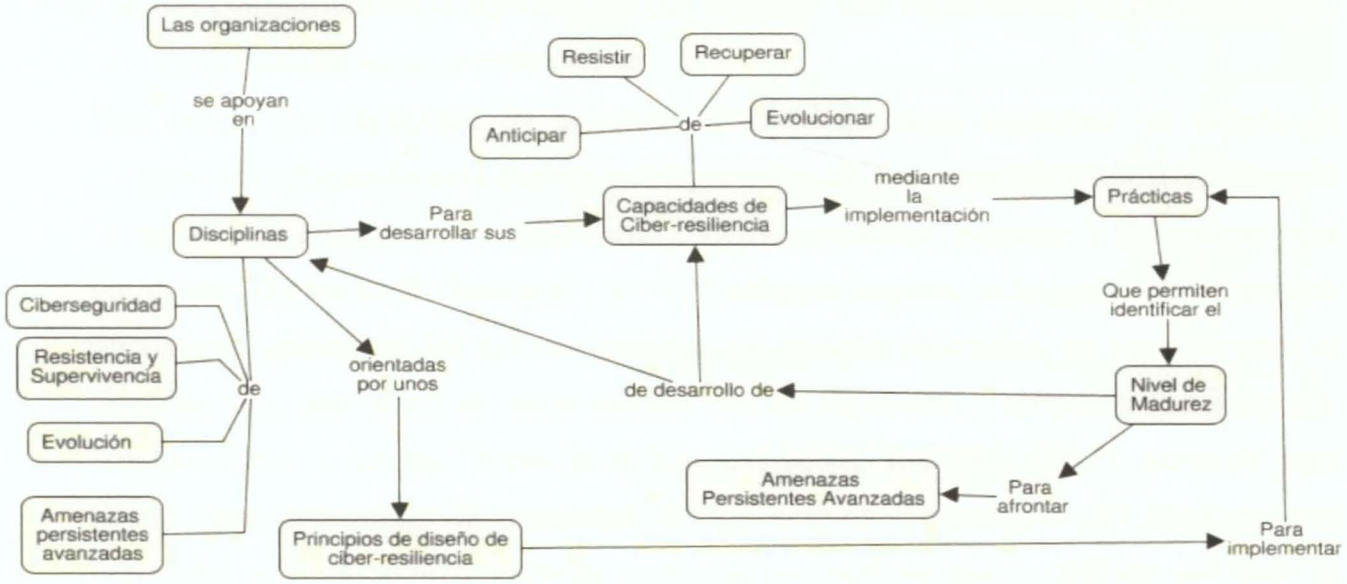


Figura 2. Mapa conceptual de las bases del modelo de madurez de ciber-resiliencia propuesto

Fuente: elaboración propia.

Las organizaciones se apoyan en las disciplinas de ciberseguridad, supervivencia y resistencia, evolución y amenazas persistentes avanzadas para desarrollar sus capacidades de ciber-resiliencia de anticipar, resistir, recuperarse y evolucionar; mediante la implementación de prácticas que permiten identificar el nivel de madurez en el desarrollo de las capacidades de ciber-resiliencias y las disciplinas que la apoyan. Las disciplinas están orientadas por unos principios de diseño para implementar prácticas que desarrollan las capacidades de ciber-resiliencia organizacional.

3.3 Capacidades organizacionales asociadas a la ciber-resiliencia

Teniendo en cuenta las definiciones de ciber-resiliencia (CERTSI, n.d.) y de las capacidades organizacionales (Dávila, 2013), se identificaron cuatro capacidades clave para desarrollar habilidades que le permitan a la organización enfrentar condiciones adversas relacionadas con ataques a sus recursos cibernéticos críticos para la misión organizacional, de tal forma que no se vea comprometida la continuidad del negocio. Las capacidades identificadas son: anticipar, resistir, recuperarse y evolucionar.

- ***Anticipar***: La capacidad de anticipar tiene como meta mantener un estado de preparación informada para prevenir compromisos de funciones de misión del negocio de ataques de adversarios y tiene como objetivos predecir, prevenir y prepararse para los ataques (Deborah Bodeau et al., 2011). Anticipar implica, en lo que respecta a ciber-resiliencia, identificar los activos críticos, sus riesgos asociados, su impacto para el negocio, y la asociación de estos activos con las funciones y servicios que soportan. Análisis como el de las "Joyas de la Corona" (CJA) (MITRE, 2017) serán de gran ayuda para determinar la criticidad de los activos cibernéticos. El foco de esta capacidad es la implementación de controles preventivos que se definen con base en un conocimiento detallado de la organización, los riesgos que pueden afectar su misión, sus funciones críticas y su relación con las tecnologías que las soportan. Para el desarrollo de esta capacidad es importante contar con herramientas de ciber-inteligencia que le permitan a la organización tener conocimiento del entorno, las amenazas y vulnerabilidades de la tecnología, así como las técnicas utilizadas por los

atacantes. En términos generales, podemos decir que esta capacidad involucra un conocimiento en detalle de la organización y del entorno cibernético y sus amenazas asociadas para implementar controles preventivos.

- ***Resistir***: La capacidad de resistir tiene como meta continuar las funciones esenciales de la misión del negocio a pesar de la ejecución exitosa de un ataque por un adversario. Tiene como objetivos combatir los ataques cibernéticos manteniendo la funcionalidad esencial para la misión del negocio en presencia de acciones adversas, y contener o derrotar acciones adversas (Deborah Bodeau et al., 2011). Esta capacidad requiere la implementación de medidas para preparar a la organización para responder los ataques a los ciber-activos críticos para la misión organizacional y la implementación de estrategias que permitan que las funciones críticas del negocio continúen operando a pesar de ser objeto de un ataque cibernético. La identificación de los requisitos de resiliencia de los ciberactivos críticos es clave para el desarrollo de esta capacidad, para lo cual resulta de gran ayuda el contar con herramientas como análisis de modos de fallas FMECA (Ali & Hong, 2018) y los análisis de impacto de ciber-ataques CMIA (Musman, Temin, Tanner, Fox, & Pridemore, 2011). Considera la implementación de medidas como la redundancia, los métodos de tolerancia a fallos, la respuesta adaptativa, la defensa en profundidad, técnicas de engaño al adversario, capacitación y formación de equipos de respuesta a incidentes. Podemos afirmar que esta capacidad tiene foco en la mitigación de las consecuencias de los ataques cibernéticos e implementa controles que pueden catalogarse más como correctivos.
- ***Recuperarse***: La capacidad de recuperarse tiene como meta restaurar las funciones críticas del negocio en la mayor medida de lo posible luego de un ataque cibernético exitoso y tiene como objetivos determinar los daños, restaurar las capacidades y determinar la confiabilidad (Deborah Bodeau et al., 2011). Recuperarse implica, adicional a las estrategias de respaldo y recuperación, contar con estrategias que permitan contar con formas alternativas de proporcionar la funcionalidad crítica requerida, de modo que, si un componente es comprometido, se pueden utilizar uno o más componentes alternativos que proporcionan la misma funcionalidad. La recuperación de las funciones críticas para la misión debe hacerse en un tiempo que no

afecte a la continuidad del negocio, por lo que la definición de la estrategia de recuperación de desastres debe considerar el análisis de impacto del negocio BIA y los requisitos de recuperación que se identifican en este análisis.

- ***Evolucionar***: La capacidad de evolucionar tiene como meta realizar cambios organizacionales para minimizar los impactos adversos de los ataques reales o previstos y tiene como objetivos transformar los procesos y comportamientos existentes y diseñar una arquitectura tecnológica que mitigue el impacto de los ataques cibernéticos (Bodeau et al., 2011). Para el desarrollo de esta capacidad se implementan prácticas como: mecanismos para cambiar o interrumpir la superficie de ataque (MTD) (McDaniel et al., 2014); técnicas de engaño e imprevisibilidad destinados a aumentar la incertidumbre de los adversarios acerca de la estructura y comportamiento de los sistemas organizacionales, y se utilizan juegos de ciberseguridad (CSG) (Musman y Turner, 2018) para modelado de ataques y métodos de defensa. En términos generales, la capacidad de evolucionar tiene como foco la implementación de estrategias organizacionales para adaptar los procesos, procedimientos y tecnología de forma continua con el propósito de minimizar el riesgo de los ataques cibernéticos.

3.4 Principios representativos de diseño de ciber-resiliencia

Para la definición de la propuesta del modelo de madurez de ciber-resiliencia organizacional, se tomó como referencia, los principios representativos de diseño de ciber-resiliencia definidos por el MITRE (Deborah Bodeau & Graubart, 2017). Tal como lo muestra la figura 3, los principios son clave para alinear las disciplinas seguridad, ingeniería de resiliencia y supervivencia, evolución, y amenazas persistentes avanzadas.

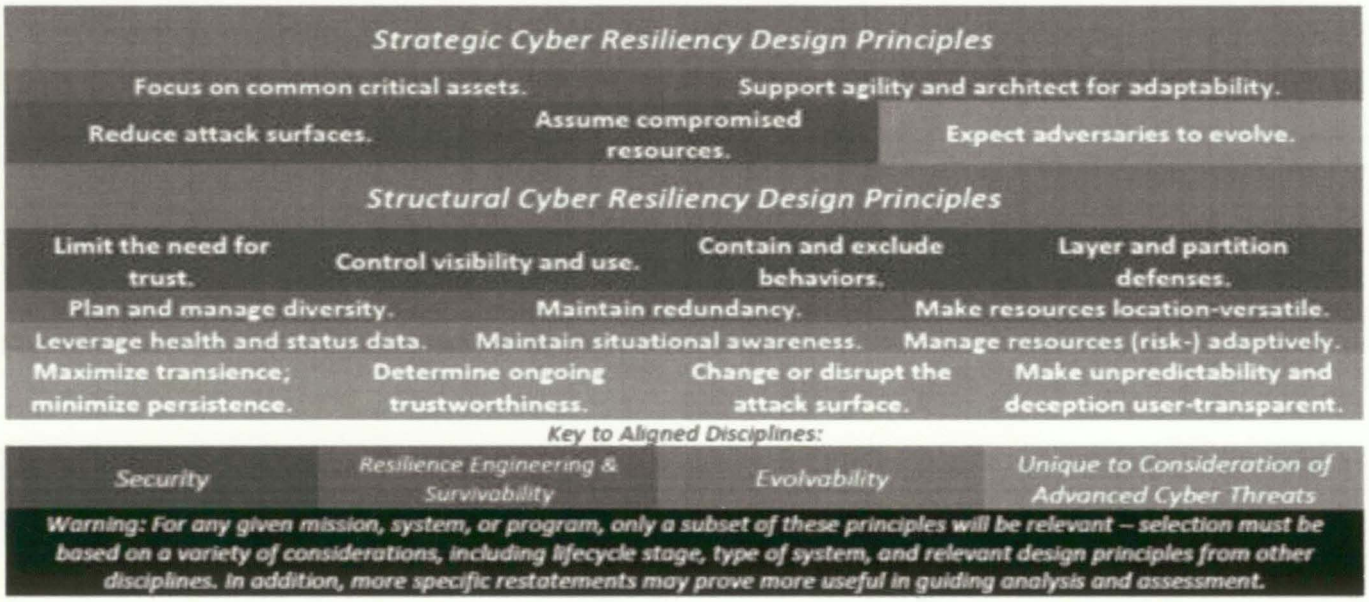


Figura 3. Principios representativos de diseño de ciber-resiliencia

Fuente: (Deborah Bodeau & Graubart, 2017)

Los principios de diseño de ciber-resiliencia orientan a la organización para focalizar sus esfuerzos cuando está desarrollando sus capacidades de ciber-resiliencia. Las capacidades de ciber-resiliencia están relacionadas con los principios de diseño estratégicos que son abordados por el MITRE (Bodeau y Graubart, 2017), como se muestra en la tabla 6.

Tabla 6

Principios estratégicos de diseño vs. capacidades organizacionales de ciber-resiliencia

Principio de diseño Estratégico	Capacidad organizacional			
	Anticipar	***Resistir***	***Recuperarse***	***Evolucionar***
Centrarse en activos críticos comunes	X	X	X	
Soportar agilidad y diseñar para la adaptación			X	X
Reducción de la superficie de ataque	X			

Principio de diseño Estratégico	Capacidad organizacional			
	Anticipar	***Resistir***	***Recuperarse***	***Evolucionar***
Dudar de la fiabilidad de todos los recursos técnicos	X	X		
Esperar que los adversarios evolucionen	X			X

Fuente: Bodeau y Graubart (2017). Traducción propia.

Los principios de diseño estratégicos están a su vez relacionados con los principios de diseño estructurales de ciber-resiliencia, tal como se muestra en la tabla 7.

Tabla 7

Principios estratégicos de diseño vs. principios estructurales de diseño

PRINCIPIOS ESTRUCTURALES DE DISEÑO	PRINCIPIOS ESTRATÉGICOS DE DISEÑO				
	Centrarse en los activos críticos y comunes	Soportar la agilidad y diseñar para adaptarse	Reducción de la superficie de ataque	Dudar de la fiabilidad de todos los recursos técnicos	Esperar que los adversarios evolucionen
Limitar la confianza por defecto			X	X	
Limitación de la visibilidad	X		X	X	
Contención y exclusión de comportamientos anómalos	X			X	X
Defensa en profundidad (capas) y segmentación de los medios	X			X	
Planificar y gestionar la diversidad	X	X		X	
Mantener redundancia	X	X			
Hacer localización de los recursos versátil	X	X			X
Aprovechamiento de la información de los indicadores de ciberseguridad	X			X	X

PRINCIPIOS ESTRUCTURALES DE DISEÑO	PRINCIPIOS ESTRATÉGICOS DE DISEÑO				
	Centrarse en los activos críticos y comunes	Soportar la agilidad y diseñar para adaptarse	Reducción de la superficie de ataque	Dudar de la fiabilidad de todos los recursos técnicos	Esperar que los adversarios evolucionen
Mantener la conciencia situacional	X	X			X
Gestionar los riesgos de los recursos de forma adaptativa	X	X			X
Maximizar la transitoriedad; minimizar la persistencia			X	X	X
Validación periódica o continua de la integridad	X			X	X
Cambiar o interrumpir la superficie de ataque			X	X	X
Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario					X

Fuente: Bodeau y Graubart (2017). Traducción propia.

3.5 Organización preparada para afrontar amenazas persistentes avanzadas

El Departamento de Defensa de Estados Unidos desarrolló una jerarquía de amenazas para describir las capacidades de los atacantes potenciales, organizada por nivel de habilidades y amplitud de recursos disponibles. Los atacantes de los niveles I y II explotan principalmente vulnerabilidades conocidas; los atacantes de los niveles III y IV están mejor financiados y tienen un nivel de experiencia y sofisticación suficiente para descubrir nuevas vulnerabilidades en los sistemas y explotarlas, y finalmente los atacantes de los niveles V y VI pueden invertir grandes cantidades de dinero (miles de millones) y tiempo (años) para crear vulnerabilidades en los sistemas, incluidos los sistemas que de otro modo estarían fuertemente protegidos (Department of Defense, United States of America, 2013). Estos expertos están dando alerta a las organizaciones de la necesidad de estar preparadas no solo frente a los atacantes convencionales ubicados en los niveles I y II, sino también para los atacantes de los niveles III y superiores, que pueden considerarse como atacantes avanzados,

de los que se pueden prever ataques que traigan como consecuencia una interrupción grave de los sistemas de información y las tecnologías de operación, poniendo en riesgo la continuidad del negocio.

Los atacantes avanzados realizan ataques que se configuran como amenazas persistentes avanzadas. Tal como lo indica Betjlich (2010), cuando hablamos de amenazas persistentes avanzadas, el término amenaza significa que el atacante no es una pieza de código sin sentido; él está motivado, financiado y organizado, buscando un objetivo particular, para lo cual estará bien rodeado y asistido con el fin de lograr la misión designada. El término persistente hace referencia a que el adversario tiene una tarea que cumplir e insistirá en lograrla, manteniendo el nivel de interacción necesario para alcanzar su objetivo. El término avanzada significa que el adversario puede operar un amplio espectro de posibles intrusiones, utilizando no solo las vulnerabilidades más evidentes y publicitadas, sino que puede investigar o desarrollar nuevas debilidades o fallas derivadas de las prácticas de seguridad y control de la empresa objetivo.

Un modelo de madurez de ciber-resiliencia debe considerar prácticas que preparen a la organización para afrontar tanto ataques perpetrados por adversarios convencionales, como para afrontar las amenazas persistentes avanzadas que son perpetradas por los adversarios avanzados. Es necesario un modelo que considere no solo la mejora de la gobernanza del riesgo para hacer que el riesgo cibernético sea parte del riesgo organizacional, los procedimientos de respuesta a incidentes, el monitoreo e intercambio de información sobre amenazas y la higiene cibernética; sino que también incluya aspectos de arquitectura e ingeniería que desde el diseño de las tecnologías de información y de operación permitan preparar a la organización para afrontar las amenazas persistentes avanzadas (Bodeau y Graubart, 2017).

3.6 Prácticas que evidencian el desarrollo de las capacidades organizacionales de ciber-resiliencia

Para la identificación de las prácticas que las organizaciones implementan para fortalecer sus capacidades de ciber-resiliencia, se partió de asociar a cada principio de diseño de ciber-

resiliencia los recursos analíticos relevantes indicados por el MITRE (Bodeau y Graubart, 2017), extractando los documentos de referencia y en los mismos, identificando las prácticas relacionadas, tal como se muestra a continuación.

Tabla 8

Identificación de prácticas del modelo de madurez de ciber-resiliencia organizacional

Principio de diseño estratégico de ciber-resiliencia	Documento	Prácticas Identificadas
Centrarse en los activos críticos comunes.	Guía de planificación de contingencias para sistemas de información federales (Swanson, Bowen, Phillips, Gallup y Lynes, 2015). Pasos a seguir para realizar un análisis de impacto en nuestro negocio (INCIBE, 2017).	Análisis de Impacto del Negocio (BIA) Planes de Contingencia para sistemas de bajo impacto, Impacto Moderado, Alto impacto.
Centrarse en los activos críticos comunes.	Análisis de las joyas de la corona (MITRE, 2017).	Análisis de las joyas de la corona. Crown Jewels Analysis (CJA) que es un proceso para identificar los activos cibernéticos que son más críticos para el cumplimiento de la misión de una organización.
Centrarse en los activos críticos comunes.	Análisis Meca (Evans, 1987; Ali y Hong, 2018).	El Análisis Modal de Fallos y Efectos (FMECA) es una metodología cuya finalidad es estudiar los posibles fallos futuros ("modos de fallo") de un producto para posteriormente clasificarlos según su importancia.

Principio de diseño estratégico de ciber-resiliencia	Documento	Prácticas Identificadas
Centrarse en los activos críticos comunes.	Evaluación del impacto de los ciberataques en las misiones (Musman et al., 2011).	Evaluación impacto de ciberataques en la misión (CMIA).
Soportar agilidad y diseñar para adaptarse	Un marco multidisciplinario para la resiliencia a desastres y disrupciones (Jackson, 2007).	Adaptabilidad que permite más opciones de operación del sistema (identificar las condiciones de adaptabilidad que debe soportar el sistema).
Reducción de la superficie de ataque	Controles de seguridad y privacidad para sistemas de información federal y organizaciones (NIST, 2013).	La reducción de la superficie de ataque incluye, por ejemplo, aplicar el principio de privilegio mínimo, emplear defensas en capas, aplicar el principio de funcionalidad mínima (es decir, restringir puertos, protocolos, funciones y servicios), desaprobar funciones inseguras y eliminar interfaces de programación de aplicaciones (API) que son vulnerables a los ciberataques.
Reducción de la superficie de ataque	Cinco maneras de reducir la superficie de ataque (Security, 2018).	Reducción de la complejidad de la red, control y monitoreo de los *end-point* (puntos finales), segmentación de la red como una medida para controlar el tráfico hacia los activos cibernéticos críticos para la organización. Monitoreo de transacciones u operaciones realizadas por el administrador y operador de los activos cibernéticos. Monitoreo periódico de la infraestructura.

Principio de diseño estratégico de ciber-resiliencia	Documento	Prácticas Identificadas
Dudar de la fiabilidad de todos los recursos técnicos.	Ciber-resiliencia y NIST. Publicación especial 800-53 Rev.4 Controles (Bodeau y Graubart, 2013).	Solo se importa software confiable al que se le ha verificado su legitimidad. Se implementan prácticas de integridad comprobada. Se protegen los entornos de gestión u operaciones contra ataques de *phishing*. Se implementan prácticas de falla en modo seguro (control de errores). Se implementan prácticas de separación/segmentación de componentes. Se diseña para tolerar el compromiso de recursos.
Limitar la confianza por defecto.	Principios de diseño de ciber-resiliencia (Bodeau y Graubart, 2017).	Prácticas de validación de datos y el comportamiento para detectar actividades maliciosas (evidencia de compromiso). Se tiene la capacidad de certificación o garantía de los atributos de confiabilidad de un elemento del sistema. Se identifican los componentes del sistema que pueden ser eslabones débiles para la ciberseguridad y se aumenta la seguridad en estos puntos (componentes, personas, procedimientos). Se desarrollan capacidades de ciberinteligencia.
Limitar la confianza por defecto	Arquitectura Zero Trust (Rose, Borchert, Mitchell, y Connelly, 2019).	La arquitectura que soporta la infraestructura tecnológica está basada en el principio Zero Trust.
Limitación de la visibilidad	Principios de diseño de ciber-resiliencia (Bodeau y Graubart, 2017).	Se restringe la visibilidad externa de los comportamientos del sistema.

Principio de diseño estratégico de ciber-resiliencia	Documento	Prácticas Identificadas
Contención y exclusión de comportamientos anómalos.	Principios de diseño de ciber-resiliencia (Bodeau y Graubart, 2017).	Se cuenta con mecanismos para deshabilitar cualquier elemento del sistema que no sea de misión crítica que exhiba un comportamiento sospechoso. Se cuenta con mecanismos para restricción o contención de actividades sospechosas, a priori o dinámicamente. Mecanismos de aislamiento estático y dinámico.
Defensa en profundidad (capas) y segmentación de los medios	Defensa en profundidad aplicado a un entorno empresarial (Guijarro, Yepez, Peralta y Ortiz, 2018).	Mecanismos para la partición estática y dinámica de elementos de los activos cibernéticos. Defensa en profundidad: "integrando capacidades de personas, tecnología y operaciones para establecer barreras variables a través de múltiples capas y misiones".
Espere que los adversarios evolucionen	Un enfoque orientado al juego para minimizar el riesgo de ciberseguridad (Musman y Turner, 2018).	Utilización de juegos de ciberseguridad (CSG) para modelado de ataques y métodos de defensa.
Espere que los adversarios evolucionen	Modelado, simulación, experimentación y juegos de guerra valorando un escenario común (Page, 2016).	Juegos de guerra para entrenamiento del personal.
Espere que los adversarios evolucionen.	Ciber-resiliencia y NIST. Publicación especial 800-53 Rev.4 Controles(Bodeau y Graubart, 2013).	Técnicas de engaño del adversario.

Principio de diseño estratégico de ciber-resiliencia	Documento	Prácticas Identificadas
Espere que los adversarios evolucionen.	Tácticas del adversario, técnicas y conocimiento común (Att y Strom, 2015).	Se conocen las tácticas y técnicas comunes usadas por el adversario.
Espere que los adversarios evolucionen.	Comprendiendo los ataques cibernéticos (PANDA, s.f.)	Hay un entendimiento del ciclo de vida de los ataques cibernéticos (*ciber kill chain*).
Maximizar la transitoriedad; Minimizar la persistencia.	Construyendo arquitecturas seguras y resilientes para el aseguramiento de la misión cibernética (Domenig, 2009).	Se implementan prácticas de no persistencia (se retiene información, servicios y conectividad por un tiempo limitado, reduciendo así la exposición a corrupción, modificación o usurpación).
Validación periódica o continua de la integridad.	Principios de diseño de ciber-resiliencia (Bodeau y Graubart, 2017).	Se emplean servicios para validar la integridad de configuraciones, módulos de software, y datos críticos.
Cambiar o interrumpir la superficie de ataque.	Técnicas de defensa del blanco móvil: una encuesta (Lei, Zhang, Tan, Zhang, y Liu, 2018).	Defensa cibernética en movimiento (MTD).
Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario.	Principios de diseño de ciber-resiliencia (Bodeau y Graubart, 2017).	Técnicas de imprevisibilidad destinados a aumentar la incertidumbre de los adversarios - acerca de estructura y comportamiento del sistema.
Planificar y gestionar la diversidad.	Análisis cuantitativo de ciberdefensas activas basadas en diversidad de plataforma temporal (Carter, Okhravi y Riordan, 2014).	Técnicas de diversidad de plataforma para eliminar puntos específicos de ataque que comprometan los activos críticos organizacionales.

Principio de diseño estratégico de ciber-resiliencia	Documento	Prácticas Identificadas
Mantener redundancia	Resiliencia y supervivencia en las redes de comunicación: estrategias, principios y encuesta de disciplinas (Sterbenz et al., 2010).	Implementación de redundancia como estrategia de tolerancia a fallos para los activos críticos.
Hacer localización de los recursos versátil	Uso de replicación para resiliencia (Bougeret, Casanova, Robert, Vivien y Zaidouni, 2014).	Mecanismos para lograr ubicación versátil de los recursos para evitar puntos únicos de falla en sistemas que requieren alta disponibilidad.
Aprovechamiento de la información de los indicadores de ciberseguridad.	Marco para el diseño de un Centro de operación de seguridad (Schinagl, Schoon y Paans, 2015).	Centro de operaciones de ciberseguridad (SOC) encargado de realizar seguimiento y analizar la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.
Aprovechamiento de la información de los indicadores de ciberseguridad.	La absoluta guía para SIEM	Se cuenta con correlación avanzada y profunda de eventos, con interface para obtener *logs* de los activos cibernéticos críticos (ERP, CRM, etc.) con herramientas como SIEM.
Mantener la conciencia situacional.	La conciencia situacional en la ciberdefensa (Pérez y Fernández, 2013).	Conciencia situacional.
Gestionar los riesgos de los recursos de forma adaptativa.	La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial	Se analizan y gestionan riesgos para amenazas conocidas, focales, latentes y emergentes.

Principio de diseño estratégico de ciber-resiliencia	Documento	Prácticas Identificadas
	(Cano, 2017).	

Fuente: elaboración propia.

Una vez identificadas las prácticas para cada principio de ciber-resiliencia, se identificó para cada práctica la capacidad de ciber-resiliencia que desarrollaba. Cada práctica se ubicó en niveles de esfuerzo para su implementación, siendo el nivel 1 el nivel que requiere menos esfuerzo de implementación y el nivel 5, el nivel con mayor esfuerzo de implementación. Cada nivel de esfuerzo corresponde a los niveles de madurez a plantear en el modelo.

3.7 Niveles de madurez de ciber-resiliencia organizacional

Para la definición de los niveles de madurez del modelo, se tomaron como referencia los definidos por el Software Engineering Institute (SEI) en su modelo CMMI (SEI, 2010), indicando para cada nivel el estado esperado de desarrollo de las capacidades de ciber-resiliencia. A continuación, se describen los niveles de madurez a considerar en el modelo:

- **Nivel 1-Inicial**: los procesos son generalmente *ad hoc* y caóticos, sin que la organización proporcione un entorno estable para dar soporte a los procesos (SEI, 2010). En lo que respecta a la ciber-resiliencia, se han implementado prácticas que son la base para iniciar el desarrollo de las capacidades de ciber-resiliencia.
- **Nivel 2-Gestionado**: se empieza a evidenciar la planificación y ejecución de acuerdo con las políticas, el empleo de personal cualificado y recursos adecuados para producir resultados controlados; involucra a las partes interesadas relevantes; se monitorea,

controla y revisa; se evalúa la adherencia a la descripción del proceso (SEI, 2010). En lo que respecta a la ciber-resiliencia se inicia a desarrollar la capacidad de anticipar.

- **Nivel 3-Definido**: los procesos están caracterizados, comprendidos y se describen en estándares, procedimientos, herramientas y métodos. En comparación con el nivel 2, el nivel 3 describe el proceso más rigurosamente, se establece claramente el propósito, entradas, criterios de entradas, actividades, roles, medidas, etapas de verificación, salidas y criterios de salidas (SEI, 2010). En lo que respecta a la ciber-resiliencia, la capacidad de anticipar está desarrollada y se comienzan a desarrollar las capacidades de responder y recuperar.
- **Nivel 4-Gestionado Cuantitativamente**: se establecen objetivos cuantitativos para la calidad y el rendimiento del proceso, utilizados como criterios para la gestión. Estos objetivos se basan en las necesidades del cliente, usuarios finales, organización e implementación del proceso (SEI, 2010). En lo que respecta a la ciber-resiliencia, las capacidades de anticipar, responder y recuperar están desarrolladas; la capacidad de evolucionar está iniciando.
- **Nivel 5-En Optimización**: la organización mejora continuamente sus procesos basándose en una comprensión cuantitativa de sus objetivos de negocio y las necesidades de rendimiento (SEI, 2010). En lo que respecta a la ciber-resiliencia, las capacidades de anticipar, responder, recuperar y evolucionar están desarrolladas.

Tomando como referencia el modelo comparativo definido en el modelo de madurez de continuidad del negocio (BCMM, 2012), se identificó que las organizaciones que se encuentren en un nivel 1-Inicial o nivel 2-Gestionado, son organizaciones "en riesgo" de pérdida de continuidad de sus operaciones luego de un ataque cibernético grave. Las organizaciones que se encuentren en niveles de madurez 3-Definido o 4-Gestionado cuantitativamente son organizaciones "ejecutantes competentes", y las organizaciones que se encuentren en un nivel 5- En optimización, son organizaciones que se pueden catalogar como "las mejores de la clase".

3.8 Visión integral de las tecnologías

Muchas empresas distinguen entre la seguridad física y de la información, entre IT y Operaciones, entre la gestión de la continuidad del negocio y la protección de datos, y entre la seguridad interna y externa. En la era digital, estas divisiones son obsoletas. La responsabilidad dispersa puede poner en riesgo a toda la organización (Panda Security Summit, 2018). Un modelo de madurez de ciber-resiliencia debe abordar de una manera integral toda la tecnología de la organización que pueda ser blanco de un ataque cibernético, ya sea tecnología de información, tecnología de operación o internet de las cosas, enfocando sus esfuerzos en la protección de los activos y ciberactivos que soportan las funciones del negocio que son críticas para el cumplimiento de la misión organizacional.

3.9 Reflexiones para la formulación del modelo de madurez de ciber-resiliencia organizacional

La ciber-resiliencia organizacional requiere que las organizaciones se apoyen en cuatro disciplinas: ciberseguridad, resistencia y supervivencia, evolución y amenazas persistentes avanzadas. Estas disciplinas en conjunto con los principios de diseño de ciber-resiliencia, dan línea a la organización acerca de hacia dónde enfocar sus esfuerzos en la implementación de prácticas para fortalecer sus capacidades de ciber-resiliencia. Estas disciplinas tienen una estrecha relación entre sí y no están pensadas para actuar de forma independiente; por el contrario, deben tener una interacción dinámica. El nivel de madurez de ciber-resiliencia organizacional puede ser identificado al evaluar las prácticas que la organización ha implementado para desarrollar sus capacidades de ciber-resiliencia. El nivel de madurez de ciber-resiliencia permite identificar el estado de preparación de las organizaciones para afrontar ataques cibernéticos sin poner en riesgo la continuidad del negocio.

4. Propuesta de modelo de madurez de ciber-resiliencia organizacional

4.1 Diseño del modelo

El mapa conceptual que se muestra a continuación resume el diseño de la propuesta de modelo de madurez de ciber-resiliencia organizacional definido.

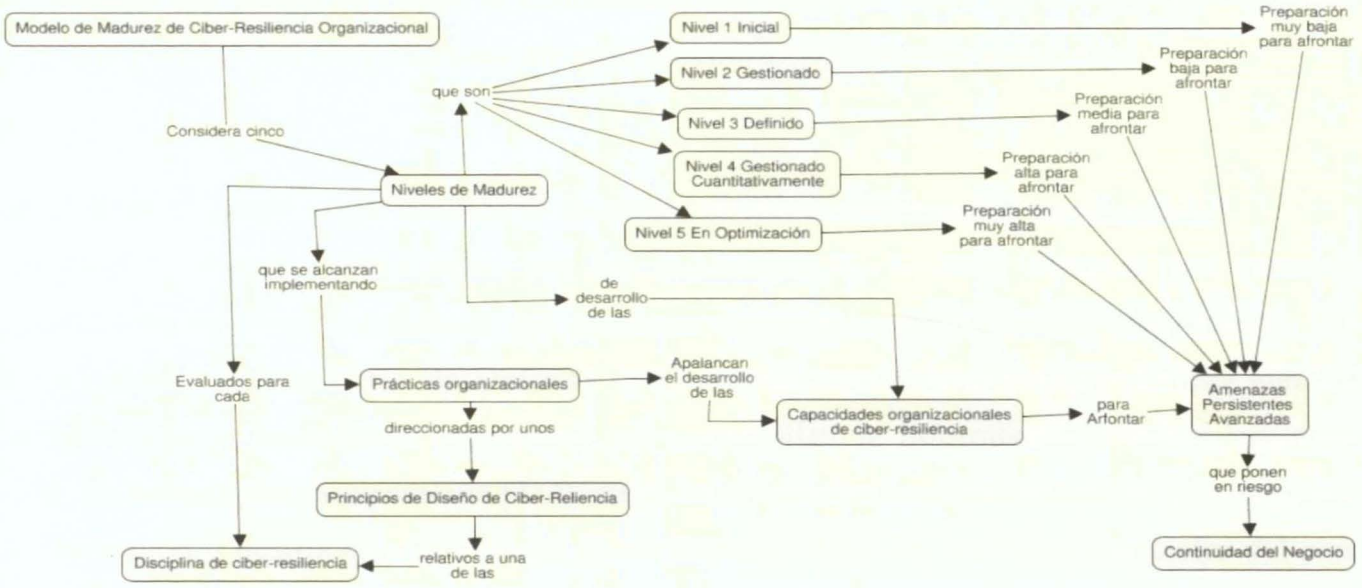


Figura 4. Mapa conceptual diseño del modelo de madurez de ciber-resiliencia organizacional

Fuente: elaboración propia.

El modelo de madurez de ciber-resiliencia organizacional considera cinco niveles de madurez de desarrollo de las capacidades organizacionales de ciber-resiliencia para afrontar amenazas persistentes avanzadas que ponen en riesgo la continuidad del negocio. Los niveles de madurez se alcanzan implementando prácticas organizacionales direccionadas por unos principios de ciber-resiliencia relativos a una de las disciplinas de ciber-resiliencia. Los niveles de madurez son evaluados para cada disciplina de ciber-resiliencia. Los niveles de madurez son nivel 1-Inicial, nivel 2-Gestionado, nivel 3-Definido, nivel 4-Gestionado Cuantitativamente y nivel 5-En optimización.

En el nivel 1-Inicial hay una preparación muy baja para afrontar las amenazas persistentes avanzadas que ponen en riesgo la continuidad del negocio. En el nivel 2-Gestionado hay una

preparación baja para afrontar amenazas persistentes avanzadas que ponen en riesgo la continuidad del negocio. En el nivel 3-Definido hay una preparación media para afrontar amenazas persistentes avanzadas que ponen en riesgo la continuidad del negocio. En el nivel 4-Gestionado cuantitativamente hay una preparación alta para afrontar amenazas persistentes avanzadas que ponen en riesgo la continuidad del negocio. En el nivel 5-En optimización, hay una preparación muy alta para afrontar amenazas persistentes avanzadas.

4.1.1 Público objetivo del modelo de madurez de ciber-resiliencia organizacional

El público objetivo del modelo son las organizaciones a nivel mundial que manejen infraestructura crítica cibernética que pueda ser un objetivo militar en una ciber-guerra. Tal como define el Ministerio de Defensa de Colombia, las infraestructuras críticas son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales del país (José, Hernandez, Estado y Ccoc, 2016). Entendemos por servicios esenciales "Los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del estado y las administraciones públicas" (José et al., 2016).

La infraestructura crítica cibernética tiene unas amenazas que las hacen el público objetivo del modelo de madurez de ciber-resiliencia organizacional propuesto. Estas amenazas están relacionadas con ciberespacio. Las amenazas identificadas para la infraestructura crítica cibernética son: guerra, terrorismo, espionaje, crimen, armas y sabotaje (José et al., 2016).

En Colombia, la infraestructura crítica cibernética está relacionada con 13 sectores estratégicos que son aquellos donde se encuentra la infraestructura estratégica de la nación que ofrece los servicios esenciales que sustentan la sociedad colombiana.

Tabla 9

Sectores y subsectores estratégicos en Colombia

	Sector	Subsector
1	Alimentación y agricultura	Agricultura Acuario Pesquero Acuícola
2	Agua	Acueducto Saneamiento básico Red matriz
3	Comercio, industria, turismo	Comercio Industria Turismo
4	Defensa	Unidad de Gestión General-MDN Ejército Nacional Armada Nacional Fuerza Aérea Colombiana Policía Nacional
5	Educación	Instituciones de educación preescolar, básica, media y superior. Institutos para el fomento de la educación superior Entidades de crédito educativo Entidades de educación para personas con discapacidad auditiva y visual
6	Electricidad	Operación Generación Transmisión Distribución Comercialización
7	Financiero	Intermediarios financieros Portafolios de inversión Aseguradores e intermediaros de seguros y reaseguros. Pensiones, cesantías y fiduciaria Intermediarios de valores
8	Gobierno	Presidencia Políticas públicas Planeación nacional Hacienda Inteligencia Sistemas emergentes Estadísticas

	Sector	Subsector
		Inclusión social y reconciliación
9	Recursos naturales-medio ambiente	Estratégico y político
		Hidrológico, meteorológico y ambiental
		Parques naturales y áreas protegidas
		Licencias y trámites ambientales
		Conservación, protección y administración de los recursos naturales renovables
		Investigación científica en biodiversidad y recursos naturales
10	Recursos minero-energéticos	Entidades adscritas
		Hidrocarburos
		Gas
		Minería
		Distribución
11	Salud y protección social	Salud pública
		Protección social
		Vigilancia y supervisión
12	Tecnologías de la información y comunicaciones	Tecnologías de la información
		Comunicaciones
		Tecnologías de operación
13	Transportes	Terrestre
		Aéreo
		Marítimo y fluvial

Fuente: CCOC (2016).

4.1.1.1 Partes interesadas

Las partes interesadas de una organización son cualquier individuo, grupo u organización que forme parte o se vea afectado por la misma, obteniendo algún beneficio o perjuicio y cada una de ellas, con sus propios intereses (CERTSI, n.d.). El modelo de madurez de ciber-resiliencia organizacional propuesto pretende dar respuesta a las diferentes necesidades de cada una de ellas, tal como se describe en la siguiente tabla.

Tabla 10

Partes interesadas internas de la propuesta de modelo de madurez de ciber-resiliencia organizacional

Parte Interesada	Necesidad	Función del Modelo de Madurez de Ciber-resiliencia
Gobierno Nacional	Conocer el nivel de ciber-resiliencia de las organizaciones que manejan la infraestructura crítica nacional.	Mejora continua ciber-resiliencia - identificación de brechas de implementación de prácticas.
Fuerzas Militares	Conocer el nivel de ciber-resiliencia de las organizaciones que manejan infraestructura crítica, para enfocar sus esfuerzos en la protección de las organizaciones con menor nivel de ciber-resiliencia que puedan ser objetivo militar.	Mejora continua ciber-resiliencia - identificación de brechas de implementación de prácticas.
Órganos de gobierno y control	Conocer el nivel de ciber-resiliencia de las organizaciones que manejan infraestructura crítica, para identificar el estado de riesgo de las organizaciones frente a la pérdida de continuidad del negocio por ataques cibernéticos tipo amenazas persistentes avanzadas.	Mejora de la ciber-resiliencia organizacional – Identificación de controles a implementar para mitigar el riesgo (basados en las prácticas del modelo).
Áreas de operaciones	Conocer el nivel madurez de ciber-resiliencia, para identificar la brecha en la implementación de prácticas y formular plan de tratamiento para mitigar el riesgo.	Mejora de la ciber-resiliencia organizacional - Identificación de controles a implementar para mitigar el riesgo (basados en las prácticas del modelo).
Responsables de riesgos y seguridad digital (seguridad	Disponer de un modelo para medir el nivel de madurez de	Mejora de la ciber-resiliencia organizacional -

Parte Interesada	Necesidad	Función del Modelo de Madurez de Ciber-resiliencia
de la información y ciberseguridad)	ciber-resiliencia de la organización a su cargo.	Identificación de controles a diseñar para mitigar el riesgo (basados en las prácticas del modelo).
Accionistas	Conocer el nivel de madurez de la ciber-resiliencia de la organización.	Información del estado del riesgo de pérdida de continuidad por ataque cibernético tipo amenazas persistentes avanzadas.
Socios/partners	Mejorar la continuidad del negocio a través de la ciber-resiliencia de los socios o *partners*.	Información del estado del riesgo de pérdida de continuidad por ataque cibernético tipo amenazas persistentes avanzadas de los socios o *partners*.

Fuente: elaboración propia.

4.1.2 Niveles de madurez y modelo comparativo

Tabla 11

Niveles de madurez vs. estado de desarrollo de las capacidades de ciber-resiliencia y modelo comparativo

NIVEL DE MADUREZ DE CIBER-RESILIENCIA ORGANIZACIONAL	*Nivel 1. Inicial*	*Nivel 2. Gestionado*	*Nivel 3. Definido*	*Nivel 4. Gestionado Cuantitativamente*	*Nivel 5 En optimización*
Estado de desarrollo de las capacidades de ciber-resiliencia	*En proceso de iniciar desarrollo de capacidades*	*Anticipar- inicial*	*Anticipar-desarrollada Resistir-Inicial Recuperar-Inicial*	*Anticipar-Desarrollada Resistir-Desarrollada Recuperar-Desarrollada Evolucionar-Inicial*	*Anticipar-Desarrollada Resistir-Desarrollada Recuperar-Desarrollada Evolucionar-Desarrollada*
Nivel de preparación para afrontar ataques cibernéticos	*Muy bajo*	*Bajo*	*Medio*	*Alto*	*Muy Alto*
Modelo Comparativo	***Organización "En Riesgo"***		***"Ejecutante competente"***		***"El mejor de la Clase"***

Fuente: elaboración propia.

El modelo diseñado considera 5 niveles de madurez: nivel 1-Inicial, nivel 2-Gestionado, nivel 3-Definido, Nivel 4 Gestionado Cuantitativamente y nivel 5- En optimización. Cada nivel de madurez representa el avance que tiene el desarrollo de las capacidades de ciber-resiliencia y el estado de preparación de la organización para afrontar ataques cibernéticos. En el nivel 1-Inicial, las capacidades de ciber-resiliencia están en proceso de iniciar su desarrollo; en el nivel 2-Gestionado, la capacidad de anticipar se empieza a desarrollar; en el nivel 3-Definido, la capacidad de anticipar está desarrollada y se empiezan a desarrollar las capacidades de resistir y recuperar; en el nivel 4- Gestionado Cuantitativamente, se han desarrollado las capacidades de anticipar, resistir y recuperar, así mismo se empieza desarrollar la capacidad de evolución; en el nivel 5-En optimización, todas las capacidades de ciber-resiliencia han sido desarrolladas.

Cada nivel de madurez está asociado a un modelo comparativo, que le permite a la organización identificar el estado de preparación de la organización para afrontar ataques cibernéticos del tipo amenazas persistentes avanzadas. Las organizaciones que tienen un nivel de madurez 1-Inicial o 2-Gestionado, son organizaciones que según el modelo comparativo se clasifican como organización "En riesgo", esto significa que la preparación para afrontar un ataque cibernético es generalmente muy baja para el nivel 1, y baja para el nivel 2. Las organizaciones que tienen un nivel de madurez 3-definido o 4-gesionado cuantitativamente, son organizaciones que se clasifican como "Ejecutante Competente", esto significa que la preparación para afrontar un ataque cibernético es media para el nivel 3 y alta para el nivel 4. Las organizaciones que tienen un nivel de madurez 5-En optimización, se clasifican como "El mejor de la clase", esto significa que la preparación para afrontar un ataque cibernético es muy alta.

La implementación de las prácticas de cada nivel de madurez es lo que permite a la organización ir pasando de un nivel inferior a un nivel superior, es la forma de reflejar la forma natural en que las capacidades están siendo desarrolladas, pues cada práctica corresponde con una capacidad de ciber-resiliencia. En los niveles inferiores, generalmente hay prácticas básicas que son insumo para ir avanzando en prácticas que requieren un esfuerzo adicional en su implementación, por ejemplo, en el caso del control de acceso y la

gestión de privilegios, en un nivel 1-Inicial, la organización contará con mecanismos de control de acceso y gestión de privilegios sobre los activos cibernéticos, y en un nivel 2-Gestionado, la organización ya asocia este control de acceso y la gestión de privilegios con las funciones o tareas formales que realiza un usuario específico y las refleja en la implementación del mínimo privilegio.

4.1.3 Disciplinas del modelo y principios de diseño de ciber-resiliencia

El modelo de madurez diseñado considera cuatro disciplinas que apoyan la ciber-resiliencia: ciberseguridad, resistencia y supervivencia, evolución y amenazas persistentes avanzadas. Cada disciplina está relacionada con un principio de diseño de ciber-resiliencia, que a su vez está relacionado con las competencias de anticipar, resistir, recuperarse y evolucionar.

- ***Disciplina de Ciberseguridad***: El enfoque de la disciplina de ciberseguridad es la implementación de controles de seguridad para proteger los activos cibernéticos de las amenazas que pueden dejar a la organización expuesta a un ataque cibernético. La disciplina de ciberseguridad se implementa basada en los principios de diseño de ciber-resiliencia de: reducción de la superficie de ataque, dudar de la fiabilidad de todos los recursos técnicos, limitar la confianza por defecto, limitación de la visibilidad, contención y exclusión de comportamientos anómalos, y defensa en profundidad y segmentación de los medios (Bodeau y Graubart, 2017).
- ***Disciplina de Resistencia y Supervivencia***: Esta disciplina orienta a la organización a enfocar sus esfuerzos para que la infraestructura tecnológica que soporta los activos y ciberactivos críticos para la misión organizacional, tenga un nivel de resiliencia que le permita seguir soportando las funciones, aun cuando se esté enfrentando un ataque cibernético. Así mismo, cuando el ataque cibernético afecte la disponibilidad de esta tecnología, contar con estrategias de recuperación y contingencia que permitan el restablecimiento de estas funciones sin afectar la continuidad del negocio. Esta disciplina se implementa basada en los principios de diseño de ciber-resiliencia de: centrarse en los activos críticos y comunes, soportar la agilidad y diseñar para

adaptarse, planificar y gestionar la diversidad, mantener redundancia, y hacer localización versátil de los recursos (Bodeau y Graubart, 2017).

- ***Disciplina de Evolución***: La disciplina de evolución tiene como foco que la organización con base en su entorno se prepare para enfrentar los riesgos cibernéticos a que está expuesta, adaptándose para mitigar los riesgos. Esta disciplina se implementa basada en los principios de diseño de ciber-resiliencia de: aprovechamiento de la información de los indicadores de ciberseguridad, mantener la conciencia situacional, y gestionar los riesgos de forma adaptativa (Bodeau y Graubart, 2017)
- ***Disciplina de Amenazas Persistentes Avanzadas***: La disciplina de amenazas persistentes avanzadas tiene como foco conocer en detalle las técnicas utilizadas por los atacantes, los impactos en la infraestructura de los ataques cibernéticos y la identificación de los mecanismos de defensa contra el adversario. Su implementación se hace basada en los principios de diseño de ciber-resiliencia de: esperar que los adversarios evolucionen, maximizar la transitoriedad; minimizar la persistencia, validación periódica o continua de la integridad, cambiar o interrumpir la superficie de ataque y hacer que la imprevisibilidad y el engaño sean transparentes para el adversario (Bodeau y Graubart, 2017).

Cada principio orienta a la organización en las prácticas que debe implementar para cada disciplina. Cada práctica está a su vez relacionada con el desarrollo de una de las capacidades organizacionales de ciber-resiliencia en un nivel de madurez específico. Las prácticas distribuidas en los niveles de madurez dan cuenta de cómo evolucionan las capacidades de ciber-resiliencia. Cada nivel de madurez cuenta con un descriptor de estado de avance de los principios de diseño de ciber-resiliencia, donde se indican las prácticas a evidenciar en el nivel de madurez que se está evaluando.

Tabla 12

Disciplinas, principios de diseño y prácticas por nivel de madurez

Disciplinas del Modelo	*Principios de diseño de ciber-resiliencia que orientan las prácticas organizacionales .*	PRÁCTICAS QUE IMPLEMENTA LA ORGANIZACIÓN EN CADA NIVEL DE MADUREZ				
Ciberseguridad	*Reducción de la superficie de ataque. *Dudar de la Fiabilidad de todos los recursos técnicos. *Limitar la confianza por defecto. *Limitación de la visibilidad. *Contención y exclusión de comportamientos anómalos. *Defensa en profundidad y segmentación de medios	*Descriptor del avance de los principios de diseño / Prácticas ciberseguridad nivel 1 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas ciberseguridad nivel 2 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas ciberseguridad nivel 3/ capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas ciberseguridad nivel 4 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas ciberseguridad nivel 5 / capacidad que desarrolla la práctica*
Resistencia y supervivencia	*Centrarse en los activos críticos y comunes. *Soportar la agilidad y diseñar para adaptarse. *Planificar y gestionar la diversidad. *Mantener la redundancia. *Hacer la localización de los recursos versátil.	*Descriptor del avance de los principios de diseño / Prácticas Resistencia y supervivencia nivel 1 / capacidad que*	*Descriptor del avance de los principios de diseño / Prácticas Resistencia y supervivencia nivel 2 /*	*Descriptor del avance de los principios de diseño / Prácticas Resistencia y supervivencia nivel 3 /*	*Descriptor del avance de los principios de diseño / Prácticas Resistencia y supervivencia nivel 4 /*	*Descriptor del avance de los principios de diseño / Prácticas Resistencia y supervivencia nivel 5 /*
Evolución	*aprovechamiento de la información de los indicadores de ciberseguridad. *mantener la conciencia situacional. *gestionar los riesgos de forma adaptativa	*Descriptor del avance de los principios de diseño / Prácticas Evolución nivel 1 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas Evolución nivel 2 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas Evolución nivel 3 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas Evolución nivel 4 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño / Prácticas Evolución nivel 5 / capacidad que desarrolla la práctica*
Amenazas persistentes avanzadas	*Espere que los adversarios evolucionen *maximizar la transitoriedad; minimizar la persistencia *validación periódica o continua de la integridad *cambiar o interrumpir la superficie de ataque *hacer que la imprevisibilidad y el engaño sean transparentes para el adversario	*Descriptor del avance de los principios de diseño de ciber-resiliencia / Prácticas amenazas persistentes avanzadas nivel 1 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño de ciber-resiliencia / Prácticas amenazas persistentes avanzadas nivel 2 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño de ciber-resiliencia / Prácticas amenazas persistentes avanzadas nivel 3 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño de ciber-resiliencia / Prácticas amenazas persistentes avanzadas nivel 4 / capacidad que desarrolla la práctica*	*Descriptor del avance de los principios de diseño de ciber-resiliencia / Prácticas amenazas persistentes avanzadas nivel 5 / capacidad que desarrolla la práctica*

Fuente: elaboración propia.

4.2 Descripción de los niveles de madurez de ciber-resiliencia

4.2.1 Nivel 1-Inicial

En este nivel, las organizaciones están en proceso de iniciar el desarrollo de sus capacidades de ciber-resiliencia. Se evidencian algunas prácticas que permiten concluir que la organización está tomando conciencia de la necesidad de desarrollar su capacidad de ciber-resiliencia. El estado de preparación para afrontar un ataque cibernético es generalmente muy bajo. Las organizaciones en este nivel son organizaciones "En riesgo".

Tabla 13

Prácticas para evidenciar por disciplina y descriptor de estado de avance de los principios de ciber-resiliencia para el nivel 1- Inicial

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIO DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Resistencia y Supervivencia	**Centrarse en los activos críticos y comunes**: *Identificación de las funciones críticas del negocio y los indicadores de continuidad. **Soportar la agilidad y diseñar para adaptarse:** *Ningún avance. **Planificar y gestionar la diversidad**: *Ningún avance **Mantener redundancias**: *Ningún avance. **Hacer localización de los recursos versátil:** *Ningún avance.	La organización ha realizado un análisis de impacto del negocio BIA y con base en este ha identificado las funciones críticas para el logro de la misión, los tiempos de inactividad máximos tolerables, los tiempos objetivos de recuperación y los puntos objetivos de recuperación de la tecnología que soporta las funciones críticas.	Anticipar
Ciberseguridad	**Reducción de la superficie de ataque**: *Gestión de privilegios y control de acceso *Escaneo periódico de los puertos de red.	Se cuenta con mecanismos de control de acceso y gestión de privilegios sobre los activos cibernéticos.	Anticipar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIO DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
	Dudar de la fiabilidad de todos los recursos técnicos: *Ningún avance **Limitar la confianza por defecto**: *Ningún avance **Limitación de la visibilidad**: *Ningún avance. **Contención y exclusión de comportamientos anómalos:** *Ningún avance. **Defensa en profundidad y segmentación de los medios**: *Ningún avance.	Se realiza escaneo periódico de los puertos de red y se corrigen las inconsistencias.	Anticipar
Amenazas persistentes avanzadas	**Espere que los adversarios evolucionen**: *Equipo de respuesta a incidentes. **Maximizar la transitoriedad; Minimizar la persistencia:** *Ningún avance **Validación periódica o continua de la integridad**: *Ningún avance **Cambiar o interrumpir la superficie de ataque** *Ningún avance. **Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario:** *Ningún avance.	Se cuenta con un equipo de respuesta a incidentes formal en la organización.	Anticipar
Evolucionar	**Aprovechamiento de la información de los indicadores de ciberseguridad**: *Indicadores de ciberseguridad definidos. **Mantener la conciencia situacional:** *Ningún avance **Gestionar los riesgos de los recursos de forma adaptativa**: *Ningún avance	Se han definido indicadores para realizar seguimiento a los controles de ciberseguridad implementados en la organización.	Anticipar

Fuente: elaboración propia.

4.2.2 Nivel 2-Gestionado

En este nivel, las organizaciones han iniciado a potenciar el desarrollo de la capacidad de anticipar. La organización conoce cuáles son los activos y ciberactivos críticos para la misión organizacional; se comienzan a definir estrategias de respaldo y recuperación; el control de acceso está alineado al principio del mínimo privilegio; se empieza a conocer al adversario y las técnicas comunes de ataque; así mismo, se inicia el entrenamiento de los equipos de respuesta a incidentes para responder a los ataques conocidos. El estado de preparación para afrontar un ataque cibernético es generalmente bajo. Las organizaciones en este nivel son organizaciones que aún pueden considerarse "En riesgo".

Tabla 14

Prácticas a evidenciar por disciplina y descriptor de estado de avance de los principios de ciber-resiliencia para el nivel 2-Gestionado

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Resistencia y supervivencia	**Centrarse en los activos críticos y comunes**: *Identificación de los activos críticos para la misión organizacional. *Se identifican los activos cibernéticos críticos comunes y comunes. *Estrategias de respaldo y recuperación. **Soportar la agilidad y diseñar para adaptarse**: *Ningún avance. **Planificar y gestionar la diversidad**: *Ningún avance **Mantener redundancias**: *Ningún avance. **Hacer localización de los recursos versátil**: *Ningún avance.	La organización identificó los activos cibernéticos más críticos para el logro de la misión a través de análisis como el de "joyas de la corona" (Crown Jewels Analysis-CJA).	Anticipar
		Se identifican los activos cibernéticos comunes a múltiples misiones o funciones de negocios que son objetivos potenciales de alto valor para los ciber atacantes, ya sea porque esos activos son críticos o porque su compromiso aumenta las opciones de movimiento lateral y persistencia de los atacantes.	Anticipar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
		La organización cuenta con estrategias de respaldo y recuperación de activos cibernéticos iniciales, que no dan cubrimiento a todos los activos cibernéticos identificados como críticos para el logro de la misión organizacional.	Recuperar
Ciberseguridad	**Reducción de la superficie de ataque**: *Control de acceso basado en el "mínimo privilegio". *Monitoreo de transacciones u operaciones de los usuarios finales. *Control y monitoreo de los *end-point* (puntos finales). *Se limitan los puntos de control de accesos remotos. *Segmentación de red. **Dudar de la fiabilidad de los recursos técnicos**: *Protección contra ataques de *phishing*. **Limitar la confianza por defecto**: *Evidencia de compromiso. **Limitación de la visibilidad**: *Ningún avance. **Contención y exclusión de comportamientos anómalos**: *Ningún avance. **Defensa en profundidad y segmentación de los medios**: *Ningún avance.	Se aplica el principio del mínimo privilegio (se diseña para restringir los privilegios asignados a los usuarios y las entidades cibernéticas, y para establecer requisitos de privilegios sobre los recursos en función de la necesidad de uso y evento por evento).	Anticipar
		Se monitorean las transacciones u operaciones realizadas por los usuarios finales para identificar actividades anormales.	Anticipar
		Se realiza control y monitoreo de los *end-point* (puntos finales)	Anticipar
		Se limitan los puntos de control de acceso para accesos remotos.	Anticipar
		Se realiza segmentación de la red como una medida para controlar el tráfico hacia los activos cibernéticos críticos para la organización.	Resistir
		Sólo se importa software confiable al que se le ha verificado su legitimidad.	Anticipar
		Se protegen los entornos de gestión u operaciones contra ataques de *phishing*.	Anticipar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
		Prácticas de validación de datos y el comportamiento para detectar actividades maliciosas (evidencia de compromiso).	Anticipar
Amenazas persistentes avanzadas	**Espere que los adversarios evolucionen**: *Entrenamiento para responder a ataques cibernéticos que utilizan técnicas conocidas *Conocimiento de las técnicas y tácticas comunes usadas por el adversario. **Maximizar la transitoriedad; Minimizar la persistencia**: *Ningún avance **Validación periódica o continua de la integridad:** *Ningún avance **Cambiar o interrumpir la superficie de ataque** *Ningún avance. **Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario:** *Ningún avance.	El personal del equipo de respuesta a incidentes es capacitado y entrenado para responder a ataques cibernéticos realizados con técnicas conocidas.	Resistir
		Se conocen las tácticas y técnicas comunes usadas por el adversario.	Resistir
Evolución	**Aprovechamiento de la información de los indicadores de ciberseguridad:** *Medición y seguimiento por parte de la alta dirección de los indicadores de ciberseguridad **Mantener la conciencia situacional:** *Visualización de eventos realizando análisis básicos. Fase de percepción. **Gestionar los riesgos de los recursos de forma adaptativa:** *Gestión de riesgos para amenazas conocidas.	Se realiza medición, seguimiento y monitoreo a los indicadores de ciberseguridad, por parte de la alta dirección de la organización.	Anticipar
		Se realiza visualización de los eventos más como una monitorización, en la que se observa un fenómeno en curso, realizando análisis muy básicos con herramientas que no permiten analítica. La conciencia está en una fase de percepción.	Anticipar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
		Se analizan y gestionan riesgos para amenazas que pueden entenderse como conocidas. La amenaza se ha conversado o comunicado dentro de la organización y se conoce de su existencia (malware, fuga de información, *botnets*).	Anticipar

Fuente: elaboración propia.

4.2.3 Nivel 3-Definido

En este nivel, las organizaciones tienen desarrollada la capacidad de anticipar y han iniciado el desarrollo de las capacidades de resistir y recuperar. En este nivel de madurez, la organización comprende las amenazas y los riesgos asociados a los activos cibernéticos comunes y críticos; cuenta con plan de recuperación de desastres con estrategias que cubren los activos identificados como críticos comunes; se han seleccionado medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos críticos para la misión organizacional; se cuenta con redundancia para algunos activos cibernéticos críticos; se realizan análisis de modos de fallas y efecto; se aplica el principio de menor funcionalidad; se monitorean transacciones de usuarios privilegiados; se gestiona la vulnerabilidad técnica y se monitorea la infraestructura; se separan componentes; se desarrollan capacidades de ciberinteligencia; se realizan juegos de guerra para entrenar al equipo de respuesta a incidentes; se entiende el ciclo de vida de las amenazas persistentes avanzadas y se cuenta con un centro de operaciones de ciberseguridad. El estado de preparación para afrontar un ataque cibernético es generalmente medio. Las organizaciones en este nivel de madurez son organizaciones que se consideran "Ejecutante Competente".

Tabla 15

Prácticas a evidenciar por disciplina y descriptor de estado de avance de los principios de ciber-resiliencia para el nivel 3-Definido

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Resistencia y Supervivencia	**Centrarse en los activos críticos y comunes**: *Se comprenden las amenazas y riesgos de los activos cibernéticos críticos y comunes. *Plan de recuperación de desastres para activos críticos comunes. *Medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos críticos seleccionadas. *Análisis de modos de falla y efectos **Soportar la agilidad y diseñar para adaptarse**: *Ningún avance. **Planificar y gestionar la diversidad**: *Ningún avance **Mantener redundancias:** *Redundancia para algunos activos cibernéticos. **Hacer localización de los recursos versátil:** *Ningún avance.	Se comprenden las amenazas y los riesgos asociados a los activos cibernéticos críticos comunes y críticos, a través de herramientas como la Evaluación de Susceptibilidad de Amenazas Cibernéticas (TSA).	Resistir
		Se cuenta con un plan de recuperación de desastres con estrategias que cubren los activos cibernéticos identificados como críticos comunes.	Recuperar
		Se han seleccionado medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos críticos para la misión organizacional. Se están usando herramientas como el análisis de Remediación de Riesgos Cibernéticos (RRA) , que identifica las medidas de mitigación recomendadas.	Resistir
		Se inicia Implementación de estrategias de redundancia que no cubren el total de los activos cibernéticos críticos para la misión organizacional.	Resistir
		Se realizan análisis de modos de fallas y efectos críticos a sistemas ciber-físicos utilizando herramientas como análisis FMECA.	Anticipar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Ciberseguridad	**Reducir la superficie de ataque**: *Implementación del principio de menor funcionalidad. *Monitoreo de transacciones de administradores y operadores de los activos cibernéticos. *Gestión de la vulnerabilidad técnica. *Monitoreo de infraestructura para detectar errores de configuración, software desactualizado, seguridad de los activos cibernéticos. ***Dudar de la fiabilidad de los recursos técnicos**: *Separación/segmentación de componentes. **Limitar la confianza por defecto**: *Capacidades de ciberinteligencia. *Identificación de eslabones débiles para la ciberseguridad. **Limitación de la visibilidad**: *Ningún avance. **Contención y exclusión de comportamientos anómalos**: *Mecanismos para deshabilitar elementos con comportamientos sospechosos. **Defensa en profundidad y segmentación de los medios**: *Ningún avance.	Se aplica el principio de menor funcionalidad (es decir, restringiendo puertos, protocolos, funciones y servicios).	Anticipar
		Se monitorean a las transacciones u operaciones realizadas por usuarios privilegiados (administrador y operador de los activos cibernéticos).	Anticipar
		Se gestiona la vulnerabilidad técnica de los activos cibernéticos.	Anticipar
		Se monitorea periódicamente la infraestructura para detectar configuraciones erróneas y software desactualizado, probar el sistema de seguridad y mantener la actividad de los usuarios bajo control.	Anticipar
		Se implementan prácticas de separación/segmentación de componentes (lógica o físicamente) basados en la criticidad y la confiabilidad, para limitar la propagación del daño.	Resistir
		Se desarrollan capacidades de ciberinteligencia para analizar y prevenir, identificar, localizar y atribuir ataques o amenazas a través del ciberespacio.	Resistir
		Se identifican los componentes del sistema que pueden ser eslabones débiles para la ciberseguridad y se aumenta la seguridad en estos puntos (componentes, personas, procedimientos).	Anticipar
		Se cuenta con mecanismos para deshabilitar cualquier elemento del sistema que no sea de misión crítica que	Resistir

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
		exhiba un comportamiento sospechoso.	
Amenazas persistentes avanzadas	**Espere que los adversarios evolucionen**: *Juegos de guerra *Entendimiento del ciclo de vida de las amenazas persistentes avanzadas. **Maximizar la transitoriedad; Minimizar la persistencia**: *Ningún avance **Validación periódica o continua de la integridad**: *Ningún avance **Cambiar o interrumpir la superficie de ataque** *Ningún avance. **Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario**: *Ningún avance.	Se realizan prácticas de juegos de guerra para preparar a equipos de respuesta para enfrentar los ataques cibernéticos.	Resistir
		Hay un entendimiento del ciclo de vida de las amenazas persistentes avanzadas (*ciber kill chain*),	Resistir
Evolución	**Aprovechamiento de la información de los indicadores de ciberseguridad**: *SOC implementado **Mantener la conciencia situacional**: *Inspección de eventos y búsqueda de detalles para formular hipótesis sobre los eventos. Conciencia en una fase de comprensión inicial.	Se cuenta con un centro de operaciones de ciberseguridad (SOC) encargado de realizar seguimiento y analizar la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.	Resistir

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
	Gestionar los riesgos de los recursos de forma adaptativa: *Se gestionan riesgos focales.	Se realiza Inspección de los eventos, se buscan detalles específicos, se solicitan aclaraciones y encuentra datos que le permiten comprobar hipótesis sobre los eventos. La conciencia está en una fase de comprensión inicial.	Anticipar
		Se analizan y gestionan riesgos para amenazas que pueden entenderse como focales. La amenaza ya se ha visto o materializado en la industria particular a la que pertenece la empresa (ataques a sistemas de control industrial, *phishing* dirigido, vulnerabilidades en IoT, ataques coordinados).	Anticipar

Fuente: elaboración propia.

4.2.4 Nivel 4-Gestionado Cuantitativamente

En este nivel, las organizaciones tienen desarrolladas las capacidades de anticipar, resistir y recuperar; así mismo, se ha iniciado el desarrollo de la capacidad de evolucionar. La organización empieza a evolucionar en todas las prácticas ya implementadas, utilizando herramientas que le permitan mejorar aún más el estado de preparación para afrontar los ataques cibernéticos. Los análisis de modos de fallas y efectos son utilizados para planeación del mantenimiento, diseño y rediseño de sistemas ciber-físicos; todos los activos organizacionales tanto críticos como comunes cuentan con estrategias de recuperación; se entiende con detalle la afectación que un ataque cibernético tiene sobre infraestructura tecnológica organizacional; se identifican las condiciones de adaptabilidad que debe tener la infraestructura para resistir los ataques; se utilizan formas alternativas de proporcionar la funcionalidad crítica requerida; se analizan y definen estrategias de diversidad de plataforma y ubicación versátil de los activos cibernéticos críticos para la misión organizacional; se

reduce la complejidad de la red; se realiza integridad comprobada; se implementan mecanismos de falla en modo seguro; se implementa defensa en profundidad. El equipo de respuesta a incidentes realiza modelado de ataques y métodos de defensa; se implementan técnicas de engaño al adversario; se plantean estrategias para prevenir, detectar y combatir las amenazas persistentes avanzadas; hay una exploración profunda de los eventos de ciberseguridad y se gestionan los riesgos para amenazas latentes. El estado de preparación para afrontar un ataque cibernético es alto. Las organizaciones en este nivel de madurez son organizaciones que se consideran "Ejecutante Competente".

Tabla 16

Prácticas a evidenciar por disciplina y descriptor de estado de avance de los principios de ciber-resiliencia para el nivel 4-Gestionado Cuantitativamente

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Resistencia y Supervivencia	**Centrarse en los activos críticos y comunes**: *Análisis de fallas y efectos utilizados para mantenimiento, diseño y rediseño de sistemas ciber-físicos. *Activos cibernéticos críticos y críticos comunes con estrategias de recuperación debidamente probadas. *Activos cibernéticos críticos comunes y críticos con medidas de mitigación para prevenir y combatir ataques cibernéticos implementadas. *Análisis de impacto de ciberataques (CMIA) **Soportar la agilidad y diseñar para adaptarse**: *Identificación de las condiciones de adaptabilidad	Los análisis de modos de fallas y efectos críticos (FMECA) son utilizados como insumos para planeación del mantenimiento, diseño y rediseño de sistemas ciber-físicos.	Evolucionar
		Todos los activos cibernéticos que soportan las funciones críticas organizacionales cuentan con estrategias de recuperación formales, a las cuales se les realizan pruebas periódicamente.	Recuperar
		Se implementan las medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos catalogados como críticos comunes y críticos.	Resistir

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
	que deben soportar los activos cibernéticos en condiciones de falla. *Formas alternativas de proporcionar la funcionalidad crítica. **Planificar y gestionar la diversidad**: *Definición de estrategias de diversidad de plataforma. **Mantener redundancias**: *Redundancia para ciberactivos críticos comunes. **Hacer localización de los recursos versátil** *Se definen estrategias de ubicación versátil de activos cibernéticos críticos.	Se realiza análisis de impacto de ciberataques (CMIA) para identificar las consecuencias de los ataques cibernéticos en la misión organizacional.	Evolucionar
		Se identificaron las condiciones de adaptabilidad que deben soportar los activos cibernéticos para que, en condiciones de falla, se puedan tener más opciones de operación.	Evolucionar
		Se utilizan de formas alternativas de proporcionar la funcionalidad crítica requerida, de modo que, si un componente es comprometido, se pueden utilizar uno o más componentes alternativos que proporcionan la misma funcionalidad.	Resistir
		Se analizan y definen estrategias de utilización de técnicas de diversidad de plataforma para eliminar puntos específicos de ataque que comprometan los activos críticos organizacionales (diversidad arquitectónica, diversidad de diseño, diversidad sintética, diversidad de información, diversidad de comando y control, diversidad de las rutas de comunicación y, de la cadena de suministro).	Evolucionar
		Implementación de redundancia como estrategia de tolerancia a fallos para los activos críticos comunes.	Recuperar
		Se analizan y definen estrategias para contar con mecanismos de ubicación versátil de los activos cibernéticos críticos.	Evolucionar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Ciberseguridad	**Reducción de la superficie de ataque**: *Reducción de la complejidad de la red. *Análisis de red, protocolos, servicios del sistema operativo y tráfico pasado a través de la red. **Dudar de la fiabilidad de los recursos técnicos**: *Integridad comprobada. *Falla en modo seguro. **Limitar la confianza por defecto**: *Certificación de los atributos de confiabilidad de un elemento del sistema. **Limitación de la visibilidad**: *Restricción de la visibilidad externa de los comportamientos del sistema. **Contención y exclusión de comportamientos anómalos**: *Mecanismos para restricción o contención de actividades sospechosas a priori o dinámicamente. **Defensa en profundidad y segmentación de los medios**: *Defensa en profundidad.	Se han implementado acciones para reducir la complejidad de la red (una estructura más sencilla, automatización, optimización del rendimiento y un entorno más seguro).	Evolucionar
		Se realizan análisis de red, los protocolos y los servicios del sistema operativo, así como el tráfico actual y pasado a través de la red para detectar factores que podrían exponer aún más la superficie de ataque.	Evolucionar
		Se implementan prácticas de integridad comprobada (proporcionar mecanismos para determinar si los servicios críticos, los almacenes de información, los flujos de información y los componentes se han dañado).	Evolucionar
		Se implementan mecanismos de falla en modo seguro (control de errores).	Resistir
		Se tiene la capacidad de certificación o garantía de los atributos de confiabilidad de un elemento del sistema.	Evolucionar
		Se restringe la visibilidad externa de los comportamientos del sistema.	Evolucionar
		Se cuenta con mecanismos para restricción o contención de actividades sospechosas, a priori o dinámicamente.	Resistir
		Se implementó defensa en profundidad: "integrando capacidades de personas, tecnología y operaciones para establecer".	Evolucionar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Amenazas persistentes avanzadas	**Espere que los adversarios evolucionen**: *Utilización de juegos de ciberseguridad para modelado de ataques y métodos de defensa. *Análisis de estrategias para prevenir, detectar y combatir APTs **Maximizar la transitoriedad; Minimizar la persistencia**: *Identificación de riesgos de persistencia de datos e información. **Validación periódica o continua de la integridad**: *Servicios para validación de integridad. **Cambiar o interrumpir la superficie de ataque:** *Defensa del objetivo en movimiento (MTD). **Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario**: *Técnicas de engaño al adversario.	Utilización de juegos de ciberseguridad (CSG) para modelado de ataques y métodos de defensa.	Resistir
		Se implementan técnicas de engaño al adversario (confundirlo, engañarlo y despistarlo).	Evolucionar
		Se analizan estrategias para prevenir, detectar y combatir amenazas persistentes avanzadas.	Resistir
		Se identifican riesgos de persistencia de datos e información para los ciberactivos críticos para la misión.	Evolucionar
		Se emplean servicios para validar la integridad de configuraciones, módulos de software, y datos críticos.	Evolucionar
		Se han implementado mecanismos de defensa del objetivo en movimiento (MTD, Moving Target Defense)	Evolucionar
Evolución	**Aprovechamiento de la información de los indicadores de ciberseguridad**: *Indicadores y alertas de ciberseguridad retroalimentan la organización. **Mantener la conciencia**	Los indicadores y alertas entregadas por el SOC, retroalimentan a la organización para la toma de decisiones e implementación de acciones tendientes a prevenir los ataques cibernéticos.	Evolucionar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
	situacional: *Fase de comprensión avanzada de los eventos de ciberseguridad. **Gestionar los riesgos de los recursos de forma adaptativa**: *Gestión de riesgos para amenazas latentes.	Se realiza exploración de los eventos, donde se realiza un estudio concienzudo y libre de los datos, se investiga sin tener pistas previas, se combinan los datos de forma novedosa y se experimenta interactivamente con las vistas de los datos, encontrando regiones de interés para su análisis y se generan nuevas hipótesis. La conciencia está en una fase de comprensión avanzada.	Evolucionar
		Se analizan y gestionan riesgos para amenazas que pueden entenderse como Latentes. Se ha enterado de que tal amenaza existe y que no sabe si la organización tiene alguna estrategia de mitigación (ciberterrorismo, ataques de día cero, *ramsonware*).	Evolucionar

Fuente: elaboración propia.

4.2.5 Nivel 5-En Optimización

En este nivel, las organizaciones tienen desarrolladas todas las capacidades de ciber-resiliencia organizacional. La organización implementa estrategias de respuesta adaptativa en condiciones de fallo para los activos cibernéticos críticos. Para la misión se implementan estrategias de diversidad de plataforma y de los procedimientos operativos críticos soportados en tecnología, para ser utilizados durante operación o en momentos de falla; mecanismos para ubicación versátil de los recursos para evitar puntos únicos de falla; se diseña para tolerar el compromiso de recursos; implementación del principio Zero Trust; mecanismos de partición estática y dinámica de elementos de los activos cibernéticos; estrategias de no persistencia; técnicas de imprevisibilidad; correlación avanzada y profunda de eventos; predicción con relación a los eventos y se analizan y gestionan riesgos para amenazas que pueden entenderse como emergentes. El estado de preparación para afrontar

un ataque cibernético es muy alto. Las organizaciones en este nivel de madurez son organizaciones que se consideran "El mejor de la clase".

Tabla 17

Prácticas a evidenciar por disciplina y descriptor de estado de avance de los principios de ciber-resiliencia para el nivel 5-En Optimización

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
Resistencia y supervivencia	**Centrarse en los activos críticos y comunes**: *Activos cibernéticos comunes con estrategias de recuperación. *Activos cibernéticos comunes con medidas de mitigación para prevenir o combatir ataques cibernéticos implementadas. **Soportar la agilidad y diseñar para la adaptarse**: *Activos cibernéticos críticos con estrategias de respuesta adaptativa en condiciones de fallo.. **Planificar y gestionar la diversidad**: *Se implementan estrategias de diversidad de plataforma y procedimientos operativos críticos. **Mantener redundancias**: *Redundancia como capacidad activa utilizada en la operación y en momentos de falla. **Hacer localización de los recursos versátil:** Implementación de mecanismos de ubicación versátil para los activos cibernéticos críticos para la misión.	Activos cibernéticos comunes con estrategias de recuperación probadas.	Recuperar
		Se implementan medidas de mitigación para prevenir o combatir los ataques cibernéticos que incluyen los activos cibernéticos catalogados como comunes.	Resistir
		Se implementan estrategias de respuesta adaptativa en condiciones de fallo para los activos cibernéticos críticos para la misión (respuesta adecuada y dinámica a situaciones específicas, utilización de contingencias operativas ágiles y alternativas para mantener capacidades operativas mínimas, limitando las consecuencias y evitando la desestabilización, tomando medidas preventivas cuando sea apropiado. Modo a prueba de fallos).	Evolucionar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
		Se implementan estrategias de diversidad de plataforma y de los procedimientos operativos críticos soportados en tecnología, para ser utilizados durante la operación o en momentos de falla.	Evolucionar
		Implementación de redundancia como capacidad activa para ser utilizada durante la operación o en momentos de falla.	Evolucionar
		Se implementan mecanismos para lograr ubicación versátil de los recursos para evitar puntos únicos de falla en sistemas que requieren alta disponibilidad (virtualización, replicación, distribución de funcionalidad o datos almacenados, movilidad física y reubicación funcional).	Evolucionar
Ciberseguridad	**Reducir la superficie de ataque**: *Practicas para reducir la superficie de ataque en constante optimización. **Dudar de la fiabilidad de los recursos técnicos**: *Diseños para tolerar compromiso de recursos. **Limitar la confianza por defecto**: *Arquitectura Zero trust. **Limitación de la visibilidad:** *Practicas para controlar la visibilidad y el uso de los activos	Se diseña para tolerar el compromiso de recursos.	Evolucionar
		Se cuenta con mecanismos de aislamiento estático y dinámico de componentes.	Evolucionar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
	cibernéticos en constante optimización. **Contención y exclusión de comportamientos anómalos:** *Mecanismos para aislamiento estático y dinámico de componentes. **Defensa en profundidad y segmentación de los medios**: *Partición estática y dinámica de elementos de los activos cibernéticos.	La arquitectura que soporta la infraestructura tecnológica está basada en el principio Zero Trust.	Evolucionar
		Se cuenta con mecanismos para la partición estática y dinámica de elementos de los activos cibernéticos.	Evolucionar
Amenazas persistentes avanzadas	**Espere que los adversarios evolucionen**: *Arquitectura organizacional implementa estrategias para prevenir, detectar y responder a las APTs. **Maximizar la transitoriedad; Minimizar la persistencia:** *Implementación de estrategias de no persistencia. **Validación periódica o continua de la integridad:** *Prácticas de validación de la integridad en constante optimización. **Cambiar o interrumpir la superficie de ataque:** *Prácticas de cambiar o interrumpir la superficie de ataque en constante optimización. **Hacer que la imprevisibilidad y el engaño sean transparentes para el adversario:** *Técnicas de imprevisibilidad.	Se integran a la arquitectura organizacional estrategias para prevenir, detectar y responder a las amenazas persistentes avanzadas.	Evolucionar
		Se implementan estrategias de no persistencia para los ciberactivos críticos (se retiene información, servicios y conectividad por un tiempo limitado, reduciendo así la exposición a corrupción, modificación o usurpación).	Evolucionar
		Se utilizan técnicas de imprevisibilidad destinadas a aumentar la incertidumbre de los adversarios, acerca de estructura y comportamiento del sistema.	Evolucionar
Evolución	**Aprovechamiento de la información de los indicadores de ciberseguridad**: *Correlación avanzada y profunda de eventos con interface a logs de activos cibernéticos críticos. **Mantener la conciencia situacional**: *Predicción con relación a los	Se cuenta con correlación avanzada y profunda de eventos, con interface para obtener logs de los activos cibernéticos críticos (ERP, CRM, etc.) con herramientas como SIEM.	Evolucionar

DISCIPLINA	DESCRIPTOR DEL ESTADO DE AVANCE DE LOS PRINCIPIOS DE DISEÑO DE CIBER-RESILIENCIA	PRÁCTICAS PARA EVIDENCIAR	CAPACIDAD
	eventos intentando encontrar el estado futuro más probable. Conciencia en fase de predicción. **Gestionar los riesgos de los recursos de forma adaptativa:** *Riesgos gestionados para amenazas emergentes.	Se realiza predicción con relación a los eventos, en la que se intenta encontrar el estado futuro más probable suponiendo que la progresión actual continuará si no se interviene, o determinamos un estado futuro particular basado en planes de acción potenciales. La conciencia está en una fase de predicción.	Evolucionar
		Se analizan y gestionan riesgos para amenazas que pueden entenderse como emergentes. Nunca había escuchado de tal amenaza (rookits en PLCs, malware en sistemas de control industrial, computación en la niebla).	Evolucionar

Fuente: elaboración propia.

4.3 Herramienta para evaluar nivel de madurez de ciber-resiliencia organizacional

Para evaluar el nivel de madurez de ciber-resiliencia organizacional, se diseñó una herramienta en Excel con la siguiente estructura.

Tabla 18

Descripción de la estructura de la plantilla de evaluación del nivel de madurez

Hoja	Contenido
Introducción	• Información del autor. • Definición de ciber-resiliencia. • Mapa mental del modelo de madurez. • Guía de uso.

Hoja	Contenido
Resultado consolidado	• Gráfico del nivel de madurez por cada disciplina que apoya la ciber-resiliencia. • Cuadro resumen del resultado de la evaluación: disciplina, nivel de madurez, descripción del nivel, estado de desarrollo de las capacidades de ciber-resiliencia organizacional, modelo comparativo y nivel de preparación para afrontar ataques cibernéticos tipo APTs (amenazas persistentes avanzadas).
Resistencia y supervivencia	• Descripción de la disciplina de resistencia y supervivencia. • Prácticas por capacidad a evidenciar en cada nivel de madurez para la disciplina y descriptor del estado de avance de los principios de: centrarse en los activos críticos y comunes, soportar la agilidad y diseñar para adaptarse, planificar y gestionar la diversidad, mantener redundancias y hacer la localización de los recursos versátil. • Estado de implementación de la práctica (¿realiza la práctica?). • Nivel de madurez evidenciado como resultado de la evaluación.
Ciberseguridad	• Descripción de la disciplina de ciberseguridad. • Prácticas por capacidad a evidenciar en cada nivel de madurez para la disciplina y descriptor del estado de avance de los principios de: reducir la superficie de ataque, dudar de la fiabilidad de los recursos, limitar la confianza por defecto, limitación de la visibilidad, contención y exclusión de comportamientos anómalos, defensa en profundidad y segmentación de medios. • Estado de implementación de la práctica (¿realiza la práctica?). Nivel de madurez evidenciado como resultado de la evaluación.
Amenazas persistentes avanzadas	• Descripción de la disciplina de amenazas persistentes avanzadas. • Prácticas por capacidad a evidenciar en cada nivel de madurez para la disciplina y descriptor del estado de avance de los principios de: espere que los adversarios evolucionen, maximizar la transitoriedad, minimizar la persistencia, validación periódica o continua de la integridad, cambiar o interrumpir la superficie de ataque, hacer que la imprevisibilidad y el engaño sean transparentes para el adversario.

Hoja	Contenido
	• Estado de implementación de la práctica (¿realiza la práctica?). Nivel de madurez evidenciado como resultado de la evaluación.
Evolución	• Descripción de la disciplina de evolución. • Prácticas por capacidad a evidenciar en cada nivel de madurez para la disciplina y descriptor del estado de avance de los principios de: aprovechamiento de la información de los indicadores de ciberseguridad, mantener la conciencia situacional, gestionar los riesgos de los recursos de forma adaptativa. • Estado de implementación de la práctica (¿realiza la práctica?). Nivel de madurez evidenciado como resultado de la evaluación.
Acerca del modelo	• Gráfico que describe en detalle la estructura del modelo de madurez de ciber-resiliencia organizacional. • Descripción de las capacidades de ciber-resiliencia organizacional. • Descripción de las disciplinas que apoyan la ciber-resiliencia organizacional. • Descripción de los principios de diseño de ciber-resiliencia.
Recursos de consulta	• Bibliografía que da contexto sobre las prácticas identificadas para cada principio de diseño de ciber-resiliencia con su respectiva URL.

Fuente: elaboración propia.

4.3.1 Paso a paso para realizar la evaluación

- Seleccionar personal que diligenciará la herramienta. Este personal debe ser conocedor de la organización y con experticia en el tema de ciberseguridad.
- Identifique el nivel de madurez que la organización se plantea como meta.
- La evaluación se diligencia en las hojas que tienen el nombre de las disciplinas que apoyan la ciber-resiliencia. El diligenciamiento se puede hacer en el orden que desee.

- En cada nivel de madurez, lea la práctica a evidenciar y responda a la pregunta: ¿REALIZA LA PRÁCTICA? Con un SI, si la organización ha implementado la práctica

y con un NO, si no la ha implementado. Diligencie el total de las prácticas para todas las disciplinas.

NIVEL	ESTADO DE DESARROLLO DE LAS CAPACIDADES DE CIBER-RESILIENCIA	PRINCIPIOS DE CIBER-RESILIENCIA - DESCRIPTOR DEL ESTADO DE AVANCE DELPRINCIPIO	PRÁCTICAS A EVIDENCIAR	CAPACIDAD	REALIZA LA PRÁCTICA?	OBSERVACIONES
Nivel 1. Inicial	En proceso de iniciar desarrollo de capacidades	**Centrarse en los activos críticos y comunes**: *Identificación de la funciones críticas del negocio y los indicadores de continuidad. **Soportar la agilidad y diseñar para adaptarse:** *Ningún avance. **Planificar y gestionar la diversidad**: *Ningún avance **Mantener redundancias**: *Ningún avance. **Hacer localización de los recursos versátil:** *Ningún avance.	La organización ha realizado un análisis de impacto del negocio BIA y con base en este ha identificado las funciones críticas para el logro de la misión, los Tiempos de inactividad máximo tolerables,los tiempos objetivos de recuperación y los puntos objetivos de recuperación de la tecnología que soporta las funciones críticas.	Anticipar		
		Centrarse en los activos críticos y comunes: *Identificación de los de los activos críticos para la misión	La organización identificó lo activos cibernéticos más críticos para el logro de la misión a través de análisis como el de "joyas de la corona" (Crown Jewels Analysis -CJA).	Anticipar	SI NO	

- Los resultados del nivel de madurez pueden ser visualizados en la hoja "RESULTADO CONSOLIDADO", donde se muestra un gráfico con el nivel de madurez de cada una de las disciplinas que apoyan la ciber-resiliencia organizacional y un cuadro resumen para entender el resultado.

- Identifique las prácticas que falta implementar para lograr el nivel de madurez meta definido para la organización; estas corresponden al GAP.
- Presente los resultados a la alta dirección.

4.4 Pruebas de campo para validación del modelo de madurez de ciber-resiliencia organizacional

Para la validación del modelo, se aplicó la herramienta de evaluación del nivel de madurez de ciber-resiliencia organizacional en cinco empresas, cuatro de ellas colombianas y una de ellas de El Salvador. Las empresas colombianas pertenecen a infraestructura crítica de los sectores estratégicos de agua (acueducto, saneamiento básico, red matriz) y electricidad (operación, generación, transmisión, distribución, comercialización). La empresa de El Salvador pertenece a la infraestructura crítica del sector estratégico de electricidad (distribución, transmisión y comercialización). Dada la confidencialidad del resultado de la evaluación, se anonimiza el nombre de las empresas evaluadas.

La herramienta de evaluación fue diligenciada por 4 responsables de ciberseguridad y 1 auditor de tecnología. El personal que diligenció las encuestas es conocedor de las organizaciones a las que pertenecen y tienen un alto conocimiento de ciberseguridad. Previo al diligenciamiento de la herramienta de evaluación, se realizó reunión para socializar la herramienta y resolver las dudas que se presentaran para su diligenciamiento. Las encuestas fueron recibidas por correo electrónico.

4.4.1 Resultado consolidado prueba de campo

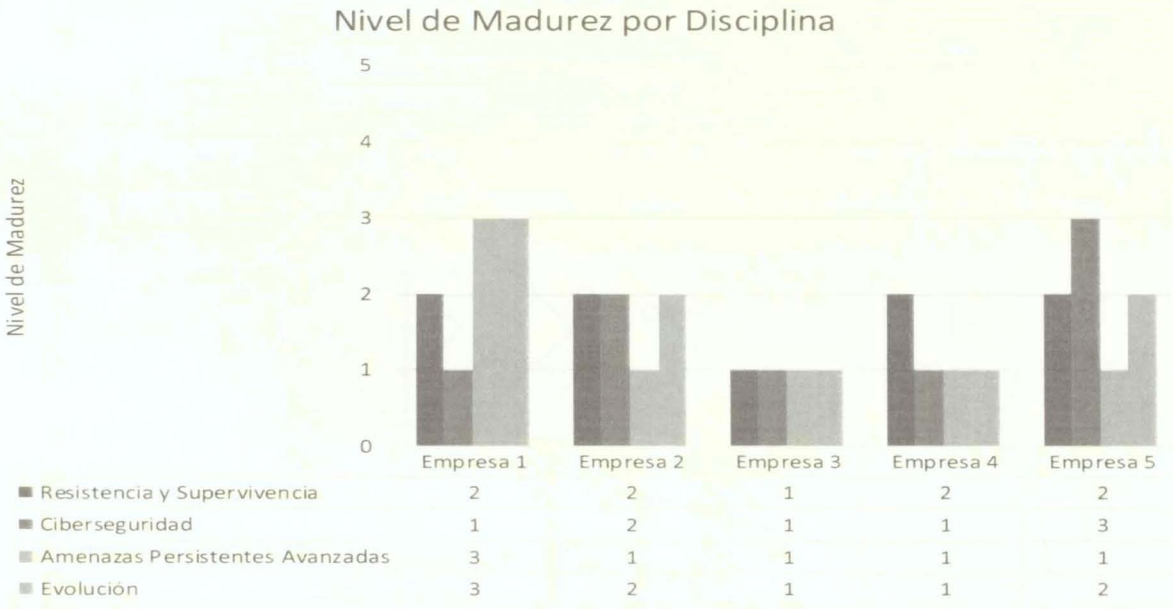


Figura 5. Nivel de madurez disciplinas de ciber-resiliencia consolidado prueba de campo

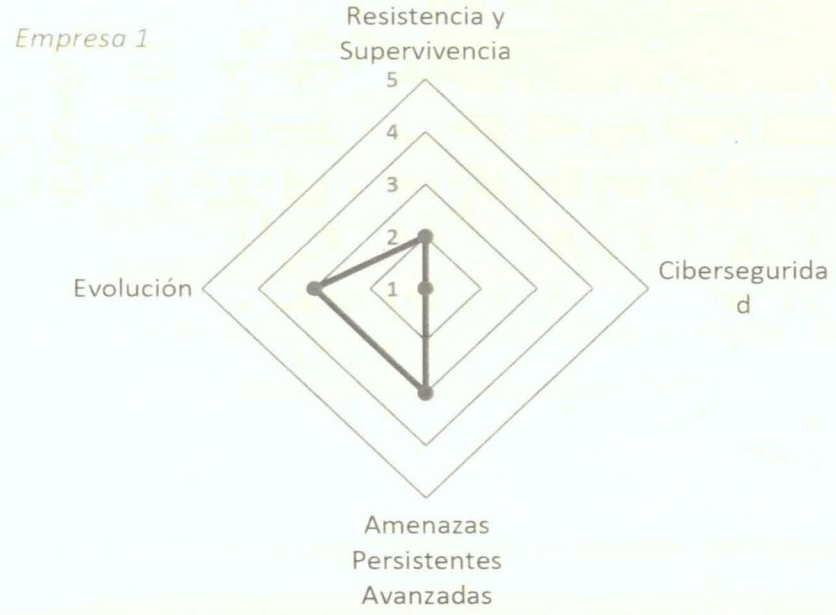
Fuente: elaboración propia.

Como resultado de la prueba de campo, se identificó que las disciplinas con un mayor nivel de madurez en las empresas evaluadas son las de resistencia y supervivencia y evolución, lo que indica que se está dando importancia a la identificación de los activos y ciberactivos críticos para la misión organizacional y las amenazas y vulnerabilidades asociadas a los mismos y a los indicadores de ciber-resiliencia. Así mismo, la disciplina con menores niveles de madurez es la de amenazas persistentes avanzadas, lo que indica que todavía no se ha

tomado conciencia acerca de los atacantes avanzados, no se ha profundizado en el conocimiento de este. La disciplina de ciberseguridad mostró que controles básicos enfocados para el atacante interno aún no han sido implementados.

Todas las organizaciones evaluadas aún están "En Riesgo" de pérdida de continuidad por un ataque cibernético del tipo amenaza persistente avanzada y su estado de preparación para afrontar este tipo de ataques es bajo. En términos generales, podemos concluir que en estas empresas se está empezando a desarrollar la capacidad de anticipar y las demás capacidades de ciber-resiliencia están en proceso de iniciar su desarrollo.

4.4.2 Resultado detallado Empresa 1



Disciplina	Nivel de Madurez	Descripción del nivel	Estado de desarrollo de las capacidades de ciber-resiliencia organizacional	Modelo Comparativo	Nivel de preparación para afrontar ataques cibernéticos
Resistencia y Supervivencia	2	*Gestionado*	*Anticipar- inicial*	*Organización "En Riesgo"*	*Bajo*
Ciberseguridad	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Amenazas Persistentes Avanzadas	3	*Definido*	*Anticipar-desarrollada Resistir-Inicial Recuperar-Inicial*	*Ejecutante competente*	*Medio*
Evolución	3	*Definido*	*Anticipar-desarrollada Resistir-Inicial Recuperar-Inicial*	*Ejecutante competente*	*Medio*

Figura 6. Resultado detallado Empresa 1

Fuente: elaboración propia.

4.4.2.1 Análisis de resultados Empresa 1

La empresa 1, deberá enfocar sus esfuerzos en mejorar las disciplinas de resistencia y supervivencia y de ciberseguridad para no estar "En riesgo", de tal forma que, como meta inicial, logre implementar prácticas que le permitan estar en un nivel 3-Definido en todas las disciplinas del modelo. Posterior a lograr el nivel de madurez 3 para todas las disciplinas, la organización debe determinar, acorde con su apetito de riesgo, el nivel de madurez objetivo final (nivel 4 o nivel 5) y con base en esto, definir un plan de mejora para la implementación de las prácticas que le están faltando por implementar en el nivel objetivo. Las prácticas priorizadas para alcanzar el nivel 3 de madurez son:

Disciplina de resistencia y supervivencia

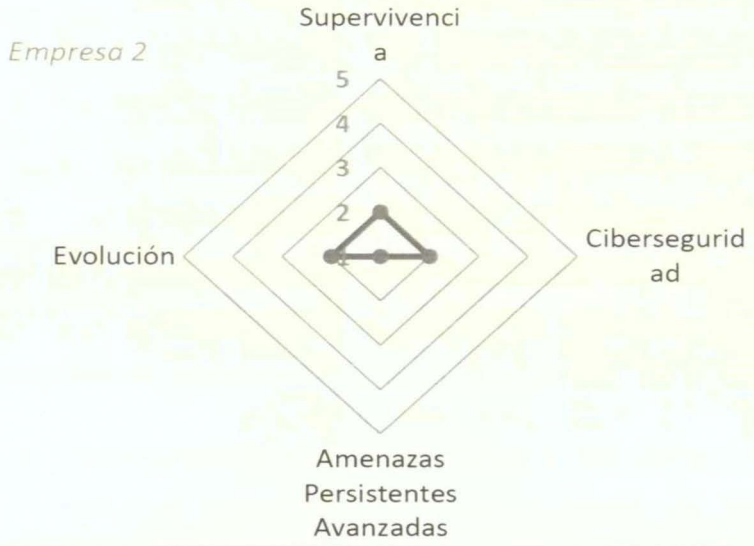
- Definir e implementar el plan de recuperación de desastres con estrategias que cubran los activos cibernéticos identificados como críticos comunes.
- Seleccionar las medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos críticos para la misión organizacional.
- Realizar análisis de modos de fallas y efectos críticos a sistemas ciber-físicos utilizando herramientas como análisis FMECA.

Ciberseguridad

- Control de acceso basado en el mínimo privilegio (se diseña para restringir los privilegios asignados a los usuarios y las entidades cibernéticas, y para establecer requisitos de privilegios sobre los recursos en función de la necesidad de uso y evento por evento).
- Monitorear las transacciones u operaciones realizadas por los usuarios finales para identificar actividades anormales.
- Monitorear periódicamente la infraestructura para detectar configuraciones erróneas y software desactualizado, probar el sistema de seguridad y mantener la actividad de los usuarios bajo control.

- Implementar prácticas de separación/segmentación de componentes (lógica o físicamente) basados en la criticidad y la confiabilidad, para limitar la propagación del daño.
- Limitar los puntos de control de acceso para accesos remotos.
- Implementar mecanismos para deshabilitar cualquier elemento del sistema que no sea de misión crítica que exhiba un comportamiento sospechoso.

4.4.3 Resultado detallado Empresa 2



Disciplina	Nivel de Madurez	Descripción del nivel	Estado de desarrollo de las capacidades de ciber-resiliencia organizacional	Modelo Comparativo	Nivel de preparación para afrontar ataques cibernéticos
Resistencia y Supervivencia	2	*Gestionado*	*Anticipar- inicial*	*Organización "En Riesgo"*	*Bajo*
Ciberseguridad	2	*Gestionado*	*Anticipar- inicial*	*Organización "En Riesgo"*	*Bajo*
Amenazas Persistentes Avanzadas	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Evolución	2	*Gestionado*	*Anticipar- inicial*	*Organización "En Riesgo"*	*Bajo*

Figura 7. Resultado detallado Empresa 2

Fuente: elaboración propia.

4.4.3.1 Análisis de resultados Empresa 2

Acorde con el modelo comparativo, la empresa 2 es una empresa "En Riesgo" de pérdida de continuidad por un ataque cibernético del tipo amenaza persistente avanzada. Su estado de preparación para afrontar los ataques cibernéticos es bajo. La disciplina con un nivel de madurez más bajo fue la de amenazas persistentes avanzadas, con un nivel de madurez 1-Inicial. Las demás disciplinas de resistencia y supervivencia, ciberseguridad y evolución, evidenciaron un nivel de madurez 2-Gestionado. Esta empresa ha iniciado a desarrollar la capacidad de anticipar, las demás capacidades de ciber-resiliencia están en proceso de iniciar su desarrollo. Se recomienda que esta empresa implemente las prácticas que le permitan pasar de estar en riesgo a ser un ejecutante competente, dando prioridad a las prácticas que le permitan alcanzar el nivel de madurez 3-Definido, lo que le permitirá tener un estado de preparación medio para afrontar las amenazas persistentes avanzadas. Las prácticas priorizadas para alcanzar el nivel 3 de madurez son.

Disciplina de resistencia y supervivencia

- Comprensión de las amenazas y los riesgos asociados a los activos cibernéticos críticos comunes y críticos, a través de herramientas como la evaluación de Susceptibilidad de Amenazas Cibernéticas (TSA).

Ciberseguridad

- Identificación de los componentes del sistema que pueden ser eslabones débiles para la ciberseguridad y aumentar la seguridad en estos puntos (componentes, personas, procedimientos).

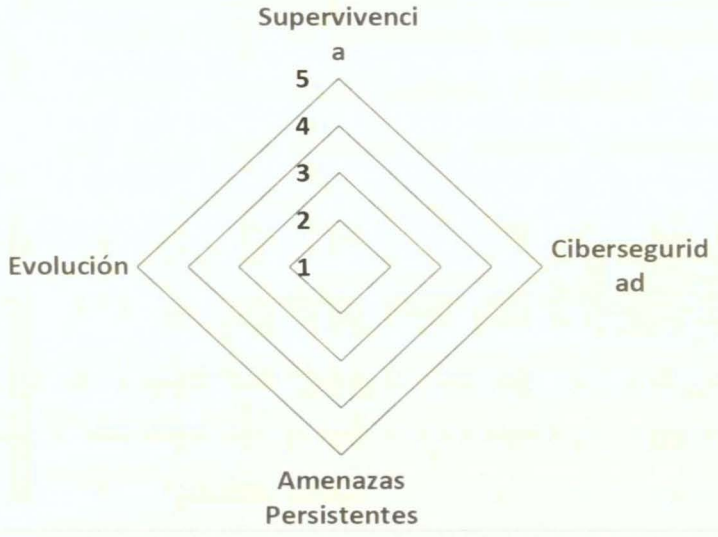
Amenazas persistentes avanzadas

- Conformar, capacitar y entrenar el equipo de respuesta a incidentes.
- Conocimiento de las tácticas y técnicas comunes usadas por el adversario.
- Prácticas de juegos de guerra.

Evolución

- Conformación del Centro de Operaciones de Ciberseguridad (SOC).

4.4.4 Resultado detallado Empresa 3



Disciplina	Nivel de Madurez	Descripción del nivel	Estado de desarrollo de las capacidades de ciber-resiliencia organizacional	Modelo Comparativo	Nivel de preparación para afrontar ataques
Resistencia y Supervivencia	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Ciberseguridad	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Amenazas Persistentes Avanzadas	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Evolución	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*

Figura 8. Resultado detallado Empresa 3

Fuente: elaboración propia.

4.4.4.1 Análisis de resultados Empresa 3

Acorde con el modelo comparativo, la Empresa 3 es una empresa "En Riesgo" de pérdida de continuidad por un ataque cibernético del tipo amenaza persistente avanzada. Su estado de preparación para afrontar los ataques cibernéticos es muy bajo. Todas las disciplinas están en un nivel de madurez 1-Inicial, donde las capacidades de ciber-resiliencia están en proceso de iniciar su desarrollo. Se recomienda que esta empresa implemente las prácticas que le permitan alcanzar un nivel de madurez 3-Definido, de tal forma que tenga un estado de preparación medio para afrontar los ataques cibernéticos. Las prácticas priorizadas para alcanzar el nivel de madurez 3 son:

Disciplina de resistencia y supervivencia

- Identificar los activos cibernéticos más críticos para el logro de la misión.
- Identificar los activos cibernéticos comunes a múltiples misiones o funciones de negocios que son objetivos potenciales de alto valor para los ciber atacantes, ya sea porque esos activos son críticos o porque su compromiso aumenta las opciones de movimiento lateral persistencia de los atacantes.
- Comprensión de las amenazas y los riesgos asociados a los activos cibernéticos críticos comunes y críticos.
- Implementar el plan de recuperación de desastres con estrategias que cubren los activos cibernéticos identificados como críticos comunes.
- Seleccionar las medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos críticos para la misión organizacional.
- Realizar análisis de modos de fallas y efectos críticos a sistemas ciber-físicos.

Ciberseguridad

- Realizar escaneo periódico de los puertos de red y corrección de las inconsistencias.
- Gestión de privilegios e implementación del principio del mínimo privilegio.
- Monitorear las transacciones u operaciones realizadas por los usuarios finales para identificar actividades anormales.
- Realizar control y monitoreo de los *end-point* (puntos finales).

- Importar solo software confiable al que se le ha verificado su legitimidad.
- Realizar validación de datos y del comportamiento para detectar actividades maliciosas (evidencia de compromiso).

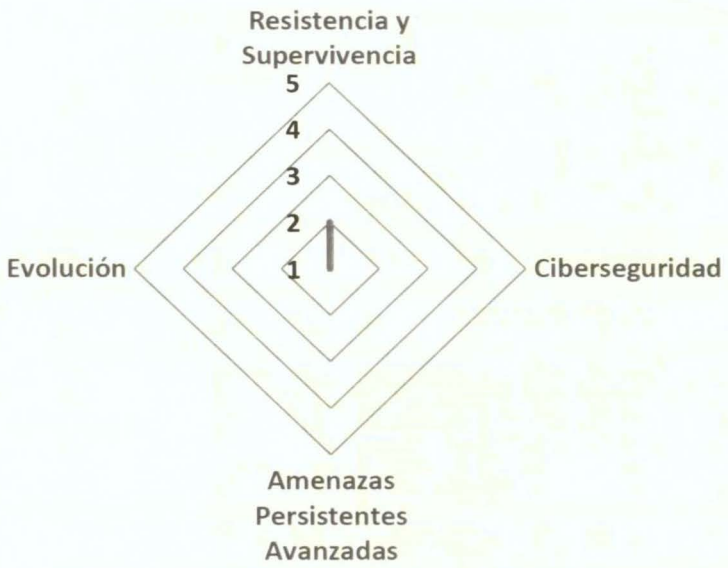
Amenazas persistentes avanzadas

- Conformar, capacitar y entrenar el equipo de respuesta a incidentes.
- Conocimiento de las tácticas y técnicas comunes usadas por el adversario.
- Prácticas de juegos de guerra.
- Entender el ciclo de vida de las amenazas persistentes avanzadas (*ciber kill chain*).

Evolución

- Definir los indicadores de ciberseguridad.
- Realizar medición, seguimiento y monitoreo a los indicadores de ciberseguridad por parte de la alta dirección de la organización.
- Analizar y gestionar los riesgos para amenazas conocidas.

4.4.5 Resultado detallado Empresa 4



Disciplina	Nivel de Madurez	Descripción del nivel	Estado de desarrollo de las capacidades de ciber-resiliencia organizacional	Modelo Comparativo	Nivel de preparación para afrontar ataques cibernéticos
Resistencia y Supervivencia	2	*Gestionado*	*Anticipar- inicial*	*Organización "En Riesgo"*	*Bajo*
Ciberseguridad	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Amenazas Persistentes Avanzadas	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Evolución	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*

Figura 9. Resultado detallado Empresa 4

Fuente: elaboración propia.

4.4.5.1 Análisis de resultados Empresa 4

Acorde con el modelo comparativo, la Empresa 4 es una empresa "En Riesgo" de pérdida de continuidad por un ataque cibernético del tipo amenaza persistente avanzada. Su estado de preparación para afrontar los ataques cibernéticos es muy bajo. La disciplina de resistencia y supervivencia se encuentra en un nivel 2-Gestionado, las demás disciplinas están en un nivel 1-inicial, por lo que podemos concluir que las capacidades de ciber-resiliencia están en proceso de iniciar su desarrollo. Se recomienda que esta empresa implemente las prácticas que le permitan alcanzar un nivel de madurez 3-Definido, de tal forma que tenga un estado de preparación medio para afrontar los ataques cibernéticos. Las prácticas priorizadas para alcanzar el nivel de madurez 3 son.

Disciplina de resistencia y supervivencia

- Seleccionar las medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos críticos para la misión organizacional.
- Realizar análisis de modos de fallas y efectos críticos a sistemas ciber-físicos.

Ciberseguridad

- Proteger los entornos de gestión u operaciones contra ataques de *phishing*.
- Realizar validación de datos y del comportamiento para detectar actividades maliciosas (evidencia de compromiso).

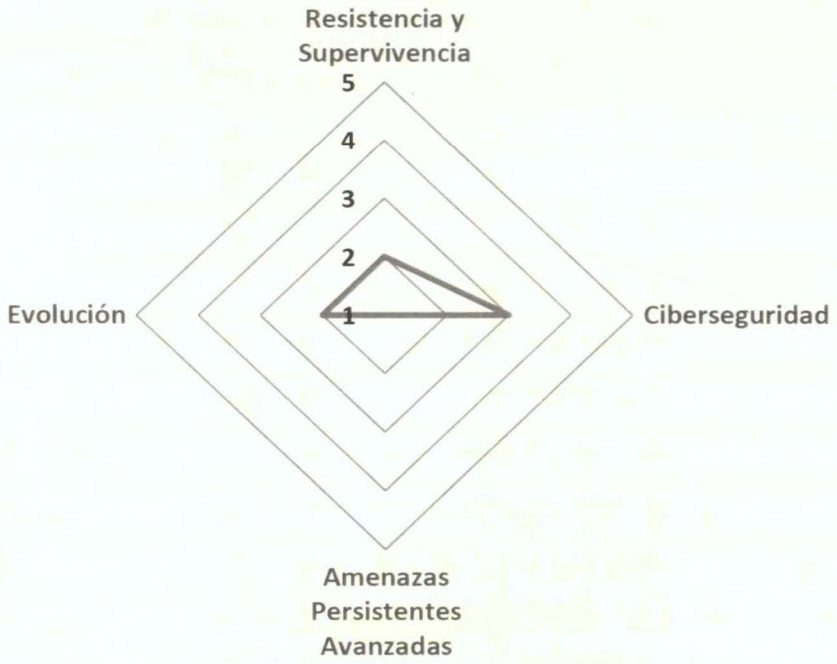
Amenazas persistentes avanzadas

- Conformar, capacitar y entrenar el equipo de respuesta a incidentes.
- Conocimiento de las tácticas y técnicas comunes usadas por el adversario.
- Prácticas de juegos de guerra.
- Entender el ciclo de vida de las amenazas persistentes avanzadas (*ciber kill chain*).

Evolución

- Realizar medición, seguimiento y monitoreo a los indicadores de ciberseguridad por parte de la alta dirección de la organización.
- Analizar y gestionar los riesgos para amenazas conocidas.

4.4.6 Resultado detallado Empresa 5



Disciplina	Nivel de Madurez	Descripción del nivel	Estado de desarrollo de las capacidades de ciber-resiliencia organizacional	Modelo Comparativo	Nivel de preparación para afrontar ataques cibernéticos
Resistencia y Supervivencia	2	*Gestionado*	*Anticipar- inicial*	*Organización "En Riesgo"*	*Bajo*
Ciberseguridad	3	*Definido*	*Anticipar-desarrollada Resistir-Inicial Recuperar-Inicial*	*Ejecutante competente*	*Medio*
Amenazas Persistentes Avanzadas	1	*Inicial*	*En proceso de iniciar desarrollo de capacidades*	*Organización "En Riesgo"*	*Muy Bajo*
Evolución	2	*Gestionado*	*Anticipar- inicial*	*Organización "En Riesgo"*	*Bajo*

Figura 10. Resultado detallado Empresa 5

Fuente: elaboración propia.

4.4.6.1 Análisis de resultados Empresa 5

Acorde con el modelo comparativo, la Empresa 5 es una empresa "En Riesgo" de pérdida de continuidad por un ataque cibernético del tipo amenaza persistente avanzada. Su estado de preparación para afrontar los ataques cibernéticos es bajo. Las disciplinas de resistencia y supervivencia, y de evolución, se encuentran en un nivel 2-Gestionado. La disciplina de amenazas persistentes avanzadas se encuentra en un nivel 1-Inicial y la disciplina de ciber-seguridad se encuentra en un nivel 3-Definido, por lo que podemos concluir que la capacidad de anticipar está en un estado inicial de desarrollo, mientras que las capacidades de resistir, recuperar y evolucionar están en proceso de iniciar su desarrollo. Se recomienda que esta empresa implemente las prácticas que le permitan alcanzar un nivel de madurez 3-Definido en todas las disciplinas de ciber-resiliencia, de tal forma que tenga un estado de preparación medio para afrontar los ataques cibernéticos. Las prácticas priorizadas para alcanzar el nivel de madurez 3 son las siguientes.

Disciplina de resistencia y supervivencia

- Entender las amenazas y los riesgos asociados a los activos cibernéticos críticos comunes y críticos.
- Seleccionar las medidas de mitigación para prevenir o combatir los ataques cibernéticos a los activos cibernéticos críticos para la misión organizacional.

- Realizar análisis de modos de fallas y efectos críticos a sistemas ciber-físicos.

Amenazas persistentes avanzadas

- Capacitar y entrenar el equipo de respuesta a incidentes.
- Conocimiento de las tácticas y técnicas comunes usadas por el adversario.
- Prácticas de juegos de guerra.
- Entender el ciclo de vida de las amenazas persistentes avanzadas (*ciber kill chain*).

Evolución

- Conformación del centro de operaciones de ciberseguridad (SOC).
- Análisis y comprensión de eventos de ciberseguridad.
- Analizar y gestionar los riesgos para amenazas que pueden entenderse como focales.

4.4.7 Errores que pueden afectar los resultados de la prueba de campo

En la aplicación de la herramienta de evaluación del nivel de madurez de ciber-resiliencia, pudieron presentarse errores relacionados con:

- Conocimiento del personal que diligenció la herramienta: es clave que el personal que diligencie la encuesta tenga conocimiento de la organización y de las prácticas que se están evaluando. La falta de conocimiento puede llevar a que se responda incorrectamente la evaluación, afectando los resultados de esta.
- Desconocimiento de la forma de diligenciar la herramienta. El desconocimiento de la forma en que funciona la herramienta puede llevar a errores en su diligenciamiento que pueden afectar el resultado de esta.
- Aplicar la herramienta considerando solo las prácticas relacionadas con tecnología de información TI. Si la organización maneja tecnología de información y tecnología de operación, las respuestas deben considerar los activos y ciberactivos que soportan ambas tecnologías; de otra forma, generará resultados incorrectos en relación con la realidad de la organización.

4.4.8 Mejoras identificadas para el modelo propuesto

Las mejoras identificadas para incluir en una próxima versión del modelo son:

- Expresar en una forma más granular algunas prácticas para identificar el camino a seguir por la organización para implementar la práctica, la evolución que da la práctica desde el nivel 1-Inicial, hasta el nivel donde sea requisito la implementación de la práctica.
- Efectuar mejoras a la herramienta de evaluación del nivel de madurez, de tal forma que se tenga una mayor comprensión del diligenciamiento de las respuestas en cada uno de los niveles de madurez; así mismo, mejorar la forma de presentar los resultados, para que se puedan identificar las prácticas implementadas y por implementar en cada una de las capacidades organizacionales.
- Automatizar la herramienta de evaluación de tal forma que un organismo de gobierno puedan usarla para analizar el nivel de madurez de ciber-resiliencia de las organizaciones que manejan infraestructura crítica del país.
- Poner otras opciones de respuesta a la implementación de las prácticas SI/NO/ parcialmente, y efectuar análisis teniendo en cuenta esto, y poder identificar más en detalle la brecha.

Conclusiones

En el trabajo realizado se abordó la problemática de cómo estructurar un modelo de madurez para orientar a las organizaciones en el desarrollo de las capacidades de ciber-resiliencia. Para la resolución de este interrogante, se plantearon tres objetivos que fueron alcanzados con el desarrollo trabajo, obteniendo como resultado:

- En el análisis del estado del arte se identificaron referencias bibliográficas con un gran aporte al modelo de madurez de ciber-resiliencia organizacional, dentro de las que se destacan los principios de diseño de ciber-resiliencia del MITRE, que fueron tomados como base para la formulación del modelo.
- Se identificaron los elementos clave para que una organización desarrolle sus capacidades de ciber-resiliencia. Estos elementos corresponden a las disciplinas de resistencia y supervivencia, ciberseguridad, amenazas persistentes avanzadas y evolución. Estas disciplinas están a su vez relacionadas con unos principios de diseño de ciber-resiliencia, los cuales permiten a las organizaciones focalizar sus esfuerzos en la implementación de prácticas para desarrollar sus capacidades de anticipar, resistir, recuperarse y evolucionar, con el propósito de estar preparadas para afrontar los ataques cibernéticos.
- La evolución de las capacidades organizacionales de ciber-resiliencia puede evidenciarse en las organizaciones, con la implementación de las prácticas que permiten su desarrollo. La identificación de las prácticas que apalancan el desarrollo de las capacidades de ciber-resiliencia se hizo teniendo en cuenta los principios de diseño de ciber-resiliencia. Cada principio tiene asociadas prácticas que desarrollan las capacidades de ciber-resiliencia.
- Se formuló una propuesta de un modelo de madurez de ciber-resiliencia organizacional que considera cinco niveles de madurez de desarrollo de las capacidades organizacionales de ciber-resiliencia para afrontar ataques cibernéticos que pongan en riesgo la continuidad del negocio. Los niveles de madurez se alcanzan implementando prácticas organizacionales direccionadas por unos principios de ciber-resiliencia

relativos a las disciplinas de resistencia y supervivencia, ciberseguridad, amenazas persistentes avanzadas y evolución.

El modelo de madurez de ciber-resiliencia organizacional diseñado, apoya la definición del plan estratégico de ciber-resiliencia organizacional, porque permite:

- Identificar las prácticas que las organizaciones deben implementar para desarrollar sus capacidades de ciber-resiliencia.
- Medir el estado de preparación de las organizaciones para afrontar los ataques cibernéticos e identificar la brecha entre el estado actual y el deseado.
- Focalizar y direccionar esfuerzos para fortalecer la ciber-resiliencia organizacional.

El modelo fue validado mediante la aplicación de una herramienta de evaluación del nivel de madurez de ciber-resiliencia organizacional en cinco empresas que manejan infraestructura crítica cibernética. Como resultado de la validación se pudo concluir que el modelo es aplicable para evaluar el nivel de preparación de las organizacionales que administran infraestructura crítica cibernética y recopilar oportunidades de mejora para ser incluidas en una versión posterior del modelo.

Aunque el modelo fue diseñado para aplicarse a infraestructuras críticas cibernéticas, podría ser extensible a cualquier industria o realidad económica con algunas adecuaciones.

Recomendaciones

Para apoyar la implementación de la Política Nacional de Seguridad Digital en Colombia, en lo relacionado con el fortalecimiento de la defensa y soberanía nacional en el entorno digital con un enfoque en gestión de riesgo y, teniendo en cuenta que este objetivo busca mejorar la protección y preservar la integridad y la resiliencia de la infraestructura crítica cibernética nacional (CONPES, 2016), se recomienda:

- Divulgar el modelo de madurez de ciber-resiliencia organizacional a las partes interesadas definidas en documento CONPES 3854 con especial énfasis a la Comisión Intersectorial y al Comando Conjunto Cibernético, en aras de analizar la posibilidad de

que esta herramienta sea utilizada para apoyar la mejora de la ciber-resiliencia de las organizaciones que administran infraestructura crítica en Colombia.

- Divulgación del modelo a las diferentes partes interesadas, para ajustar y mejorar la herramienta de evaluación del nivel de madurez de Ciber-resiliencia.
- Proponer la definición de un plan de trabajo que permita identificar el nivel de preparación de las organizaciones que manejan infraestructura crítica para afrontar ataques cibernéticos.
- Realizar trabajo conjunto entre el CCOC y proyecto distrito tecnológico de la Alcaldía de Medellín, para abordar el tema de ciber-resiliencia en la infraestructura crítica cibernética, de tal forma que se fomente la creación de herramientas que apoyen el desarrollo de las disciplinas de resistencia y supervivencia, ciberseguridad, amenazas persistentes avanzadas y evolución, para desarrollar las capacidades organizacionales de anticipar, resistir, recuperar y evolucionar que son claves para lograr que una organización sea ciber-resiliente.

Trabajos futuros

El desarrollo de esta investigación presenta dos aristas sobre las cuales futuros investigadores podrían desarrollar proyectos. La primera de ellas se refiere a expresar en forma más granular algunas de las prácticas para identificar el camino a seguir por la organización para implementar la práctica y la evolución de la práctica desde el nivel 1-Inicial, hasta el nivel meta establecido por la organización.

La segunda corresponde a efectuar mejoras en la herramienta de evaluación del nivel de madurez de ciber-resiliencia, tales como automatizar la herramienta, disponer de más opciones de respuesta y la posibilidad de generar automáticamente informes de las brechas existentes entre el estado actual y el deseado por la organización.

Glosario

Activo crítico. Instalaciones, sistemas o equipo eléctrico que, si es destruido, degradado o puesto indisponible, afecte la confiablidad u operatividad del sistema eléctrico. Acorde con las recomendaciones del Comité Tecnológico del CNO para la definición de activos críticos que comprometan la seguridad de operación del SIN. (CNO, 2015)

Amenaza. Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. (Icontec, 2017)

Ataque. Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo. (Icontec, 2017)

Ataque cibernético. acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. (Conpes 3854 de 2016)

Ciber activo. Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota. (CNO, 2015)

Ciber activo crítico. Dispositivo para Ia operación confiable de activos críticos que cumple los atributos descritos a continuación:

- El ciber activo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
- El ciber activo usa un protocolo enrutable con un centro de control. o,
- El ciber activo es accesible Por marcación

(CNO, 2015)

Ciberespacio. Es una red interdependiente de infraestructuras de información y comunicaciones, que incluye internet, redes de telecomunicaciones, sistemas informáticos, y procesos y controles embebidos. (US-CERT NICCS Cyber Glossary)

Cibernética. Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Academia de la Lengua Española)

Cibernético. Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Academia de la Lengua Española)

Ciber-Resiliencia. Cuando un sistema es capaz de soportar todo tipo de presiones sin cambiar su comportamiento, entonces es robusto. Cuando un sistema no es capaz de soportar más presiones, pero puede integrar cambios para disminuirlas y puede seguir adelante, entonces es ciber-resiliente. (US-CERT NICCS Cyber Glossary)

Ciberseguridad. es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio (Conpes 3854).

Continuidad del Negocio. Capacidad de una organización para continuar entregando productos o servicios a unos niveles predefinidos aceptables después de un incidente de interrupción. [ISO 22301:2012]

Infraestructura crítica. Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009)

Resiliencia. es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Conpes 3854)

Riesgo. Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas. (Conpes 2854 de 2016)

Vulnerabilidad. Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (Conpes 3854)

Referencias

Ali, N., & Hong, J. E. (2018). Failure detection and prevention for cyber-physical systems using ontology-based knowledge base. *Computers*, *7*(4). https://doi.org/10.3390/computers7040068

Att, K., & Strom, B. (2015). *Adversarial Tactics , Techniques and Common Cyber Attack Lifecycle ATT & CK*. (15).

BCMM, V. C. (2012). *Modelo de Madurez de Continuidad del Negocio - Versión 2.0 (Español)*. *0*(973), 1994–2012.

Bodeau, Deb, & Graubart, R. (2013). Cyber Resiliency and NIST Special Publication 800-53 Rev . 4 Controls. *Mitre Technical Report Mtr130531*, (September), 45.

Bodeau, Deborah, & Graubart, R. (2017). *Cyber Resiliency Design Principles*.

Bodeau, Deborah, Graubart, R., Picciotto, J., & McQuaid, R. (2011). Cyber Resiliency Engineering Framework. In *2012*. https://doi.org/MTR110237

Bougeret, M., Casanova, H., Robert, Y., Vivien, F., & Zaidouni, D. (2014). Using group replication for resilience on exascale systems. *International Journal of High Performance Computing Applications*, *28*(2), 210–224. https://doi.org/10.1177/1094342013505348

Cano, J. J. (2017). *La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial*. *5*, 1–5.

Caralli, R. A., Allen, J. H., Curtis, P. D., White, D. W., & Young, L. R. (2016). CERT ® Resilience Management Model. https://doi.org/10.1109/SocialCom.2010.173

Carrasco, L. D. S. (2015). *Ciber-resiliencia*. 1–15.

Carter, K. M., Okhravi, H., & Riordan, J. (2014). *Quantitative Analysis of Active Cyber Defenses Based on Temporal Platform Diversity*. Retrieved from http://arxiv.org/abs/1401.8255

CERTSI. (n.d.). *IMC _ 01- Metodología de evaluación de Indicadores para Mejora de la*

Ciberresiliencia (IMC).

Christopher, J. D., Gonzalez, D., White, D. W., Stevens, J., Grundman, J., Mehravari, N., … Dolan, T. (2014). Cybersecurity Capability Maturity Model (C2M2). *Department of Homeland Security*, (February), 1–76. Retrieved from https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program

Cibernético, C. C. (2016). *Sectores Estratégicos de la República de Colombia desde la óptica Cibernética.*

CIS, C. for I. S. (2019). *CIS Controls Versión 7 Spanish Translation*. Retrieved from https://learn.cisecurity.org/cis-controls-download

CONPES. (2016). *Política Nacional de Seguridad Digital*. 91. Retrieved from https://colaboracion.dnp.gov.co/CDT/Conpes/Econ﷿micos/3854.pdf

Cortés Novoa, A. F. (2017). *Amenazas Persistentes Avanzadas (APT): Modelo de funcionamiento y análisis de caso de estudio projectsauron*. Retrieved from http://repository.unipiloto.edu.co/handle/20.500.12277/2677

Curtis, P. D., & Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. *2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015*, 0–5. https://doi.org/10.1109/THS.2015.7225323

Dávila, J. C. (2013). *Capacidades Organizacionales: Dinámicas Por Naturaleza*. *26*(47), 11–33.

Department Of Defense United States Of America. (2013). *Resilient Military Systems and the Advanced Cyber Threat.*

Domenig, D. (2009). Building Secure, Resilient Architectures for Cyber Mission Assurance. *Applied Nursing Research*, *17*(3), 213–216. https://doi.org/10.1016/j.apnr.2004.07.001

Evans, P. E. (1987). Failure Mode Effects and Criticality Analysis. *Conference Record - Midcon*, *11*, 168–171. https://doi.org/10.1007/978-3-642-82014-4_3

Guijarro, A., Yepez, J., Peralta, T., & Ortiz, M. (2018). Defensa en profundidad aplicado a un entorno empresarial. *Espacios*, *39*(42).

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, M. del P. (2010). Metodología de la investigación. In *Metodología de la investigación*. https://doi.org/-ISBN 978-92-75-32913-9

Jackson, S. (2007). A multidisciplinary framework for resilence to disasters and disruptions. *Journal of Integrated Design and Process Science*, *11*(2), 91–108.

José, C. N., Hernandez, W., Estado, J. De, & Ccoc, M. (2016). *Infraestructura crítica cibernética*.

Lei, C., Zhang, H. Q., Tan, J. L., Zhang, Y. C., & Liu, X. H. (2018). Moving Target Defense Techniques: A Survey. *Security and Communication Networks*, *2018*(September). https://doi.org/10.1155/2018/3759626

Londoño, O. L., Maldonado, L. F., & Calderón, L. C. (2014). Guía para construir estados del arte. *International Corporation of Networks of Knowledge*, 1–39. https://doi.org/10.5672/apunts.2014-0983.es.(2012/1).107.10

McDaniel, P., Jaeger, T., La Porta, T. F., Papernot, N., Walls, R. J., Kott, A., … Neamtiu, I. (2014). Security and science of agility. *Proceedings of the ACM Conference on Computer and Communications Security*, *2014-Novem*(November), 13–19. https://doi.org/10.1145/2663474.2663476

MITRE. (2017). *Crown Jewels Analysis*. 1–6.

Musman, S., Temin, A., Tanner, M., Fox, D., & Pridemore, B. (2011). Evaluating the impact of cyber attacks on missions. *5th European Conference on Information Management and Evaluation, ECIME 2011*, 446–456.

Musman, S., & Turner, A. J. (2018). A game oriented approach to minimizing

cybersecurity risk. *International Journal of Safety and Security Engineering*, *8*(2), 212–222. https://doi.org/10.2495/SAFE-V8-N2-212-222

National Institute of Standars and Technology (NIST). (2018). *Marco para la mejora de la seguridad cibernética en infraestructuras críticas*. https://doi.org/10.6028/NIST.CSWP.04162018

NIST. (2013). NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. *NIST SP-800-53 Ar4*, 400+. https://doi.org/10.6028/NIST.SP.800-53Ar4

Page, E. H. (2016). Modeling and Simulation, Experimentation, and Wargaming - Assessing a Common Landscape. *Mitre Corporation*, (16), 1–11. Retrieved from https://www.mitre.org/sites/default/files/publications/16-2757-modeling-and-simulation-experimentation-and-wargaming.pdf

PANDA. (n.d.). *Understanding Cyber-Attacks*.

Panda security summit. (2018). *Ciber resiliencia: la clave de la seguridad empresarial*. Retrieved from https://www.pandasecurity.com/spain/mediacenter/src/uploads/2018/05/Informe-Ciber-resiliencia-ES.pdf

Partridge, K. G., & Young, L. R. (2011). *CERT ® Resilience Management Model (RMM) v1 . 1 : Code of Practice Crosswalk Commercial Version 1 . 1*. (October).

Pastor Perez, V., & Coz Fernandez, J. R. (2013). La conciencia situacional en la Ciberdefensa. *Revista SIC (Seguridad Informática y Comunicaciones)*, (February 2013), 90–92. Retrieved from http://revistasic.es/index.php?option=com_content&view=article&id=749&Itemid=733

Pérez-Mergarejo, E., Pérez-Vergara, I., & Rodríguez-Ruíz, Y. (2014). Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas. *Maturity Models and the Suitability of Its Application in Small and Medium Enterprises.*, *35*(2), 146–158.

Retrieved from http://ezproxy.uniandes.edu.co:8080/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=108922111&lang=es&site=eds-live&scope=site

Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S., & Calvo-Manzano, J. A. (2017). Modelos de Madurez en Ciberseguridad: una revisión sistemática. *Iberian Conference on Information Systems and Technologies, CISTI*. https://doi.org/10.23919/CISTI.2017.7975865

Ricci, N., Rhodes, D. H., & Ross, A. M. (2014). Evolvability-Related Options in Military Systems of Systems Evolvability-Related Options in Military Systems of Systems. *Procedia - Procedia Computer Science*, *28*(December), 314–321. https://doi.org/10.1016/j.procs.2014.03.039

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2019). Zero Trust Architecture. *Nist*, 40. https://doi.org/https://doi.org/10.6028/NIST.SP.800-207-draft

Schinagl, S., Schoon, K., & Paans, R. (2015). A framework for designing a security operations centre (SOC). *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2015-March*(April 2017), 2253–2262. https://doi.org/10.1109/HICSS.2015.270

SEI. (2010). CMMI ®para Desarrollo, Versión 1.3. *CMMI Para Dsarrolo, Version 1.3*, 23. https://doi.org/CMU/SEI-2010-TR-033 ESC-TR-2010-033

Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, *54*(8), 1245–1265. https://doi.org/10.1016/j.comnet.2010.03.005

Suárez, H., Gómez-Hidalgo, M., & Alvárez-Peláez, J. (2014). Ciber-Resiliencia: Aproximación a un Marco de Medición. *International Journal of Precision Engineering and Manufacturing-Green Technology*, *3*(1), 111–128. Retrieved from http://www.inteco.es/extfrontinteco/img/File/Estudios/int_ciber_resiliencia_marco_me

dicion.pdf

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2015). *Contingency planning guide for information technology systems: recommendations of the National Institute of Standards and Technology* (Vol. 1). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34.pdf

White, G. B. (2011). The community cyber security maturity model. *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 173–178. https://doi.org/10.1109/THS.2011.6107866