Institución Universitaria

Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa

Fredy Humberto Gómez Orjuela

Héctor Valencia Valencia

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2021

Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa

Fredy Humberto Gómez Orjuela

Héctor Valencia Valencia

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

MSc. Héctor Fernando Vargas Montoya

Línea de Investigación: Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2021

A nuestras familias por su paciencia acompañamiento y apoyo incondicional que nos motivó para terminar este proceso y lograr el objetivo propuesto.

Agradecimientos

Queremos expresar nuestro agradecimiento por todo el apoyo, los aportes y la paciencia que nuestros profesores, director del proyecto de grado, compañeros de clase, de trabajo y del proyecto de investigación, tuvieron con nosotros, sin ustedes este logro no habría sido posible.

"El proyecto ideal no existe, existe la oportunidad de realizar una aproximación"

Paulo Mendes Da Rocha

Resumen

Este proyecto establece un procedimiento de Gestión de incidentes de Ciberseguridad que se articula e integra a las actividades claves de la gestión de riesgos, continuidad del negocio, gestión de crisis y resiliencia con la respuesta corporativa de acuerdo con el nivel de escalamiento que un incidente de ciberseguridad pueda requerir para el restablecimiento de la disponibilidad de los posibles servicios afectados y que son soportados por las tecnologías de la operación (TO), dicho proyecto fue enfocado a las organizaciones del sector energético. Dicho procedimiento para la gestión de incidentes tiene en cuenta los requerimientos mínimos que una empresa de energía debe cumplir para ofrecer dicho servicio, con lo cual, ante un evento de seguridad, se propone una respuesta articulada, validando que la disponibilidad del servicio de energía cumpla con dichos requerimientos.

Para lograr el resultado esperado fue necesario; 1) definir una ficha técnica con los criterios mínimos de disponibilidad para la prestación del servicio de energía, 2) realizar un comparativo de los referentes relacionados con el tema de investigación para determinar las actividades claves de gestión de riesgos, gestión de crisis, continuidad y resiliencia, 3) identificar los componentes para diseñar un procedimiento de gestión de incidentes de ciberseguridad que se ajuste al sector y 4) validar con un caso de estudio que se pruebe su coherencia, efectividad y articulación con la respuesta corporativa para la atención de los incidentes de ciberseguridad.

El resultado obtenido es un procedimiento ante eventos de ciberseguridad que comprenda una gestión integral, en especial en los sistemas de control industrial donde el nivel de madurez en el manejo de este tipo de incidentes es bajo.

Palabras clave: Activos, ciberactivos, ciberseguridad, continuidad de negocio, gestión de crisis, gestión integral de riesgos, incidentes de seguridad, resiliencia, tecnologías de operación.

Abstract

This project establishes a Cybersecurity Incident Management procedure that is articulated and integrated into the key activities of risk management, business continuity, crisis management and resilience with the corporate response according to the level of escalation that an incident of cybersecurity may require for the reestablishment of the availability of the possible services affected and that are supported by the technologies of the operation (TO), said project was focused on the organizations of the energy sector. Said procedure for incident management takes into account the minimum requirements that an energy company must meet to offer said service, with which, in the event of a security event, an articulated response is proposed, validating that the availability of the energy service complies with these requirements.

In order to achieve the expected result it was necessary to: 1) define a technical sheet with the minimum availability criteria for the provision of the energy service, 2) carry out a comparison of the references related to the research topic to determine the key activities of risk management, crisis management, continuity and resilience, 3) identify the components to design a cybersecurity incident management procedure that is adjusted to the sector and 4) validate with a case study that tests its coherence, effectiveness and articulation with the corporate response for the attention of incidents cybersecurity.

The result is a security event procedure that includes comprehensive management, especially in industrial control systems where the level of maturity in incident management is low.

Keywords: Information assets, cyber security, business continuity, crisis management, integrated risk management, security incidents, resilience, operation technologies.

Contenido

Pág.

Lista de figuras

Lista de tablas

Glosario de términos

El glosario que a continuación se relaciona, aplica para los términos encontrados durante el desarrollo del trabajo de investigación realizado para la construcción del diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa.

- Activo. Es un recurso controlado por la entidad como resultado de sucesos pasados, del que la entidad espera obtener, en el futuro, beneficios económicos [1].

- 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 Concejo Nacional de Operación (CNO) para la definición de activos críticos que comprometan la seguridad de operación del Sistema Interconectado Nacional (SIN) [2].

- Amenaza. Posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí [3].

- Amenaza informática. La aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (Ministerio de Defensa de Colombia) [4].

- Ataque (attack). Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un uso no autorizado de un activo) [5].

- Ataque cibernético. Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia) [4].

- Causa. Condición de origen interno o externo que genera la posibilidad de que se presente un riesgo [6].

- CERT. (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas. Se refiere a una institución definida y concreta con capacidad centralizada para la coordinación de gestión de incidentes. (Universidad Carnegie Mellon) [3].

- 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 [3].

- Ciber activo crítico. Dispositivo para la 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 [3].

- Ciberespacio. Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009) [4].

- Ciber-Resiliencia. La ciber-resiliencia, es la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes [7].

- Ciberseguridad. Se entiende como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética, buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio de las interacciones digitales. La ciberseguridad tiene el fin de proteger a los usuarios y los activos de Estado en el Ciberespacio y comprende 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 para dicho fin [3].

- Crisis. Situación anormal e inestable que amenaza a los objetivos estratégicos de la organización, la reputación o la viabilidad [8].

- Confidencialidad (confidentiality). Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados [5].

- Confiabilidad (reliability). Propiedad de la consistencia del comportamiento deseado y los resultados [5].

- Consecuencia (consequence). Resultado de un evento que afecta a los objetivos [5].

- Continuidad del Negocio. Capacidad de una organización para continuar entregando productos o servicios a unos niveles predefinidos aceptables después de un incidente de interrupción. [9].

- Convergencia: Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1) [4].

- Disponibilidad (availability). Propiedad de ser accesible y utilizable a demanda por una entidad autorizada [5].

- Ecosistema Digital: Se refiere a la dinámica de relaciones propias que tiene una organización en la red, en la que las conexiones definen una identidad digital de la empresa, que no es otra cosa que la capacidad de modificar anticipadamente su modelo de negocio para mantener sintonía con la red [10].

- Enfoque Sistémico (PHVA): Es un concepto gerencial que facilita la gestión que se realiza en las organizaciones, con el fin de obtener los resultados esperados. También se conoce como una herramienta de mejora continua, presentada por Deming; se basa en un ciclo de 4 pasos: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act). Es un instrumento fundamental para la administración de los procesos, en el mantenimiento y mejoramiento continuo de su desempeño y por consecuencia de los resultados del área o de la empresa [11].

- Estructura de alto nivel: La estructura de alto nivel es un sistema de redacción que se ha desarrollado por un comité de control, que pretende la uniformidad de las normas ISO. El propósito de esta estructura es lograr consistencia y alineamiento de los estándares de sistemas de gestión de la ISO por medio de la unificación de su estructura, textos y vocabulario fundamentales [12].

- Evento (event). Ocurrencia o cambio de un conjunto particular de circunstancias [5].

- Evento de seguridad de la información (information security event). Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, una falla en los controles o una situación previa desconocida hasta el momento y que puede ser relevante para la seguridad [5].

- Gestión de la continuidad de negocio. Proceso de gestión integral que identifique las amenazas potenciales para una organización y los impactos en las operaciones comerciales esas amenazas, de realizarse, podrían causar, y que proporciona un marco para aumentar la resiliencia organizacional con la capacidad de dar una respuesta eficaz que salvaguarde

los intereses de sus grupos de interés clave, reputación, la marca y las actividades de creación de valor. [9].

- Gestión de crisis. Desarrollo y aplicación de la capacidad de la organización para hacer frente a las crisis [8].

- Gestión de incidentes de seguridad de la información (information security incident management). Procesos para la detección, reporte, evaluación, respuesta, tratamiento, y aprendizaje de incidentes de seguridad de la información [5].

- Gestión de la resiliencia organizacional. (Gestión) Actividades coordinadas para dirigir y controlar (resiliencia organizacional) las capacidades de una organización para absorber un ambiente cambiante y adaptarse a él. [13]

- Gestión del riesgo. Actividades coordinadas para dirigir y controlar la organización con relación al riesgo [14].

- Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. [15].

- Incidente. Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital [3].

- Incidente de seguridad de la información (information security incident). Evento único o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen

una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información [5].

- Incidente de ciber Seguridad. Cualquier acto malicioso o evento sospechoso que compromete o intenta comprometer la seguridad física o electrónica de un Ciber Activo Crítico o su perímetro [2].

- 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 [4].

- Infraestructura crítica cibernética: 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" [16].

- Integridad (integrity). Propiedad de exactitud y completitud [5].

- Ransomware: Su nombre no es casualidad: el término con el que comienza, "ransom", es una palabra inglesa que significa "rescate". El ransomware es un software extorsivo: su finalidad es impedirte usar tu dispositivo hasta que hayas pagado un rescate. el riesgo del ransomware depende del tipo de virus. Existen, básicamente, dos clases de ransomware: el ransomware de bloqueo, por un lado, y el ransomware de cifrado, por el otro. Se diferencian de este modo el ransomware de bloqueo afecta las funciones básicas del equipo y el ransomware de cifrado cifra archivos individuales. El tipo de malware importa no solo por lo que hace, sino también porque afecta el modo de identificarlo y de contrarrestar sus efectos. Las dos clases generales se dividen, a su vez, en distintos tipos de ransomware. Algunos ejemplos de ransomware son Locky, WannaCry y Bad Rabbit. [17].

- 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 [18].

- Resiliencia organizacional: Capacidad de una organización para anticipar, preparar, responder y adaptarse al cambio incremental y repentinas interrupciones con el fin de sobrevivir y prosperar [19].

- Respuesta corporativa. Actuar rápidamente por parte de la empresa y los equipos de respuesta de manera informada y con el efecto deseado cuando se vea afectada por una crisis y sostener la respuesta ante la crisis a largo plazo, con un esfuerzo dirigido estratégicamente para recuperar la reputación y el valor. Marco de referencia para la gestión de las crisis [8].

- Riesgo. Efecto de la incertidumbre sobre los objetivos. ISO 31000:2018. En términos generales, y en línea con la Sociedad de análisis de riesgos (SRA), el riesgo describe las consecuencias (futuras) que pueden surgir del funcionamiento de nuestros sistemas y de nuestras actividades, y la incertidumbre asociada. Se refiere a las consecuencias de una actividad futura, por ejemplo, el funcionamiento de una Infraestructura Critica, cuando las consecuencias son con respecto a algo que los seres humanos valoran (servicios Públicos, transporte, salud. Entre otros) [14]

- Riesgo informático. Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información [3].

- Riesgo de seguridad digital. Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el

ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan [18].

- Seguridad digital. Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país [3].

- Seguridad de la información (information security). Preservación de la confidencialidad, la integridad y la disponibilidad de la información [5].

- Seguridad Lógica. Consiste en la aplicación de barreras que resguarden el acceso a los datos y sólo se permite acceder a ellos a las personas autorizadas [4].

- Vulnerabilidad (vulnerability). Debilidad de un activo o de un control (2.16) que puede ser explotada por una o más amenazas. NTC-ISO/IEC 27000. la vulnerabilidad de un sistema se refiere al riesgo y el grado en que el sistema puede verse afectado por una fuente de riesgo o agente, El concepto de vulnerabilidad visto como una propiedad global del sistema incorpora otros tres conceptos claves en una infraestructura critica, a) Grado de pérdidas y daños b) Grado de exposición a los peligros, y daños (esto depende de la robustez del sistema, que es el antónimo de vulnerabilidad); y c) Grado de resiliencia [5].

Introducción

El mundo digital está transformando muchas industrias, y la de energía y servicios públicos no es una excepción. Hoy en día, la tecnología digital está cambiando la forma en que operan las empresas de energía y servicios públicos tales como crean valor, atención de los clientes, gestionan los riesgos, optimizan los procesos y capturan nuevas oportunidades de mercado.

Esta evolución acelerada de la tecnología y las comunicaciones en todas las esferas de la vida, particularmente en las empresas, demanda entender ahora una nueva realidad interconectada, en la que los productos y servicios se definen en medio de lo que se llama un ecosistema digital y que se refiere a la dinámica de relaciones propias que tiene una organización en la red, en la que las conexiones definen una identidad digital de la empresa, que no es otra cosa que la capacidad de modificar anticipadamente su modelo de negocio para mantener sintonía con la red [10]. Muestra de ello es ver como se está produciendo una convergencia entre las tecnologías de los sistemas de información (IT) y las tecnologías de Operación (OT), que antes estaban claramente separados dentro de diferentes unidades de negocio en una organización. Esta convergencia ya ha iniciado y las empresas se encuentran en esa travesía [20].

Otra situación que se observa en las empresas donde convergen tanto las tecnologías de información como las tecnologías de operación, es que la respuesta ante un incidente de seguridad no se visualiza integral y se presentan esquemas paralelos tanto de recursos como de procedimientos, lo que incrementa el desperdicio y las dificultades en la respuesta y recuperación, aumentando los tiempos y posibles conflictos en las organizaciones [21] por lo cual, establecer procesos para la integración de las diferentes respuestas igualmente con gestión de crisis, se hace fundamental ante eventos de ciberseguridad.

En este contexto, La ciberseguridad define desde el punto de vista empresarial, una realidad que le permite prepararse, comprender, responder y recuperarse de escenarios de ciber riesgos propios de un ecosistema digital [10], pero esta ciberseguridad en los sistemas de tecnología de la operación (en adelante TO), se ve comprometida por nuevas amenazas, explotación de vulnerabilidades, así como de mayores complejidades en los ataques, haciendo que los

procedimientos de respuestas a incidentes de ciberseguridad se deban crear o ajustar a una nueva realidad.

Los sofisticados actores y los estados nacionales explotan las vulnerabilidades para robar información y dinero y están desarrollando capacidades para interrumpir, destruir o amenazar la prestación de servicios esenciales. En 2017, la firma consultora de auditoría y seguridad Deloitte, informó que la industria de la energía era el segundo objetivo más popular para los ataques cibernéticos en 2016 [22]. Casi tres cuartos de las compañías de petróleo y gas de los Estados Unidos, según la consultora, tuvieron un incidente cibernético en dicho año; no obstante, sólo una pequeña mayoría citaron el riesgo como una de las principales preocupaciones en sus informes anuales.

Estas compañías hoy en día tienen miles de dispositivos conectados y esto conlleva a una situación muy preocupante de ciber riesgo en el petróleo y el gas [23]. A su vez, el riesgo de ataques cibernéticos en infraestructura crítica y fraude o robo de datos ha sido siempre una prioridad para los líderes empresariales a nivel mundial. Según el Informe de Riesgos Globales 2020 del Foro Económico Mundial, el riesgo de ciberataques a la infraestructura crítica y el fraude o robo de datos se clasificaron entre los 10 principales riesgos con mayor probabilidad de ocurrir, mientras que la reciente Perspectiva de Riesgos del COVID-19 del Foro Económico Mundial identificó los ciberataques como la tercera mayor preocupación debido a nuestra actual y sostenida transición hacia los patrones de trabajo digital.

Los datos disponibles respaldan estas preocupaciones; se estima que los daños por delitos cibernéticos alcanzarán los US$6 billones para 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo. Además del costo financiero, el cibercrimen y los ciberataques socavan la confianza de los usuarios en la economía digital. Las encuestas indican que, de la población mundial con acceso a Internet, menos del 50% confía en que la tecnología mejorará sus vidas, lo que demuestra una creciente y profunda falta de confianza con respecto a la privacidad de los datos [24].

Rimel Fraile Fonseca, Experto de Digiware, indica que uno de los sectores más afectados por el cibercrimen es el energético, donde estudios revelan un incremento sustancial en los ataques

durante los últimos años, con un costo aproximado de US$ 17.20 millones al año. “La industria que se dedica a la generación, transporte y distribución de energía está registrando un elevado índice de incidentes y se ubica en segundo lugar en cuanto a ciberataques después del sector financiero.

A medida que la transformación digital se ha extendido en este mercado, también ha aumentado el cibercrimen, con ataques cada vez más sofisticados a las infraestructuras críticas -entendidas como aquellas que proveen servicios básicos a la población” [25].

En Colombia, se registraron más de 7 billones de intentos de ciberataques durante 2020, de un total de 41 mil millones en América Latina y el Caribe. Considerando solo los meses de octubre, noviembre y diciembre, hubo 1,6 mil millones de intentos de ataques en el país. Durante este período, amenazas conocidas como correos electrónicos de phishing se extendieron por América Latina con archivos HTML adjuntos, tratando de redirigir el navegador web a sitios web maliciosos. El malware basado en la web se ha convertido en el vehículo más común para distribuir archivos infectados, convirtiéndose a menudo en la puerta de entrada para el ransomware. Aunque el volumen de intentos de ciberataques sigue siendo extremadamente alto, lo más preocupante es el grado de sofisticación y eficiencia que están logrando los ciberdelincuentes mediante el uso de tecnologías avanzadas e inteligencia artificial (IA) para desarrollar ataques dirigidos con mayores posibilidades de éxito.

Esto significa que, en menos intentos, los ciberdelincuentes pueden hacer más daño. “El año 2020 demostró la capacidad de los delincuentes para invertir tiempo y recursos en ataques más lucrativos, como el ransomware. Además, se están adaptando a la nueva era del trabajo remoto con acciones más sofisticadas para engañar a las víctimas y acceder a las redes corporativas”, explica Juan Carlos Puentes, Country Manager de Fortinet Colombia. “También se observa una tendencia hacia los ataques periféricos y no solo a la red central. El uso de dispositivos IoT en entornos industriales de misión crítica son algunos ejemplos de puntos de acceso para los delincuentes" [26].

En el reporte de ciberseguridad 2020, elaborado por el observatorio de ciberseguridad de la Universidad de Oxford, se presenta un informe acerca de las tendencias regionales en el estado de preparación en ciberseguridad, 2016-2020, allí se observan los resultados de las evaluaciones de

seguridad cibernética en toda la región y detalla los puntos clave sobre los que se sustenta dicha capacidad, a través de un Modelo de Madurez para las Naciones (CMM, por sus siglas en inglés), que fue la base de los estudios regionales de la OEA y el BID en 2016 y 2020, con un enfoque integral que entiende la capacidad dentro de cinco dimensiones: (i) política y estrategia; (ii) cultura y sociedad; (iii) educación, capacitación y habilidades; (iv) marcos legales y regulatorios, y (v) estándares, organizaciones y tecnologías [24].

Así mismo, tras un ataque cibernético, Estados Unidos cerró en mayo del 2021 algunas de las plantas de transporte de oleoducto y declara el estado de la emergencia, dicho ciberataque de acuerdo con las fuentes de información fue generado por el grupo hacktivista DarkSide, generando una indisponibilidad nunca vista en la operación de este tipo de infraestructuras [27] .

Dada la magnitud y complejidad de esta tarea, es altamente aconsejable recurrir a las guías técnicas, estándares y metodologías ofrecidas por los organismos de normalización y autoridades en materia de ciberseguridad industrial para la implantación de un procedimiento de gestión de incidentes, que permita disponer de un mecanismo sólido para hacer frente de manera eficaz a una variedad de problemas de los riesgos a los que está expuesta, siempre ha sido algo que las organizaciones se esfuerzan para lograr [28].

En este sentido, es importante reconocer como lo han mencionado diferentes autores que la gestión de la organización, sumada a la gestión del riesgo, la ciberseguridad, la continuidad del negocio, así como la resiliencia son temas que aún se dificulta poderlos integrar, y se siguen manejando como silos [29]. Esto obstaculiza una adecuada gestión de los incidentes de ciberseguridad y la reducción de posibles impactos sobre la operación.

Por los resultados obtenidos durante la investigación de este proyecto a través del estado del arte, no se evidenció un procedimiento ante eventos de ciberseguridad que comprenda de manera integral diferentes aspectos como el manejo de incidentes, el manejo de las crisis, la continuidad de negocio y la resiliencia alineados con la respuesta corporativa, en especial enfocado en los sistemas de control industrial donde el nivel de madurez en el manejo de este tipo de incidentes es bajo.

Ante esta situación, si se crea y ejecuta un procedimiento de Gestión de incidentes de Ciberseguridad que articule e integre las actividades claves de la gestión de riesgos, continuidad del negocio, gestión de crisis y resiliencia con la respuesta corporativa de acuerdo con el nivel de escalamiento, se tendría una respuesta adecuada ante un evento de ciberseguridad que afecte la disponibilidad de los servicios que son soportados por las tecnologías de la operación (TO).

Por lo anterior lo que se buscó con éste proyecto de investigación, fue elaborar el diseño y documentar un procedimiento de gestión de incidentes de ciberseguridad en el contexto operativo de las Tecnologías de Operación de los sistemas de control industrial, mejorado en sus diferentes actividades siguiendo un enfoque sistémico, articulando mejores prácticas en riesgos, continuidad, gestión de crisis y resiliencia organizacional, con el fin de fortalecer las capacidades de respuesta y recuperación, articulado a la respuesta corporativa de la organización y dando cumplimiento a los requerimientos mínimos exigidos para ofrecer el servicio de energía.

En este sentido el proyecto de investigación se enmarcó en el siguiente objetivo general:

> "Diseñar un procedimiento de Gestión de Incidentes de Ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que, basado en prácticas internacionales, pueda integrarse a la respuesta corporativa, reduciendo los niveles de exposición al riesgo ante eventos de ciberseguridad".

Para lograr este objetivo, se plantearon los siguientes objetivos específicos:

- "Establecer las características y requerimientos mínimos del servicio de TO para tener en cuenta en el procedimiento, en cuanto a disponibilidad".
- "Identificar las actividades claves de la gestión de riesgos, continuidad del negocio, gestión de crisis y resiliencia, que se pueda articular a la respuesta corporativa".
- "Caracterizar los elementos que componen el procedimiento de Gestión de Incidentes de Ciberseguridad, a través de la revisión de estándares nacionales e internacionales".
- "Validar el procedimiento de Gestión de Incidentes de Ciberseguridad, a través de un caso de estudio".

Para lograr los objetivos, este trabajo final de dividió en un Marco teórico y estado del arte, donde se presentan los estudios y conceptos principales de los temas a tratar, la Metodología, la cual

describe los pasos que se llevaron a cabo para el desarrollo del proyecto y los Resultados, por último, se entregan las conclusiones, recomendaciones y trabajos futuros.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

Para construir el marco teórico es importante partir del entendimiento de algunos conceptos claves, iniciemos con el concepto de sistema de control industrial, presente en diferentes sectores productivos, es aplicado a un ambiente industrial y tienen como función principal el de gobernar un proceso productivo que se encuentra interconectado a un conjunto de dispositivos utilizados para manejar, monitorear y comandar a otro conjunto de elementos físicos o lógicos (sistemas), está compuesto por una variedad de sistemas compuestos por computadoras, dispositivos eléctricos, hidráulicos y mecánicos, así como por procesos manuales supervisados por humanos que monitorean y controlan todo tipo de proceso físico. Estos sistemas de control tienen, en general, periodos largos de operación y su modificación obedece solo a las actualizaciones necesarias o a la ocurrencia de fallas. Estos sistemas de control industrial han evolucionado en la implementación de dispositivos que antes eran discretos y cableados hacia dispositivos inteligentes distribuidos geográficamente, de gran capacidad de configuración, comunicación con módulos y protocolos. Esta evolución que paso de aplicaciones propietarias y cerradas, a implementaciones de arquitectura abierta, basadas en tecnologías digitales con estándares de tecnologías de información de dominio público [30].

Asociados a los sistemas de control industrial se encuentran las Infraestructuras Criticas que son en esencia sistemas artificiales a gran escala que funcionan interdependientes para producir y distribuir bienes esenciales (como como la energía, el agua y los datos) y servicios (como el transporte, la banca y la sanidad). Una infraestructura se considera crítica si su incapacidad de operar o destrucción tiene un impacto significativo en la salud, la seguridad, la economía y el bienestar social (Directiva 2008/ 114/CE). Un fallo en una infraestructura de este tipo, o la pérdida de su servicio, puede ser perjudicial para una sola sociedad y su economía, mientras que también puede producirse en cascada a través de las fronteras, provocando fallos en múltiples infraestructuras con posibles consecuencias catastróficas [31] [32].

En cuanto a la tecnología información (TI) se puede decir que se refiere a todo el espectro de las tecnologías necesarias para el procesamiento de la información, incluido software y hardware,

tecnologías de comunicaciones y servicios relacionados [31]. Las tecnologías de operación (OT) se conocen así al hardware y software que detecta o causa un cambio a través de la supervisión directa y/o control de dispositivos físicos, lógicos, procesos y eventos en la industria [31], se encuentran en una amplia gama de sectores con alta utilización de activos, realizando una gran variedad de tareas que van desde el monitoreo de Infraestructura crítica (CI) hasta el control de robots en una planta de fabricación [33].

Es importante mencionar algunas diferencias en las Tecnologías de información (TI) y las Tecnologías de Operación relevantes para su aplicación en los ambientes de producción; a) los sistemas de control industrial operan sobre procesos físicos, donde el concepto de tiempo real es de crucial importancia en el dimensionamiento de las posibles consecuencias que una interrupción puede generar, mientras que una interrupción en un servidor de correo no genera mayores inconvenientes desde la producción de un bien o servicio, y b) de las 3 características a proteger con respecto a la información: confidencialidad, disponibilidad e integridad, en el ambiente de TI se privilegia la confidencialidad, en cambio en un ambiente de TO se requiere de alta disponibilidad, por esto la diferencia de cómo se gestionan y se miden las consecuencias.

En cuanto a la ciberseguridad, se puede mencionar que desde el punto de vista empresarial es una realidad que prepara a la organización para comprender un escenario de amenazas digitales propias del ecosistema en el que opera y establece un conjunto de nuevas prácticas de defensa, anticipación y resiliencia, antes desconocidas y poco nombradas [10]. La ciberseguridad hace referencia al uso de la arquitectura de red, software y otras tecnologías para proteger a las organizaciones y a las personas contra los ataques cibernéticos. El objetivo de la ciberseguridad es prevenir o mitigar el daño a las redes informáticas, las aplicaciones, los dispositivos y los datos, o la destrucción de estos [34].

Otros conceptos relevantes en el trabajo de investigación, tiene que ver con las amenazas y vulnerabilidades en el contexto de la ciberseguridad para esto es importante reconocer que la gran mayoría de los componentes tecnológicos que usan todas las organizaciones a nivel mundial tienen vulnerabilidades. Según la compañía CYBSEC Security muchas de estas debilidades pueden nacer con el producto como parte del diseño, tal vez por la omisión de los requisitos mínimos de

seguridad de la información que todo nuevo producto software debe cumplir que debe considerarse por el analista de sistemas desde la fase misma de ingeniería de requisitos [35], y en otros contextos, de la operación como es en los sistemas de control industrial igual sucede, en parte debido al alto grado de dependencia que estos sectores presentan de internet y de las tecnologías de la información y de la comunicación (TIC), un fallo en la red o una incidencia sobre la misma podría suponer una vulnerabilidad y/o amenaza en materia de seguridad, bien de índole energética, sanitaria, económica… etc. Todo ello destaca la necesidad de realizar acciones que doten a esta nueva realidad de una estrategia de ciberseguridad [36].

¿Pero qué son las amenazas y vulnerabilidades en el ámbito de la ciberseguridad?, se encuentra que las amenazas de seguridad de la información o ciber amenazas son definidas por el Instituto Nacional de Estándares y Tecnologías (NIST) como un evento con potencial de afectar negativamente a las operaciones de una organización o a sus activos, a través del acceso no autorizado a un sistema de información, la destrucción, divulgación o modificación de información y/o la denegación de servicio.

En cuanto a las vulnerabilidades, la ISO 27000:2018 la define como la debilidad de un activo o control que puede ser explotado por una o más amenazas.

Se habla ahora de los riesgos y ciber riesgos en el contexto de la ciberseguridad. Según Voutssas M [22], define el riesgo como la probabilidad de que un evento nocivo ocurra combinado con su impacto o efecto nocivo en la organización. Se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto.

Según el portal de ISO 27001 en español, el riesgo asociado a la seguridad de la información se define como la “posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información”. Si se considera al riesgo como una ecuación, sus variables incluirían la combinación de la probabilidad de ocurrencia de un incidente de seguridad, considerado como una “serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.” y las consecuencias de este expresado en

términos del impacto producido, donde una vulnerabilidad puede considerarse como una "Debilidad de un activo o control que puede ser explotada por una o más amenazas" y una amenaza como "Causa potencial de un incidente no deseado, que puede provocar daños o un sistema o la organización" [35].

Para hablar de los ciber riesgos o riesgos cibernéticos, es importante primero mencionar unos conceptos del origen del término. El concepto moderno de lo cibernético, tecnología computacional basada en la comunicación humana, fue acuñado por Norbert Wiener (1894–1964) en su obra Cybernetics: or Control and Communication in the Animal and the Machine (Cibernética: o control y comunicación en personas y máquinas) [37].

Hoy en día, lo cibernético se caracteriza por ser todo lo que se relaciona con la tecnología computacional, especialmente, pero no únicamente, con Internet. Mucho se está hablando en estos momentos por el mundo, de los Ciber Riesgos o Cyber Risks, refiriéndose a los riesgos que acechan en el Ciber espacio. En especial el tema ha sido analizado con respecto al sistema bancario que sufre muchas pérdidas por estos motivos, pero, asimismo, se está hablando fuertemente en el mundo del seguro de estos peligros que acechan, dentro y fuera de la empresa aseguradora [37].

El tema de los Ciber Riesgos va mucho más allá de la acción de un hacker y se relaciona con actividades informáticas ilegales para sustraer, alterar, modificar, manipular, inutilizar o destruir información o activos, como ser dinero, bonos o bienes inmateriales, información, de las compañías o usuarios afectados, utilizando para dichos propósitos medios electrónicos o dispositivos electrónicos [37]. Por tanto, los ciber riesgos son todos aquellos peligros que se pueden dar debido al incremento de la importancia de las tecnologías en todo el proceso de negocio de las empresas.

Este incremento en las tecnologías es un arma clara de doble filo. Por un lado son claramente necesarias para la evolución de las organizaciones ya que aportan una mejora en la mayoría de los aspectos del negocio pero a la vez incrementan la vulnerabilidad del sistema, abriendo muchas más brechas por las que pueden acceder los hackers y, en el peor de los casos, a los ciber atacantes (cabe recordar que la diferencia entre hacker y ciber atacante es que los primeros se consideran

que son aquellos que tienen habilidades especiales con la programación y los segundos son aquellos que usan estas habilidades con intenciones fraudulentas o dañinas) [38].

Asociados a la ocurrencia de los ciber riesgos, se debe ser consciente de que cada uno de ellos puede derivar en otras variantes. Por ejemplo, una vez se ha producido un robo de información o un secuestro digital, posteriormente se puede sufrir una ciber extorsión reclamando dinero como compensación de no divulgar o para desbloquear la información. Además de todo esto, siempre que ocurre un ciberataque, hay otros daños asociados que se pueden derivar. Además de la pérdida de reputación, puede haber otras pérdidas, como puede ser la de competitividad, si se sufre el robo de información confidencial y secreta, una pérdida de beneficios por el tiempo que han estado parados los sistemas o incluso una responsabilidad civil derivada de haber sufrido un robo de información de terceros [38].

Otro concepto relevante en la investigación tiene que ver con los incidentes de seguridad de la información, según la ISO 27000:2018 se define como la ocurrencia de uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad de comprometer las operaciones comerciales y amenazar la seguridad de la información. Otro resultado lo entrega el Internet Security Glossary, RFC 2828, que dice que es un evento de seguridad relevante para un sistema en el cual las políticas de seguridad han sido desatendidas o traspasadas. En este sentido, los incidentes generan un ambiente de desconcierto y confusión en las organizaciones, durante el cual, si no se encuentran preparadas para atender dicha manifestación de violaciones a las políticas de seguridad, múltiples desaciertos se pueden cometer y comprometer la seguridad de la organización [39].

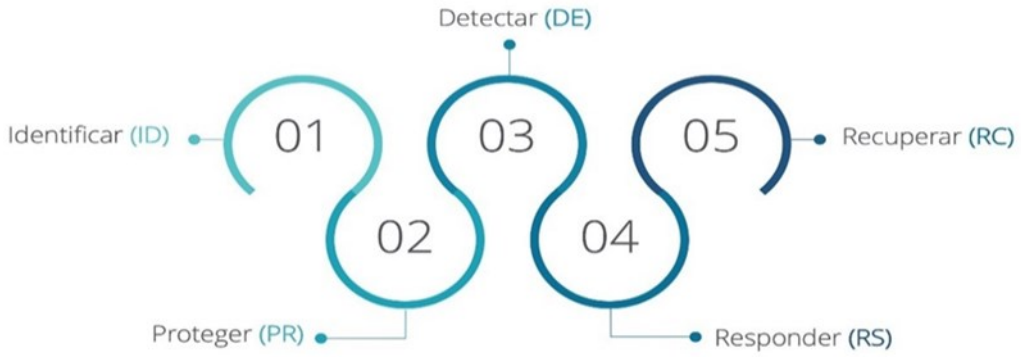
Continuando con la construcción del marco teórico, es importante mencionar la existencia actualmente en cuanto a modelos y estándares de orden internacional, tanto en las Tecnologías de Información como en las Tecnologías de Operación, y en ese sentido, es importante precisar que las OT tratan sobre la interacción entre los dispositivos computarizados y el mundo exterior, con el fin principal de capturar datos de la operación en los diferentes niveles de gestión de activos productivos o esenciales como por ejemplo SCADA, PLC´s, HMI, entre otros asociados a infraestructuras críticas. Tal es el caso del Instituto Nacional de Estándares y Tecnología de Estados

Unidos (NIST, por sus siglas en inglés) que es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.

El NIST desarrollo bajo la dirección de la Casa Blanca con la participación de la industria, la academia y los múltiples niveles de gobierno, el Marco de Ciberseguridad como una guía voluntaria de fácil entendimiento, con un "lenguaje común" que abarcara la totalidad de la gestión de riesgos de la seguridad cibernética y que las personas con todos los niveles de experiencia en seguridad cibernética puedan entenderlo fácilmente.

En la Figura 1-1, se muestra el núcleo que proporciona cinco funciones continuas de la ciberseguridad, las cuales se explican brevemente más abajo. Asimismo, también brinda un conjunto de actividades para lograr resultados específicos de ciberseguridad y hace referencia a ejemplos de orientación para lograrlos.

Figura 1-1. Núcleo del Marco de Referencia de Ciberseguridad (CSF, sus siglas en ingles).



Fuente: [40]

La función de identificar desarrolla una comprensión organizacional para administrar el riesgo de ciberseguridad para los sistemas, las personas, los activos, los datos y las capacidades. La función de proteger describe las salvaguardas para garantizar la entrega de servicios y limita el impacto. La función de responder incluye medidas con respecto a un incidente detectado y su capacidad de contener el impacto. La función de recuperar son actividades de resiliencia, recuperación de operaciones y restauración.

Un reto importante en las organizaciones hoy en día y que está relacionado con estas buenas prácticas, se llama Continuidad del Negocio, y se refiere a poder seguir prestando sus servicios ante eventos que afectan su operación y preparación para afrontar amenazas o incidentes. La norma ISO22300:2018 lo define como la capacidad de una organización para continuar con la entrega de productos y servicios en plazos aceptables a una capacidad predefinida en relación con un incidente perturbador [9].

De igual manera existe la capacidad de gestión de crisis. El instituto británico en su estándar BS 11200;2014 lo define como una situación anormal e inestable que amenaza a los objetivos estratégicos de la organización, la reputación o la viabilidad, otro autor Paul Remy nos habla desde su experiencia vivencial sobre como “las crisis son circunstancias que amenazan la vida o salud del negocio: quieren liquidarlo o dejarlo gravemente afectado, de forma que su futuro previsible difícilmente será el mismo” [41]

En cuanto a los temas de resiliencia es importante reconocer que cada vez los entornos donde las empresas, el estado y la sociedad conviven e interactúan de manera sistémica son cada vez más complejos, y particularmente al interior de cada una de ellas, se observan las mismas dificultades a nivel micro. En esa misma línea, la Organización Internacional de Estándares (ISO, por sus siglas en inglés) propone desde la norma ISO 22316:2017 que la resiliencia es la capacidad de una organización para absorber y adaptarse en un entorno cambiante que le permita cumplir sus objetivos, sobrevivir y prosperar [13]. Otro referente internacional es el Instituto Nacional de Ciberseguridad de España, menciona que el concepto de resiliencia se puede definir desde la ciberseguridad como la ciber-resiliencia, que es la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes [42].

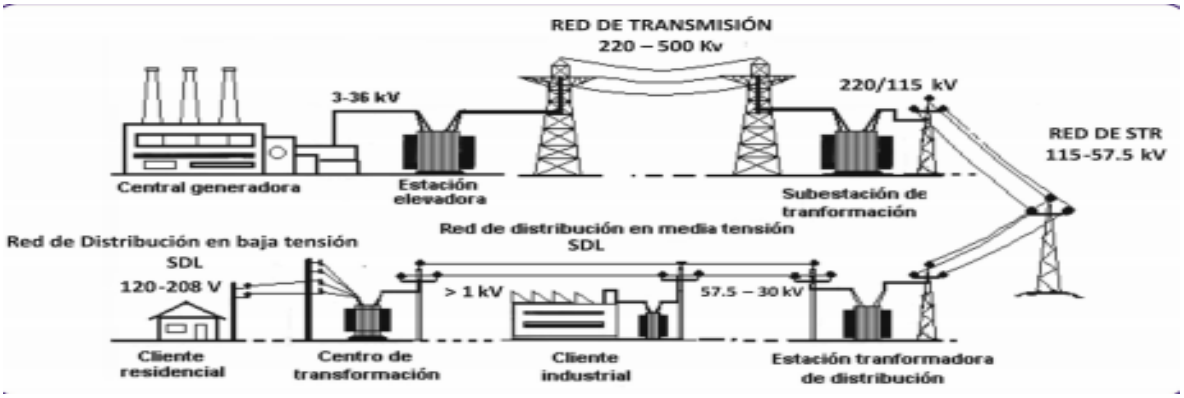
Otro de los componentes claves en la investigación del estado del arte fue conocer sobre cómo se presta el servicio de distribución energía, las generalidades, la regulación, los criterios para su operación, el proceso y su caracterización, los clientes, el objetivo, los indicadores, su seguimiento, producción y provisión del servicio como se describe a continuación.

1.1.1 Contexto prestación del servicio de energía

La actividad de distribución consiste en transportar la energía eléctrica por los Sistemas de Trasmisión Regional -STR- y los Sistemas de Distribución Local -SDL- Los SDL están conformados por el conjunto de redes, postes, transformadores, etc., que son utilizados para entregar la energía eléctrica en el domicilio de los usuarios finales. La mayoría de SDL se conectan entre sí a través de los STR. Los cuales interconectan diferentes regiones del país. Estos STR a su vez se conectan a otra red de mayor capacidad llamada el Sistema de Transmisión Nacional -STN- que interconecta a su vez los grandes centros de generación de la electricidad.

En la siguiente Figura 1-2, se puede ver de manera esquemática las diferentes actividades que acaban de explicarse y la forma como se relacionan entre ellas.

Figura 1-2. Proceso distribución de energía



Fuente: Distribución de energía eléctrica - CREG

La prestación del servicio de energía eléctrica se efectúa mediante las actividades de Transmisión: que consiste en llevar la energía desde los sitios de producción (centrales de generación) hasta los sitios de consumo, es decir, las ciudades y la mayoría de los municipios del país, pero no hasta las viviendas. Las torres y líneas de transmisión de energía podrían asimilarse a las autopistas nacionales que comunican todo el país, de las actividades de Distribución: que utilizan las redes de distribución para transportar la energía de menor voltaje que las líneas de transmisión, con el fin de llevar la energía desde las redes de distribución (postes, transformadores y redes) hasta las

viviendas o empresas, están las actividades del Servicio de Iluminación en espacios públicos de la ciudad y están las actividades de Comercialización de la energía eléctrica [43].

La distribución de electricidad es la etapa final en el suministro de electricidad a los usuarios finales. La red de un sistema de distribución lleva electricidad a partir de la red de transporte de alta tensión y la entrega a los consumidores. Típicamente, la red incluiría las líneas eléctricas y subestaciones transformadoras en media tensión (34,5 kV 2 kV a), y el cableado de distribución de bajo voltaje (menos de 1 kV) [44].

Si se fija en la evolución y tendencias de la industria energética, se puede observar que las redes eléctricas, desde la generación y la transmisión hasta la distribución y la comercialización están experimentando altos niveles de transformación en sus arquitecturas y una mayor convergencia entre las tecnologías de la operación (TO) y las tecnologías de la información (TI), así como de las tecnologías de las comunicaciones (TC). En las redes futuras, aparecerán cientos o miles de millones de dispositivos de energía distribuidos, paneles solares, nuevos medidores inteligentes para mediciones avanzadas, nuevos generadores de energía, otros medios de transporte eléctrico, ciudades y edificios inteligentes, nuevos tipos de almacenamiento de energía, así como de otros sistemas electrónicos de diversas magnitudes. Todos estos elementos adquirirán nuevas capacidades y soportaran nuevos servicios, lo que llevará a las redes y medios de comunicaciones a brindar acceso a interconectividad en lugares donde antes no había acceso. Aparecerán nuevas formas de generar y consumir energía y se utilizará de forma más flexibles y en ese momento aparecerán nuevas vulnerabilidades y riesgos cibernéticos [45] que se deberán tratar, para garantizar la prestación del servicio objeto de esta investigación. Y por último dentro de los elementos claves para el desarrollo de la investigación se encuentra conceptos como son la estructura de alto nivel y el enfoque sistémico basado en la gestión (PHVA). Mirar estos términos:

1.1.2 La estructura de alto nivel

Es un sistema de redacción que se ha desarrollado por un comité de control, que pretende la uniformidad de las normas ISO. La estructura de alto nivel define ahora, conceptos comunes a todas

las normas ISO como pueden ser el riesgo, la gestión documental, partes interesadas, contexto, etc.

El propósito de esta estructura es lograr consistencia y alineamiento de los estándares de sistemas de gestión de la ISO por medio de la unificación de su estructura, textos y vocabulario fundamentales.

Para las empresas, el enfoque es útil porque fomenta el uso de un solo sistema de gestión integrado que puede cumplir los requisitos de varias normas a la vez.

La Estructura de Alto Nivel del "Anexo SL", se ha convertido en la gran protagonista, a la hora de revisar las principales normas ISO (9001 y 14001, por ejemplo) y en la herramienta de uso imprescindible, durante la implementación de dichos Sistemas de Gestión en las organizaciones.
La Estructura de Alto Nivel, es un modelo normalizado, establecido para preparar el sistema de redacción de las normas de gestión ISO. Se encuentra definida en el Apéndice SL del documento ISO/IEC Directivas, Parte 1. Se trata de un denominador común, establecido por parte del Comité ISO, para que todas las nuevas normas de gestión respeten y compartan un objetivo común: la uniformización de las normas de gestión [46].

La Estructura de Alto Nivel "Anexo SL", no debe verse como un simple cambio en el esquema de los Sistemas de Gestión, eso sería simplificar demasiado, sino que es la respuesta a la búsqueda de un objetivo mucho más amplio, ya que con ella se puede [46]:

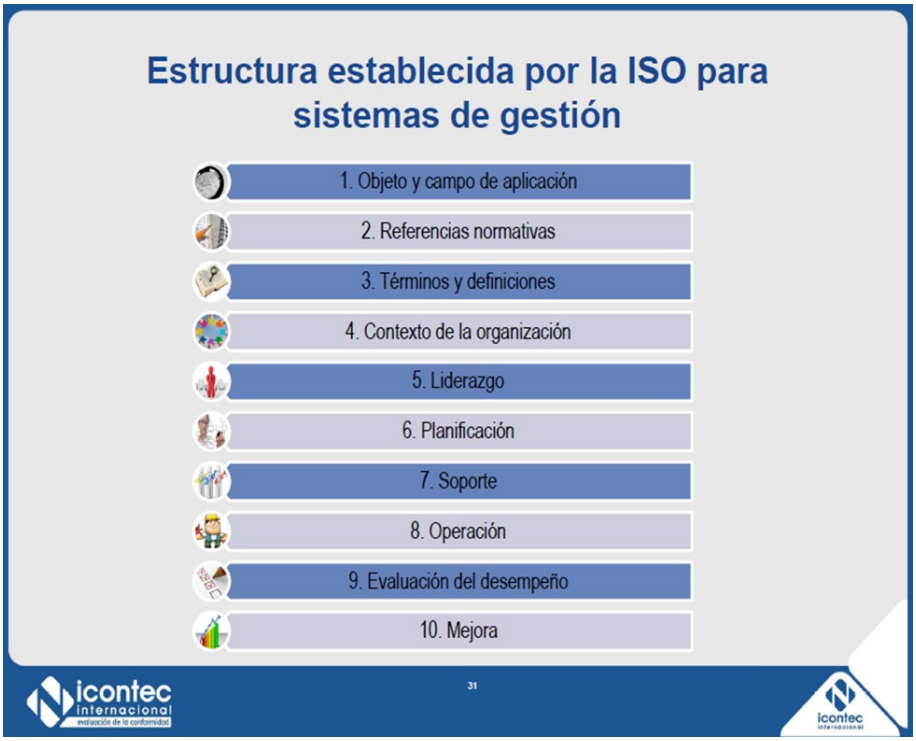
- Sincronizar diferentes normas (ISO 14001, ISO 9001, ISO 27001…).
- Adoptar un lenguaje común, para facilitar que las organizaciones integren diferentes Sistemas de Gestión y puedan disfrutar de algunas ventajas añadidas, como puede ser, la eliminación de la duplicidad documental.

La Estructura de Alto Nivel, consta de una estructura general común (Índice), con unos títulos de capítulos idénticos y con el mismo número de artículos [46]. Además, el Anexo SL, establece (Figura 1-3 y Figura 1-4):

Figura 1-3. Estructura de alto nivel

Fuente: [12]

Figura 1-4. Contenido estructura de alto nivel ISO



Fuente: [47]

1.1.3 Qué es el Ciclo PHVA

El ciclo PHVA de mejora continua es una herramienta de gestión presentada en los años 50 por el estadístico estadounidense Edward Deming. Tras varias décadas de uso, este sistema o método de gestión de calidad se encuentra plenamente vigente (ha sido adoptado recientemente por la familia de normas ISO) por su comprobada eficacia para: reducir costos, optimizar la productividad, ganar cuota de mercado e incrementar la rentabilidad de las organizaciones. Logrando, además, el mantenimiento de todos estos beneficios de una manera continua, progresiva y constante [48].

Aplicar el ciclo PHVA a partir de la adecuada interpretación de su planteamiento original, de su forma de operación, sus manifestaciones y el potencial que representa para la administración de la organización y para las personas, tiene como el fin el mejorar la efectividad de sus resultados.

Las fases del ciclo PHVA

Las siglas del ciclo o fórmula PHVA forman un acrónimo compuesto por las iniciales de las palabras Planificar, Hacer, Verificar y Actuar. Cada uno de estos 4 conceptos corresponde a una fase o etapa del ciclo (Figura 1-5) [48]:

- Planificar: En la etapa de planificación se establecen objetivos y se identifican los procesos necesarios para lograr unos determinados resultados de acuerdo con las políticas de la organización. En esta etapa se determinan también los parámetros de medición que se van a utilizar para controlar y seguir el proceso.
- Hacer: Consiste en la implementación de los cambios o acciones necesarias para lograr las mejoras planteadas. Con el objeto de ganar en eficacia y poder corregir fácilmente posibles errores en la ejecución, normalmente se desarrolla un plan piloto a modo de prueba o testeo.
- Verificar: Una vez se ha puesto en marcha el plan de mejoras, se establece un periodo de prueba para medir y valorar la efectividad de los cambios. Se trata de una fase de regulación y ajuste.

- Actuar: Realizadas las mediciones, en el caso de que los resultados no se ajusten a las expectativas y objetivos predefinidos, se realizan las correcciones y modificaciones necesarias. Por otro lado, se toman las decisiones y acciones pertinentes para mejorar continuamente el desarrollo de los procesos.

Figura 1-5. Ciclo PHVA

Fuente: [49]

El ciclo de Control se enriqueció con las aportaciones del Dr. Kaoru Ishikawa, quien lo definió como un proceso constituido por seis pasos según lo relacionado con la Tabla 1-1.

Tabla 1-1. Contenido ciclo PHVA

Planear	1 2	• Establecer Políticas, determinar Objetivos y Metas. • Establecer Métodos para alcanzar los Objetivos y las Metas / Estandarización
Hacer	3 4	• Comunicación, toma de conciencia y formación. • Ejecución de las actividades / Registro de datos.
Verificar	5	• Verificar los procesos y resultados obtenidos.
Actuar	6	• Tomar las acciones

Fuente: Ciclo de Control aportaciones Dr. Kaoru Ishikawa

1.2 Estado del arte

"Los diferentes sectores de la industria afrontan cambios profundos en el entorno de negocios en el marco de un contexto digital que avanza de forma acelerada, a diferencia de los lentos procesos de regulación, adaptación y gestión de los ciber riesgos que en el mediano plazo podrían causar grandes catástrofes." [50].

Estas organizaciones de todos los tamaños, tanto en el sector público como en el privado, dependen cada vez más de los activos y de las tecnologías disponibles, sin embargo, son las fallas de estos activos los que generan unos impactos directos en los diferentes procesos de los negocios que soportan. Esto, además, puede convertirse en una incapacidad para la prestación de los servicios, lo que finalmente afecta la misión de la organización.

Dadas estas relaciones, la gestión de los riesgos para estos activos es un factor clave para posicionar la organización para el éxito, acá es necesario reconocer la alta interdependencia y conectividad que tienen los riesgos cibernéticos y como las fallas que generan las interrupciones son de orden sistémico y no pueden ser un tema exclusivamente de las áreas de tecnología como sucede a diario, este es ya un asunto de interés de seguridad nacional y como tal dependen de un ciberespacio estable, seguro y resistente que se encuentra cada vez más expuesto y vulnerable a una amplia gama de riesgos derivados de amenazas y peligros tanto físicos como cibernéticos [23].

Esta dinámica de gestión de riesgos empresarial donde los diferentes actores claves tienen una vista parcial o segmentada reitera la vista de islas o silos que configura un riesgo corporativo sensible que es fragmentado en el entendimiento de estos, sin considerar las conexiones o acoplamientos que existen entre cada uno de ellos. Ignorar esta realidad en la lectura de los riesgos corporativos es mantener una vista desarticulada de los componentes de la dinámica del negocio y crear zonas grises donde se incuben nuevas amenazas y posibles eventos adversos, que, al materializarse, generan mayores inciertos, muchas preguntas y pocas respuestas. El ejercicio de lectura segmentada de los riesgos empresariales afecta la manera como se establecen las estrategias para sus tratamientos. En este sentido, la comprensión de los riesgos cibernéticos concluye con una revisión tecnológica, generalmente asociada con los riesgos de tecnología de información, con lo cual la ciberseguridad termina adscrita como un tema operativo que debe ser solucionado por los de tecnología. Asumir esta posición, es ignorar la vista sistémica e integrada que tienen los ciber riesgos, creando puntos ciegos en las iniciativas corporativas que pueden terminar afectando a sus diferentes grupos de interés [51].

Leer el riesgo cibernético de forma aislada, segmentada y desintegrada de la realidad empresarial, es equivalente a tratar de comprender la dinámica de los ecosistemas digitales actuales desde la vista de uno de sus participantes. El riesgo cibernético es un riesgo empresarial que busca encontrar oportunidades y retos para hacer de la organización un organismo vivo y resiliente, es un espacio de construcción de propuestas que utiliza el incierto como insumo para hacer la diferencia y crear la confianza requerida con los clientes [52].

Lo anterior implica establecer un modelo de vigilancia basada en riesgos [53] que cubra no sólo los riesgos conocidos y definidos en las buenas prácticas, sino que incluya aquellos latentes y emergentes, con el fin de construir una postura resiliente de la organización, que vaya más allá de la atención y control de un incidente. Esto es, reconocer los activos estratégicos de alto valor, ubicar a las personas como el centro de la estrategia, conectar con las tecnologías disruptivas y emergentes, asegurar la coordinación y cooperación con sus terceros de confianza (cadena de suministro) y tener un cuerpo directivo alfabetizado y educado sobre los retos del entorno cibernético y la inevitabilidad de la falla [54].

En este contexto, la ciberseguridad de los sistemas TO, en particular, se ve comprometida por vulnerabilidades sobrevenidas en un entorno con exigencias de seguridad específicas orientadas a la producción y considerablemente diferenciadas de las exigencias y estándares de los sistemas de información corporativos. A ello hay que añadir un escenario de crecientes amenazas de distinta naturaleza, bien intencional o accidental (errores, fraudes, espionaje, sabotaje, causas naturales, etc.), canalizadas en su mayor parte a través del ciberespacio y en no pocas ocasiones dirigidas a perturbar desde terceros países el funcionamiento de las infraestructuras críticas por razones geopolíticas o económicas.

En los últimos años, el riesgo de que se produzcan ciber incidentes está aumentando en los sistemas de control industrial (ICS), que son la función principal de las infraestructuras críticas (CI). Como resultado, las empresas que poseen ICs deben mejorar la capacidad de respuesta de la organización a los incidentes cibernéticos. Dado que los incidentes cibernéticos en las ICS no sólo causan problemas a la ciberseguridad, sino también a la seguridad de la planta y al negocio de la empresa, es esencial la respuesta de toda la empresa, incluyendo no sólo el departamento de TI, sino también el departamento de ICS y la capa de gestión. Para promover sin problemas esta respuesta de toda la empresa, los comandantes de incidentes que se ajustan entre los departamentos son esenciales. Sin embargo, muchas empresas que tienen ICS no educan adecuadamente a los Comandantes de Incidentes [29].

Esta situación ha llevado a la necesidad de establecer una gobernanza para controlar y alinear la estrategia empresarial [55] [56]. Aunque la aplicación de la gobernanza del riesgo (supervisión y control de riesgos) ha demostrado ser una tarea difícil para los consejos de administración en los últimos años [57] [58] algunas organizaciones siguen gestionando el riesgo en silos dentro de los departamentos y áreas de su organización. Mientras que los enfoques en silos implican debilidades en la defensa de una de la organización (es decir, cada departamento tiene su propia manera de afrontar los riesgos), también pueden causar graves problemas para comprender de forma holística la exposición de una organización a los riesgos o la duplicación de esfuerzos [59]. Una alineación de la gestión de la ciberseguridad con la gestión de riesgos en toda la empresa puede producir una mejor gestión de los riesgos, desde los análisis, mitigación, capacidad de recuperación y la

resiliencia. Se ha comprobado que su alineación (interconectividad y asociación) puede situar a toda la organización en un estado de seguridad más elevado a través de una perspectiva unificada de control, responsabilidad y toma de decisiones [60] [61]. Lo que es más importante, la ciberseguridad demuestra evolucionar desde las disciplinas técnicas hacia un enfoque holístico y un enfoque estratégico en la gestión de los riesgos. Al lograr la alineación, una organización es menos vulnerable a los cambios del mercado o a la ineficacia interna porque la alineación crea una solución común y centrada/unificada [62].

En resumen, la alineación de la ciberseguridad, la gestión del riesgo y la estrategia empresarial proporciona un apoyo holístico para la supervisión de los riesgos y alinea todas las estrategias hacia una sola (estrategia organizativa) para emplear todas las fuerzas en un solo ámbito para proteger a la organización y ofrecer capacidades integrales para lograr su objetivo. La Ciberseguridad alineada con la gestión de riesgos empresarial desempeña un papel esencial en la gestión y el control de forma holística. Pero existen inhibidores que no lo hacen tan fácil. Entre los principales inhibidores están las deficiencias de capacitación, las deficiencias culturales y la falta de una gobernanza adecuada [29].

Como respuesta a esta situación, gobiernos como el de Estados Unidos vienen trabajando en estrategias que proporcionan al Departamento de Seguridad Nacional un marco para identificar las responsabilidades de seguridad cibernética durante los próximos cinco años. De esta manera buscan mantener el ritmo del panorama de riesgo cibernético en evolución, mediante la reducción de las vulnerabilidades y la creación del concepto de ciber resiliencia; contrarrestar a los actores maliciosos en el ciberespacio; responder a incidentes, además de que el ecosistema cibernético sea más seguro y resistente.

Igualmente actores de alcance regional y global articulados desde instituciones como el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA), gobiernos de la región y organizaciones multilaterales vienen trabajando de manera conjunta para enfrentar los retos de la ciberseguridad, desde la generación de políticas de ciberseguridad fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, y la protección de infraestructuras críticas entre otros.

Un punto relevante que se relaciona con el trabajo de investigación es la "Divulgación responsable", este fue el aspecto con el puntaje de madurez más bajo de la región. La amplitud y el enfoque integrado del CMM permiten contextualizar aún más las puntuaciones de los aspectos individuales. En este sentido, los riesgos asociados con la falta de un mecanismo institucionalizado para compartir información sobre vulnerabilidades descubiertas y políticas sobre piratería ética podrían verse agravados por los puntajes igualmente bajos para las capacidades de respuesta interna, incluyendo "organización de protección de infraestructura crítica", "gestión de crisis", "gestión y respuesta a riesgos" y "seguro de delito informático", que se ubican en la parte inferior y han visto pocas mejoras desde 2015 [24].

Por otra parte, la organización ISO en febrero del 2018 presentó ISO/IEC TR 27103:2018 – Information technology — Security techniques (46), en busca de proporcionar una guía para facilitar la implementación de un marco de seguridad cibernética alineado con mejores prácticas existentes, de hecho, la ISO 27103 fomenta los mismos conceptos y las mejores prácticas contenidas en el Marco de Referencia de Ciberseguridad de NIST (CSF, por sus siglas en inglés).

A nivel global se hacen esfuerzos para implementar en dichos negocios niveles de seguridad, que permitan minimizar el riesgo con la adopción de las tecnologías que han llegado al mundo del control, monitoreo y la automatización industrial y para lograrlo, existen actualmente numerosas organizaciones dedicadas a la creación de normatividad y marcos de trabajo dedicadas a este sector de la Ciberseguridad, también se han desarrollado estándares (NERC, IEEE, IEC, ISO) con el objetivo de manejar esta situación y muchos más siguen en desarrollo.

También es importante destacar las redes colaborativas determinadas a fortalecer las relaciones entre las entidades gubernamentales, internacionales para la lucha contra la ciberdelincuencia a nivel internacional, (OTAN, OEA, OCDE) son alianzas que permiten unir esfuerzos colaborativos a nivel legal, económico, cultural y humanitario, para hacer frente a la nueva generación de delitos y actividades ilícitas en el ciberespacio, reconocido como otro dominio de operaciones para la defensa en este caso "Ciberdefensa" [63].

Este nuevo contexto evidencia la necesidad de reforzar las capacidades de ciber educación, entrenamiento, investigación y prácticas, con el fin de estar efectivamente capacitados a la hora de garantizar la resiliencia de las personas, las empresas y el estado en caso de ser afectados por cualquier incidente de ciberseguridad, ser capaces de prevenir, responder, mitigar y recuperarse de los incidentes que puedan presentarse es el fin último de toda gestión en las organizaciones.

Colombia se ha destacado a nivel latinoamericano por sus recientes esfuerzos en incrementar y mantener sus capacidades de Ciberseguridad y Ciberdefensa desde las políticas nacionales, primero desde el CONPES 3701 y luego desde el CONPES 3854, en el CONPES 3701, se aborda una estrategia para afrontar las diferentes amenazas, a las que se encuentran significativamente expuestas las entidades del país, mediante la inclusión del tema “Ciberdefensa y ciberseguridad” en el Plan Nacional de Desarrollo, que busca fortalecer las capacidades del Estado y mitigar el impacto de dichos ataques [15]. Se debe seguir creciendo y mejorar en medidas legales, técnicas, organizacionales, generación de capacidades y cooperación con el fin de alcanzar la continuidad y resiliencia en cada uno de los sectores de la sociedad en cuanto a los ataques cibernéticos que puedan presentarse y afectar los sectores productivos críticos del país.

Dada la magnitud y complejidad de esta tarea, es altamente aconsejable recurrir a las guías técnicas, estándares y metodologías ofrecidas por los organismos de normalización y autoridades en materia de ciberseguridad industrial para la implantación de un procedimiento de gestión de incidentes. Disponer de un mecanismo sólido para hacer frente de manera eficaz a una variedad de problemas de los riesgos siempre ha sido algo que las organizaciones se esfuerzan para lograr [64] [65].

Sin embargo, todavía hay preguntas sin respuesta sobre por qué las organizaciones no tienen éxito en la implementación efectiva de seguridad en todos los niveles. En la actual economía digital global, los riesgos de la ciberseguridad se encuentran entre los factores más importantes considerado [66] [67] debido a su impacto, velocidad, sofisticación, y dinámica [68]. Así, la literatura reconoce el papel fundamental de la gestión del ciclo del conocimiento para la organización a pesar del hecho de que hay debates abiertos en curso respecto a lo que es [69].

Es importante reconocer como lo han mencionado diferentes autores que la gestión de la organización, sumada a la gestión del riesgo, la ciberseguridad, la continuidad del negocio, así como la resiliencia son temas que aún se dificulta poderlos integrar, y se siguen manejando como silos [29]. Esto obstaculiza una adecuada gestión de los incidentes de ciberseguridad, incluyendo la respuesta corporativa desarticulada con la respuesta a los incidentes de ciberseguridad y en especial los que se están presentado en las tecnologías de operación (TO) que se han convertido en la prioridad de los atacantes por lo estratégico que son para las empresas, los gobiernos y la economía en el mundo.

Con base en lo anterior a continuación, presentamos un resumen del estado del arte y su relación con el trabajo de investigación desarrollado:

Tabla 2. Resumen del estado del arte y su relación con el trabajo de investigación desarrollado

Tema /Aspecto	Trabajo relacionado	Contribución	Vacíos / Limitantes	Proyecto Propuesta
Gestión de Crisis	[21] Towards Cyber-Security Protection of Critical Infrastructures by Generating Security Policy for SCADA Systems Hacia la seguridad cibernética Protección de las Infraestructuras mediante la generación de políticas de seguridad para Sistemas SCADA.	El trabajo actual relacionado con la gestión de crisis tiende a considerar que los componentes evolucionan y se organizan en sistemas, **pero hasta donde se sabe, no existe una solución sistémica** que integre todos los requisitos anteriores. Por lo tanto, se cree que una solución integrada de ese tipo podría aportar muchas ventajas, incluida la integración de la protección de la seguridad cibernética mediante la generación de políticas de seguridad.	Determina la problemática de la **falta de integración** en la respuesta a los incidentes de seguridad y la gestión de crisis, **pero desde lo técnico** a nivel de equipos como el SCADA, **pero no a nivel de procesos**, procedimientos, esquema de atención, roles, responsabilidades y protocolos que estén **articulados con la respuesta corporativa**.	Aborda el problema desde la Gestión de Incidentes para su **escalamiento**

Tema /Aspecto	Trabajo relacionado	Contribución	Vacíos / Limitantes	Proyecto Propuesta
Consciencia Situacional de la empresa y su impacto en la gestión de riesgos y la seguridad	[64] Towards an Intelligence-Driven Information Security Risk Management Process for Organizations Hacia un proceso de gestión de riesgos para la seguridad de la información basado en la inteligencia para las organizaciones.	En esta investigación se utiliza la teoría de la conciencia de la situación de Endsley y se **examina cómo la estructura y las funciones de la empresa desarrolla la conciencia** de la situación de la empresa en materia de seguridad y gestión de riesgos y cómo las facetas de la empresa estadounidense podrían adaptarse para mejorar la conciencia de la situación en el proceso de gestión de los riesgos para la seguridad de la información en las organizaciones.	**Aborda la organización en sus diferentes niveles de gestión** y decisión para generar un nivel de concienciación que ayude al control del riesgo con foco en TI, **pero no toca la Gestión de Incidentes, ni como la organización participa en la respuesta y recuperación en paralelo.**	**Articulación en la organización**

Tema /Aspecto	Trabajo relacionado	Contribución	Vacíos / Limitantes	Proyecto Propuesta
Homologación de la Terminología en la Gestión de Riesgos en Ciberseguridad en la Organización	[69]. Shifting from Information Security towards a Cybersecurity Paradigm. Pasando de la seguridad de la información a un paradigma de seguridad cibernética.	Este documento sostiene que el uso de un sistema unificado en la terminología fomenta el valor y mejora la supervisión de riesgos (contramedidas y salvaguardias). Por lo tanto, como en respuesta a la confusión resultante, este documento explora la terminología y los significados intercambiables, y analiza la naturaleza del legado teórico, así como los efectos perjudiciales en los factores organizativos internos y externos. Lo hace con el propósito de identificar y aclarar las causas y los efectos de la confusión.	Aporta a la unificación de la terminología de Gestión de Riesgos en Ciberseguridad en la Organización, **pero no profundiza en la implementación en la Gestión de Incidentes ni en la respuesta de nivel corporativo**, pero si facilita los términos a utilizar en los diferentes niveles de gestión.	**Este documento contribuirá a aclarar el alcance de ciberseguridad, Terminología, homologación y entendimiento en la Organización.**

Tema /Aspecto	Trabajo relacionado	Contribución	Vacíos / Limitantes	Proyecto Propuesta
Concienciación, capacitación y entrenamiento en Gestión de Incidentes de Ciberseguridad	**Autores:** Hidekazu Hirai, Yuma Takayama, Tomomi Aoyama, Yoshihiro Hashimoto Ichiro Koshijima [70]. Development of the Cyber Exercise for Critical Infrastructures Focusing on Inter-Organization Communication Desarrollo del Ejercicio Cibernético para Infraestructuras Críticas Centrado en la Comunicación entre Organizaciones.	Debido a que los incidentes cibernéticos en los SCI no sólo causan problemas a la ciberseguridad, sino también problemas a la seguridad de la planta y el negocio de la empresa, la respuesta de toda la empresa, incluyendo no sólo el departamento de TI, sino también el departamento de SCI y **la capa de gestión es esencial**. Para promover sin problemas esta **respuesta de toda la compañía.** Sin embargo, muchas compañías que tienen Equipo de Incidentes no educan adecuadamente a los Comandantes de Incidentes. Por lo tanto, en esta investigación, se	**Trabaja en la capacitación** del equipo de gestión de incidentes para mejorar su desempeño ante la ocurrencia de un ciberataque, **pero no trabaja en la articulación** de una respuesta a nivel corporativo como tampoco en el fortalecimiento del procedimiento existente.	**Fase de entrenamiento del equipo de respuesta.**

Tema /Aspecto	Trabajo relacionado	Contribución	Vacíos / Limitantes	Proyecto Propuesta
		desarrolló un ejercicio cibernético dirigido a educar a los Comandantes de Incidentes.		
Gestión de Riesgos de Ciberseguridad en la organización y sus enfoques de nivel estratégico y táctico para su implementación	[29] **Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment** La resiliencia bajo la previsión estratégica: Los efectos de la gestión de la ciberseguridad y la alineación de la gestión del riesgo empresarial	En la búsqueda de la eficacia y la resiliencia, este documento examina los antecedentes de la gestión de la ciberseguridad para explorar cómo los controles de riesgo en silos influyen en la eficacia de la empresa. Al mismo tiempo, **explora las fortalezas adicionales en la mejora de la gestión del riesgo mediante la alineación con la gestión de riesgos empresariales (ERM) para garantizar que el manejo del riesgo es proactivo, estratégico y gestionado.**	Trabaja mucho en el ámbito de TI pero no aborda los temas de TO ni **mucho menos en la gestión integral del riesgo en ciberseguridad a nivel empresarial.**	**La Gestión de Incidentes a Nivel Empresarial (Estratégico), Corporativo (Táctico) y de Negocio – Proceso (Operativo).**

Tema /Aspecto	Trabajo relacionado	Contribución	Vacíos / Limitantes	Proyecto Propuesta
La gestion de los riesgos corporativos y su relación con los riesgos de ciberseguridad y los vacíos en las estrategias para su intervención	Autor: Jeimy Cano. [51] **Superando los silos en la gestión de riesgos corporativos. Breves anotaciones para el riesgo cibernético.**	El ejercicio de lectura segmentada de los riesgos empresariales afecta la manera como se establecen las estrategias para sus tratamientos. En este sentido, la comprensión de los riesgos cibernéticos, generalmente se asocia con los riesgos de tecnología de información, con lo cual la ciberseguridad termina adscrita como un tema operativo Asumir esta posición, es ignorar la vista sistémica e integrada que tienen los ciber riesgos, creando puntos ciegos en las iniciativas corporativas.	Trabaja muy bien el amarre desde lo estratégico con los riesgos de ciberseguridad y los riesgos corporativos, pero no hace énfasis a nivel de las Tecnologías de Operación presentes en las infraestructuras criticas	**Aporta en la visión sistémica de los ciber riesgos con los riesgos corporativos y se debe complementar desde el trabajo de investigación el foco en las TO y como se asocian las infraestructuras criticas**

Fuente: Elaboración Propia

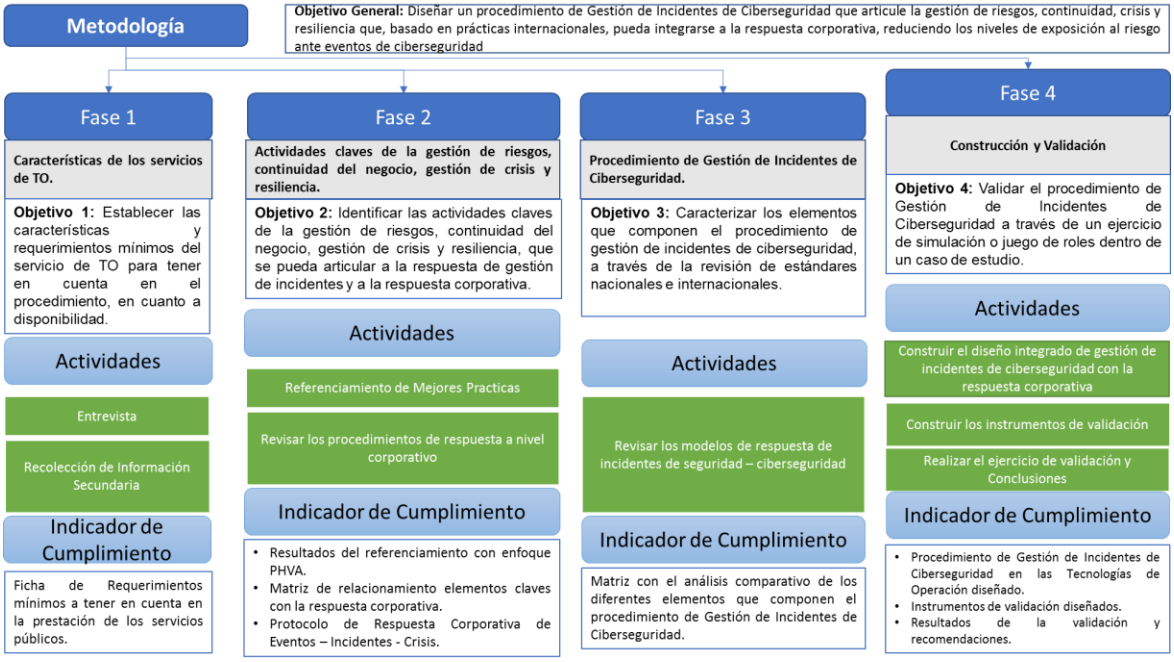
En conclusión, lo que se resalta en el anterior cuadro resumen del estado del arte, es la evidencia del problema planteado en este trabajo de investigación en cuanto a la falta de integración en la respuesta a los incidentes de ciberseguridad con la respuesta corporativa. Aspectos como; el trabajo por silos en la gestión de riesgos, continuidad, crisis y resiliencia, el mayor énfasis en la respuesta técnica del incidente a nivel de equipos como el SCADA, las redes de comunicaciones, los servidores, entre otros, dejando de lado los procesos, procedimientos, esquema de atención, roles, responsabilidades y protocolos que estén articulados con la respuesta corporativa.

También se puede evidenciar que existe un mayor nivel de madurez en la respuesta a los incidentes de ciberseguridad en el mundo de las tecnologías de información, lo que no ocurre con las tecnologías de la operación, lo que refuerza esa visión separada de estos dos mundos al momento de atender un incidente que afecta el servicio donde para su operación se requiere de ambas tecnologías. Otro aspecto que se puede observar, en el estado del arte es que no existe una solución sistémica que considere la gestión de riesgo, continuidad, crisis y resiliencia en la gestión de los incidentes de seguridad articulado con la respuesta corporativa. Por lo anterior y como una solución integrada, es que este trabajo de investigación plantea el diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa con un enfoque basado en el ciclo PHVA teniendo en cuenta el antes, el durante y el después del incidente, donde la respuesta pasa hacer parte de la gestión integral del incidente.

2. Metodología

En consideración del objetivo general y los 4 objetivos específicos, el desarrollo del proyecto de grado se basó en 4 fases (Figura 2-1), en donde cada fase corresponde a un objetivo específico.

Figura 2-1. Fases desarrolladas en la metodología



Fuente: Elaboración propia.

A continuación de describen cada una de las fases desarrolladas para dar cumplimiento a los objetivos.

2.1 Fase 1: Características de los servicios de TO

En esta fase se identificaron las características y requerimientos mínimos del servicio de energía a considerar y que se puedan ver afectados ante un evento de seguridad que afecte la disponibilidad.

Objetivo específico 1: Establecer las características y requerimientos mínimos del servicio de TO para tener en cuenta en el procedimiento, en cuanto a disponibilidad. Para llevar a cabo esta fase se realizaron las siguientes actividades:

2.1.1 Actividad 1. Entrevista

Se realizaron 14 entrevistas con personal experto de los servicios a cubrir, dichas personas hacen parte de las áreas de generación, transmisión y distribución de energía. Para facilitar las entrevistas, se desarrolló un guion que orientó a las personas consultadas para dar las respuestas sobre las diferentes situaciones de ciberseguridad, continuidad, gestión de crisis, procesos y manejo de incidentes de seguridad.

Dicho guion tiene 15 preguntas, en general semi abiertas, lo que permitió obtener comentarios en relación con la repuesta inicial cerrada (Si-No – Parcialmente – No Responde), dicho formato se encuentra en el Anexo 1: Formato Entrevista.

A continuación, se entrega la lista de preguntas realizadas.

- **Bloque de preguntas – Características técnicas:**

    a. ¿Conoce cuáles son las características técnicas que se requieren para la correcta prestación del servicio de distribución de energía?
    SI ___ NO___ Parcialmente _____
    Diga Cuales son, explique:

b. ¿Si su respuesta fue afirmativa o parcialmente, puede determinar cuáles son las mínimas requeridas para poder continuar la prestación del servicio en caso de presentarse un incidente de seguridad que lo afecte?

   Diga Cuales son, explique:

- **Bloque de Preguntas - Características funcionales:**

c. ¿Conoce cuáles son las características funcionales a nivel de los Ciberactivos de las Tecnologías de Operación, que se requieren para la correcta prestación del servicio de distribución de energía?
   SI ___ NO___ Parcialmente _____
   Diga Cuales son, explique:

d. ¿Si su respuesta fue afirmativa o parcialmente, puede determinar cuáles son las mínimas requeridas para poder continuar la prestación del servicio en caso de presentarse un incidente de seguridad que lo afecte?
   Diga Cuales son, explique:

- **Bloque de Preguntas - Características de seguridad Operacional:**

e. ¿Conoce cuáles son las características y requerimientos de seguridad Operacional a nivel del activo (Subestación de Energía) que se requieren para la correcta prestación del servicio de distribución de energía?
   SI ___ NO___ Parcialmente _____
   Diga Cuales son, explique:

f. ¿Si su respuesta fue afirmativa o parcialmente, puede determinar cuáles son las características y requerimientos de seguridad Operacional a nivel del activo (Subestación de Energía) mínimas requeridas para poder continuar la prestación del servicio en caso de presentarse un incidente de seguridad que lo afecte?

Diga Cuales son, explique:

- **<u>Bloque de preguntas – Requerimientos externos (legales, normativos y regulatorios):</u>**

g. ¿Conoce cuáles son los requerimientos legales, normativos y regulatorios que se deben cumplir en la prestación del servicio de distribución de energía?
SI ___ NO___ Parcialmente _____
Diga Cuales son, explique:

h. ¿Si su respuesta fue afirmativa o parcialmente, puede determinar cuáles son los mínimos requeridos que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un incidente de seguridad que lo afecte?
Diga Cuales son, explique:

- **<u>Bloque de preguntas – Requerimientos internos (ANS, proceso, negocio):</u>**

i. ¿Conoce cuáles son los requerimientos mínimos para cumplir por parte de la Unidad Soportes de las Tecnologías de las Operaciones en los acuerdos de niveles de servicio (ANS) con el Negocio/ proceso de Distribución Energía, para mantener (disponibilidad, continuidad, etc.) una correcta prestación del servicio de distribución de energía?
SI ___ NO___ Parcialmente _____
Diga Cuales son, explique:

j. ¿Si su respuesta fue afirmativa o parcialmente, puede determinar cuáles son los mínimos del acuerdo de nivel de servicio (ANS) que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un incidente de seguridad que lo afecte?
Diga Cuales son, explique:

k. ¿Conoce cuáles son los requerimientos de proceso que se deben tener para la correcta prestación del servicio de distribución de energía?

SI ___ NO___ Parcialmente _____

Diga Cuales son, explique:

l. ¿Si su respuesta fue afirmativa o parcialmente, cuáles son los mínimos requerimientos de proceso que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un incidente de seguridad que lo afecte?

Diga Cuales son, explique:

m. ¿Conoce cuáles son los requerimientos del Negocio T&D a nivel de los Activos productivos (Subestaciones, Centros de Control y Telecomunicaciones) y con qué objetivos – metas - índices están relacionados para medir su cumplimiento desde la prestación del servicio de distribución de energía?

SI ___ NO___ Parcialmente _____

Diga Cuales son, explique:

n. ¿Si su respuesta fue afirmativa o parcialmente, de los anteriores, cuáles son los mínimos requerimientos de Negocio T&D a nivel de los Activos productivos (Subestaciones, Centros de Control y Telecomunicaciones) que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un Incidente de seguridad que lo afecte y reducir al máximo los impacto?

Diga Cuales son, explique:

o. l. ¿De las características y requerimientos mínimos identificados y según su conocimiento cuál sería el orden de prioridad que debe tener en cuenta un equipo de gestión de incidentes al momento de atender un evento o falla en caso de presentarse y que afecte la prestación del servicio de distribución de energía?

Listarlos en orden de importancia.

Los resultados obtenidos en esta primera actividad permitieron conocer desde la organización y el sector, cuáles eran esos requerimientos mínimos a tener en cuenta para el servicio, incluso ante

una posible interrupción o degradación del mismo. Para esto se utilizarán el Anexo 2: Consolidado de las Encuestas Def Req Servicio SD Energía).

2.1.2 Actividad 2. Recolección de Información Secundaria

En esta actividad se buscó recoger información relevante con relación a las fuentes secundarias consultadas de acuerdo con los requerimientos, especificaciones y variables críticas identificadas en las entrevistas con los expertos conocedores del servicio, proceso, negocio y sector.

De esta manera se logró establecer las características y requerimientos mínimos del servicio de TO para tener en cuenta en el procedimiento de gestión de incidentes, en cuanto a disponibilidad, insumo importante para lograr el objetivo específico 1.

Esta información se obtuvo de las siguientes fuentes que fueron consultadas a través de internet en los sitios oficiales:

- Constitución Política de Colombia de 1991 - Tratados Internacionales
- Ley 142 de 1994, es la Ley de Servicios Públicos Domiciliarios en Colombia
- Ley 143 de 1994 Por la cual se establece el régimen para la generación, interconexión,
- Ley 1581 de 2012 Protección de Datos Personales
- Ley 1712 de 2014 de Transparencia y de Acceso a la Información
- CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL (CONPES) organismo asesor del gobierno colombiano en lo que respecta al desarrollo económico y social del país (3701, 3854, 3995)
- Comisión de Regulación de Energía y Gas -CREG (097, 070, 015, 025, 080, 038)
- Consejo Nacional de Operación del Sector Eléctrico (CNO) (788, 1241, 1043, 1347)
- Ministerio de Defensa - Comando Conjunto Cibernético (CCOC)(Plan Nacional de Protección y Defensa de Infraestructura Critica Cibernética, plan sectorial, Plan de Protección Específico de Infraestructura Crítica Cibernética, Plan Sectorial de Protección y Defensa para el Sector Electricidad de Colombia PSPSE V1.0,).

Esta información secundaria fue consolidada a través de la siguiente Tabla 2-1, validando cómo dichas fuentes les aportaba a los requerimientos mínimos del Servicio Distribución Energía Eléctrica en Colombia y su énfasis en cuanto a la disponibilidad.

Tabla 2-1. Recolección información de fuentes secundarias.

Características y Requerimientos mínimos del servicio de TO en cuanto a disponibilidad					
Fuente secundaria	Requerimiento 1	Requerimiento 2	Requerimiento 3	Requerimiento 4	Requerimiento n
Fuente 1					
Fuente 2					
Fuente 3					
Fuente n					

Fuente: Elaboración Propia.

En cada fuente secundaria analizada se seleccionaron los elementos que tenían relación con los requerimientos del servicio de distribución de energía eléctrica, con el fin de identificar desde las fuentes secundarias consultadas su relación con las características y requerimientos mínimos para tener en cuenta para el servicio con foco en la disponibilidad. En el capítulo de resultados podrán encontrar el Anexo 3: Consolidado Inf Ftes Sec Req Servicio SD E

2.2 Fase 2: Actividades claves de la gestión de riesgos, continuidad del negocio, gestión de crisis y resiliencia

Objetivo específico 2: Identificar las actividades claves de la gestión de riesgos, continuidad del negocio, gestión de crisis y resiliencia, que se pueda articular a la respuesta de gestión de incidentes y a la respuesta corporativa.

En esta fase se identificaron los elementos claves a tener en cuenta desde un marco de referenciamiento de las mejores prácticas a nivel nacional e internacional en la gestión de riesgos,

gestión de continuidad, gestión de crisis y gestión de la resiliencia, y se definió la manera de articular dichos elementos con las actividades de alto nivel que se llevan a cabo para realizar la respuesta corporativa para ello se llevaron a cabo las siguientes actividades:

2.2.1 Actividad 1. Referenciamiento de mejores prácticas

Se hizo una exploración de diferentes fuentes de información (Internet, Páginas Web Oficiales, Normas de Referencia, Guías y documentos técnicos) con el fin de encontrar los elementos claves de las siguientes prácticas de gestión:

- Gestión de Riesgos – ISO 31000 – ISO 27005 – IEC 62443 – MAGERIT – Pilar.
- Gestión de Continuidad – ISO 22301 – ISO 27031 – ISO 22317
- Gestión de Crisis – BS 11200 - ISO 22320
- Gestión de Resiliencia – ISO 22316 – BS 65000

En la revisión de cada una de las normas se buscaron los siguientes parámetros:

- Revisar la articulación de los elementos claves de las normas consultadas desde el ciclo de la gestión sistémica utilizando la planeación, la ejecución, la verificación y el ajustar (PHVA).
- Articulación desde un enfoque sistémico propio de los sistemas de gestión y la estructura de alto nivel
- Reconocimiento desde su origen en el antes – durante - después de la ocurrencia de un evento o incidente con foco en la gestión.
- Tomar como base del análisis y del fortalecimiento las actividades definidas por el marco de NIST en sus diferentes funciones.

El objetivo final de esta actividad es la de seleccionar las normas que puedan estar más alineadas con el proyecto, por lo cual, luego del análisis de cada una de ellas, se seleccionara la norma o buena práctica a seguir.

Esta información fue consolidada a través de la siguiente Tabla 2-2, validando cómo dicha fuente le puede aportar a un manejo de incidentes de seguridad.

Tabla 2-2. Recolección Elementos Claves

Ciclo de Gestión - PHVA	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
P	Contexto Liderazgo Planificación				
H	Soporte Operación				
V	Evaluación Desempeño				
A	Mejora				

Fuente: Elaboración Propia.

2.2.2 Actividad 2. Revisar los procedimientos de respuesta a nivel corporativo

Para la realización de esta actividad, se buscaron fuentes secundarias en internet (referenciación del mercado, encontrando 9 casos) con el propósito de obtener los tipos de respuesta a nivel corporativo ante la ocurrencia de un incidente de seguridad que implicaran la atención de emergencias, crisis, continuidad y resiliencia.

Para obtener los resultados, se construyó la siguiente matriz (Tabla 2-3) teniendo en cuenta los resultados de la actividad anterior, marco de referenciamiento de las mejores prácticas a nivel nacional e internacional en la gestión de riesgos, gestión de continuidad, gestión de crisis y gestión

de la resiliencia, y su articulación con las actividades de alto nivel que se llevan a cabo para realizar la respuesta corporativa articulados con el procedimiento de gestión de incidentes.

Tabla 2-3. Matriz de relacionamiento elementos claves con la respuesta corporativa.

Ciclo de Gestión - PHVA	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia	Caso 1	Caso 2	Caso 3	Caso 4	Caso 5	Caso 6	Caso 7	Caso 8	Caso 9
P	Contexto Liderazgo Planificación													
H	Soporte Operación													
V	Evaluación Desempeño													
A	Mejora													

Fuente: Elaboración Propia.

Con estos resultados y para facilitar la articulación de la respuesta corporativa durante la ocurrencia de eventos, incidentes y crisis que se pudieran generar en una organización, se diseña un protocolo de respuesta corporativa teniendo en cuenta la gradualidad de los efectos y consecuencias, el uso de recursos, con la definición de roles y un nivel de escalamiento hasta involucrar los niveles corporativos y del equipo de crisis gerencial, con la respuesta del equipo de gestión de incidentes.

2.3 Fase 3: Procedimiento de Gestión de Incidentes de Ciberseguridad

En esta fase se establecieron las actividades para tener en cuenta dentro del procedimiento de gestión de incidentes, considerando las buenas prácticas existentes a nivel de modelos de gestión de respuesta en TI y TO, como resultados, se define un procedimiento para la gestión de los diferentes incidentes y que pueda ser integrado a la respuesta corporativa.

Objetivo específico 3: Caracterizar los elementos que componen el procedimiento de gestión de incidentes de ciberseguridad, a través de la revisión de estándares nacionales y/o internacionales.

Para el logro de este objetivo se llevaron a cabo las siguientes actividades.

2.3.1 Actividad 1. Revisar los modelos de respuesta de incidentes de seguridad – ciberseguridad

Se hizo un referenciamiento a nivel nacional e internacional de los modelos, estándares y buenas prácticas en gestión de incidentes de ciberseguridad a nivel de TI y TO, con el fin de poder caracterizar las principales etapas a tener en cuenta en la respuesta a incidentes y de esta manera, realizar la articulación de los requerimientos mínimos del servicio con los elementos a potenciar desde el marco de referencia de gestión de riesgos, continuidad, crisis y resiliencia con la respuesta de nivel corporativo ante eventos tecnológicos.

Después de consultar las fuentes secundarias y analizar la información relacionada con el tema objeto de la investigación, se seleccionaron los siguientes referentes internacionales que dan una visión general y son los que le pueden aportar a este proyecto de investigación, brindando los insumos para diseñar el nuevo procedimiento integrado de gestión de incidentes de ciberseguridad alineado con la respuesta corporativa.

Las fuentes consultadas a través del internet y las páginas web oficiales fueron:

- NIST Cybersecurity Framework: Marco para la mejora de la seguridad cibernética en infraestructuras críticas Versión 1.1, publicado 16/04/2018.
- Estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide, Agosto 2012
- MINTIC: Guía para la Gestión y clasificación de Incidentes de Seguridad de la Información, 6/11/2016.
- INCIBE: Guía Nacional de Notificación y Gestión de Ciber incidentes, publicado el 21/02/2020
- ISO/IEC 27035 – 1 y 2: Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad – parte 1, principios y parte 2, directrices para planificar y prepararse para la respuesta a incidentes, 11/01/2016.

Los hallazgos que se obtuvieron del análisis de las fuentes consultadas se consolidaron en la siguiente Matriz (Tabla 2-4) de análisis comparativo de los referentes de Gestión de Incidentes de Ciberseguridad.

Tabla 2-4. Matriz Análisis comparativo de los diferentes elementos que componen el procedimiento de Gestión de Incidentes de Ciberseguridad.

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	Norma o buena práctica 1		Norma o buena práctica 2		Norma o buena práctica n	
PHVA	Fase	Actividades	Fase	Actividades	Fase	Actividades
P						
H						
V						
A						

Fuente: Elaboración Propia.

2.4 Fase 4: Construcción y Validación

En esta fase se realizó el diseño y la validación del procedimiento de gestión de incidentes de ciberseguridad en una organización donde se observe la articulación con la respuesta corporativa y la mejora efectiva de la gestión de incidentes integrando la gestión de riesgos, continuidad, crisis y resiliencia.

Objetivo específico 4: Validar el procedimiento de Gestión de Incidentes de Ciberseguridad a través de un ejercicio de simulación o juego de roles dentro de un caso de estudio.

Para el logro de este objetivo se llevaron a cabo las siguientes actividades.

2.4.1 Actividad 1. Construir el diseño integrado de gestión de incidentes de ciberseguridad y respuesta corporativa

Para llevar a cabo esta actividad se tuvieron en cuenta todos los resultados de las actividades anteriores; es decir:

- Ficha de Requerimientos mínimos para tener en cuenta en la prestación de los servicios públicos.
- Resultados del referenciamiento con enfoque PHVA de los elementos claves de riesgos, continuidad, crisis y resiliencia que podrían mejorar la gestión de incidentes.
- Matriz de relacionamiento de elementos claves de la respuesta corporativa con la gestión de incidentes.
- Protocolo de Respuesta Corporativa de Eventos – Incidentes - Crisis.
- Matriz con el análisis comparativo de los diferentes elementos que componen el procedimiento de Gestión de Incidentes de Ciberseguridad.

Los resultados y análisis se llevaron a la siguiente matriz (Figura 2-2), con el fin de poder dimensionar el aporte que estos elementos realizaban a cada una de las actividades del Framework de referencia de gestión de incidentes.

Figura 2-2. Formato para el diseño integrado de gestión de incidentes de ciberseguridad

Formato para el diseño integrado de gestión de incidentes de ciberseguridad

Ciclo de Gestión - PHVA	Marco de Referencia Planeación de la Gestión de Incidentes	Estructura de Alto Nivel ISO
P		• Contexto • Liderazgo • Planificación

Ciclo de Gestión - PHVA	Marco de Referencia Planeación de la Gestión de Incidentes	Estructura de Alto Nivel ISO
V		• Evaluación Desempeño

Ciclo de Gestión - PHVA	Marco de Referencia Planeación de la Gestión de Incidentes	Estructura de Alto Nivel ISO
H		• Operación • Soporte

Ciclo de Gestión - PHVA	Marco de Referencia Planeación de la Gestión de Incidentes	Estructura de Alto Nivel ISO
A		• Mejora

Fuente: Elaboración Propia

Ya con estos resultados integrados, se procedió con la documentación de la propuesta del nuevo Procedimiento de Gestión de Incidentes de Ciberseguridad, teniendo en cuenta tanto la articulación que debe existir con el protocolo de respuesta corporativa como de los requerimientos mínimos del servicio en un marco del ciclo PHVA.

En consecuencia, el resultado de esta actividad es el **Procedimiento de Gestión de Incidentes de Ciberseguridad** articulado con los demás procesos y en ese sentido, se espera la validación (siguiente actividad), ante u evento de seguridad que afecte la disponibilidad, se tendría u procedimiento de atención a dicho incidente.

2.4.2 Actividad 2. Construir los instrumentos de validación

Para esta actividad fue necesario consultar en qué consistían los ejercicios de simulación, y para esta investigación se tomaron los siguientes referentes:

- BQA consultorías. Firma que ha venido trabajando en el Sector Eléctrico colombiano y en el sector de la Aviación como referente en la Seguridad Operacional
- CD&A Consultores de Riesgos & Continuidad SAS. Firma Consultora en Gestión de Riesgos, Crisis y Continuidad del Negocio, viene trabajando por muchos años en temas relacionados con la gestión de emergencias, continuidad, crisis y resiliencia.
- Ejercicios de Simulación Csirt EPM.

A continuación, se presenta la Tabla 2-5 que se construyó para identificar los elementos claves de los referentes utilizados y en el consolidado identificar la fuente que servirá de base para la construcción de la Guía para realizar la simulación.

Tabla 2-5. Matriz de relaciones de los Referentes para los Ejercicios de Simulación y Simulacros

		Referentes Ejercicios de Simulación y Simulacros			
	Elementos a tener en cuenta para una Simulación	**Consolidado**	**BQA**	**CD & A**	**Csirt Sector Eléctrico**
1	Introducción				
2	Justificación				
3	Alcance				
4	Objetivos				
5	Enfoque				
6	Tipo de ejercicio				
7	Pre - requisitos				
8	Supuestos				
9	Identificar elemento crítico a evaluar				
10	Definición de participantes y roles para el ejercicio.				
11	Facilitador				
12	Observador				
13	Evaluador				
14	Jugadores				
15	Guion (Trama)				
16	Escenario				
17	Línea de Tiempo				
18	Eventos Principales (Hitos)				
19	Mapa del Ejercicio				
20	Análisis de Riesgos y plan de controles				
21	Listas de Verificación				
22	Ficha del Ejercicio				
23	Ejecución de la Simulación				
24	Evaluación de la Simulación				

		Referentes Ejercicios de Simulación y Simulacros			
	Elementos a tener en cuenta para una Simulación	**Consolidado**	**BQA**	**CD & A**	**Csirt Sector Eléctrico**
25	Lecciones aprendidas - Incorporación de mejoras y ajustes				

Fuente: Elaboración Propia

Con este ejercicio se pudo definir para el trabajo de investigación cómo diseñar una Guía para llevar a cabo el Ejercicio de Simulación de un Caso de Estudio y tomar de cada referente lo que consideramos era relevante para la guía.

Igualmente, dentro de este documento guía, se encuentran varios formatos que servirán para la validación de la aplicación tanto del Protocolo de Respuesta Corporativa como del Procedimiento Gestión de Incidentes de Ciberseguridad.

Igualmente, dentro de este documento guía, se encuentran varios formatos (Tabla 2-6 y Tabla 2-7) que servirán para la validación de la aplicación tanto del Protocolo de Respuesta Corporativa como del Procedimiento Gestión de Incidentes de Ciberseguridad. Para la valoración de la metodología propuesta, se plantea un caso de estudio sobre una empresa ficticia del sector de energía.

Tabla 2-6. Formato de Ejecución de la Simulación #1

Ejecución de la Simulación

Tipo y nombre del ejercicio	**Simulación de respuesta ante un ataque cibernético a la infraestructura tecnológica en la Empresa Destello E.S. P.**
Instituciones involucradas	Operación - Equipo Gestión Incidentes - Equipo Respuesta Corporativo (Comunicaciones, Logística, Legal, Seguros - Equipo Respuesta Crisis (Gerente General, Directivo Transmisión y Distribución)

Lugar	Reunión Teams - Salón social Urbanización Veleros	**Fecha**	22 de junio de 2021	
Responsable	Fredy Humberto Gómez - Héctor Valencia V.	**Hora**	8:00am a 12:00m	
GUION				
Hora	**Evento**	**Acción Para Tomar**	**Duración**	**Responsable**
	ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo	**ACCIONES REALIZADAS en atención del evento**	**OBVSERVACIONES**	
	ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo	**ACCIONES REALIZADAS en atención del evento**	**OBVSERVACIONES**	
	ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo	**ACCIONES REALIZADAS en atención del evento**	**OBVSERVACIONES**	

Fuente: Elaboración Propia

Tabla 2-7. Formato Evaluación del Ejercicio de Simulación

Evaluación de la Simulación

Tipo y nombre del ejercicio	**Simulación de respuesta ante un ataque cibernético a la infraestructura tecnológica en la Empresa Destello E.S. P.**			
Instituciones involucradas	Operación - Equipo Gestión Incidentes - Equipo Respuesta Corporativo (Comunicaciones, Logística, Legal, Seguros - Equipo Respuesta Crisis (Gerente General, Directivo Transmisión y Distribución)			
Lugar	Reunión Teams - Salón social Urbanización Veleros.	**Fecha**	22 de junio de 2021	
Responsable	Fredy Humberto Gómez - Héctor Valencia V.	**Hora**	8:00am a 12:00m	
Evaluación del Ejercicio de Simulación				
Evaluación del Procedimiento Gestión de Incidentes vs Caso de Estudio				
Evaluación del Protocolo de Respuesta Corporativa Vs Caso de Estudio				

Fuente: Elaboración Propia

2.4.3 Actividad 3. Realizar el ejercicio de simulación

Siguiendo un Caso de Estudio en una empresa de referencia donde se utilicen las Tecnologías de Operación y para presentar los resultados, se aplicarán los instrumentos elaborados con el fin de validarlos y recoger las recomendaciones que puedan surgir durante el ejercicio para hacer los ajustes correspondientes.

En ese sentido, se tomó en cuenta la Guía desarrollada en esta investigación a partir de varios referentes de buenas prácticas para llevar a cabo ejercicios de Simulación y Simulacros, con ello, poder ejecutar el ejercicio de valoración de la metodología sobre el caso de estudio definido.

3. Resultados

A continuación, por cada una de las fases indicadas en la metodología, se entregan los diferentes resultados obtenidos.

3.1 Fase 1: Características de los servicios de TO

Objetivo específico 1: Establecer las características y requerimientos mínimos del servicio de TO para tener en cuenta en el procedimiento, en cuanto a disponibilidad.

3.1.1 Actividad 1. Entrevista

Para establecer las característica y requerimientos mínimos en la prestación del servicio de distribución de energía, se diseñó y aplicó el guion de entrevista definido en la metodología (ver Anexo 1: Formato Entrevista) que ayudó como orientación en las preguntas y la recolección de respuestas.

A continuación, se presentan los resultados por cada pregunta y el análisis de acuerdo con las respuestas obtenidas, las respuestas completas se pueden consultar en el Anexo 2: Consolidado de las Encuestas Def Req Servicio SD Energía

Se presenta la ficha técnica utilizada en la entrevista realizada (Tabla 3-1), el cual el 71.4% de los encuestados dio respuestas a las diferentes preguntas.

Tabla 3-1. Ficha Técnica de la Entrevista

Entrevista	
Objetivo:	Determinar cuáles son las características y requerimientos mínimos en la prestación del servicio de distribución de energía que un equipo de respuesta a incidentes debe tener en cuenta al momento de atender un evento de ciberseguridad que pueda afectar la prestación del servicio.
# de Entrevistas Solicitadas	14
# de Entrevistas Realizadas	10
# de Entrevistas No Realizadas	4
Cantidad de preguntas	15
Perfiles consultados	• Jefe de soporte de las Tecnologías de Operación • Consultor Experto en Sistemas de Control Industriales • Arquitecto de TO • Coordinador de Operaciones del Sistema Interconectado Nacional • Profesional experto en Sistemas SCADA • Profesional Experto en Automatización • Profesional Experto en Comunicaciones • Gestor de Operación Integrada Energía • Profesional en Gestión de Información Operación y Calidad • Líder Equipo de Respuesta a Incidentes de Ciberseguridad

Fuente: Elaboración Propia

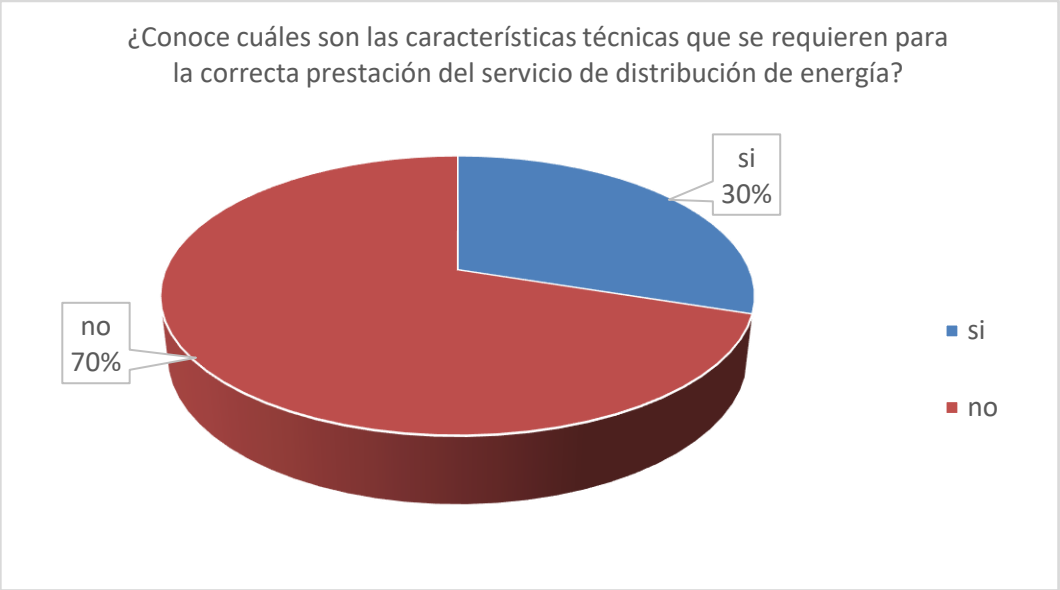
A continuación, por cada bloque de pregunta se entrega el análisis de las encuestas.

- **<u>Bloque de preguntas – Características técnicas:</u>**

  a. ¿Conoce cuáles son las características técnicas que se requieren para la correcta prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
3	7		
30.0	70.0		

Figura 3-1. Tabulación Respuesta pregunta 1



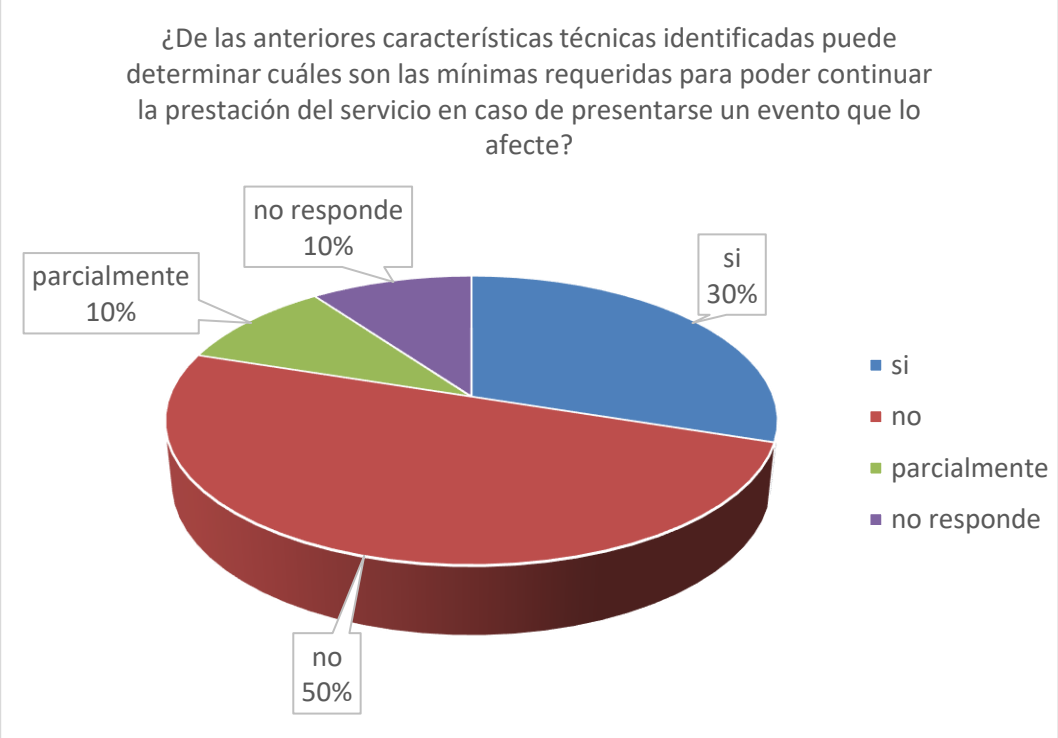
Fuente: Elaboración propia

Se puede apreciar en la Figura 3-1 que el 70% de las personas no conocen las características técnicas sobre el servicio de energía, lo que genera una preocupación al momento de estar al frente de un evento de seguridad (o de otra índole que afecte la disponibilidad). Sin embargo, un 30% si conoce dichos requerimientos, lo que genera una oportunidad para que los demás puedan estar enterados.

b. ¿Si su respuesta fue afirmativa o parcialmente, puede determinar cuáles son las mínimas requeridas para poder continuar la prestación del servicio en caso de presentarse un incidente de seguridad que lo afecte?

Si	No	Parcialmente	No responde
3	5	1	1
30.0	50.0	10.0	10.0

Figura 3-2. Tabulación Respuesta pregunta 2



Fuente: Elaboración propia

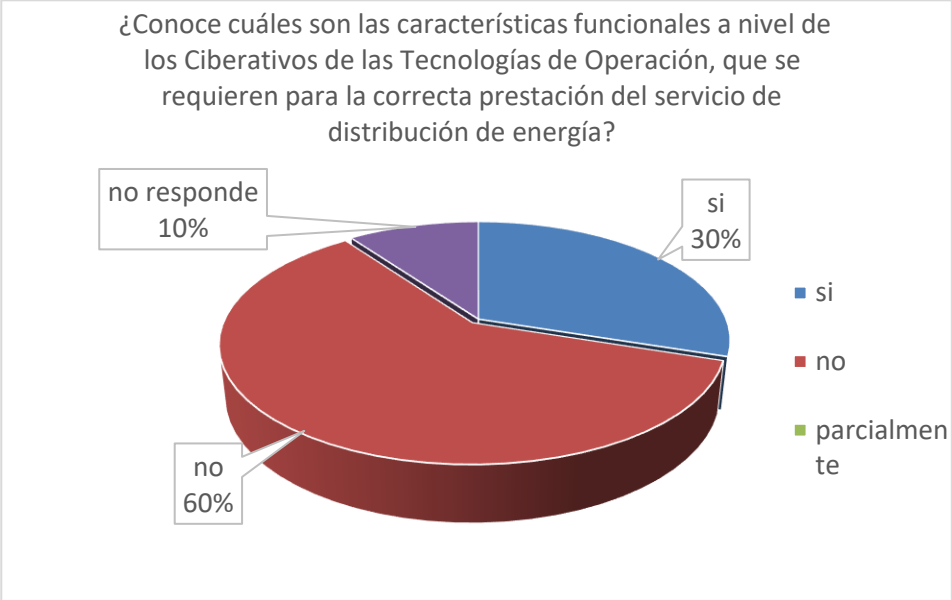
En concordancia con la respuesta anterior, en la Figura 3-2 se observa que el 30% de las personas dieron algunos de los aspectos técnicos para la operación, como los componentes a nivel eléctrico, niveles de tensión, disponibilidad de las plataformas tecnológicas como el SCADA, entre otras.

- **Bloque de preguntas – Características funcionales:**

c. ¿Conoce cuáles son las características funcionales a nivel de los Ciberativos de las Tecnologías de Operación, que se requieren para la correcta prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
3	6		1
30.0	60.0	-	10.0

Figura 3-3. Tabulación Respuesta pregunta 3



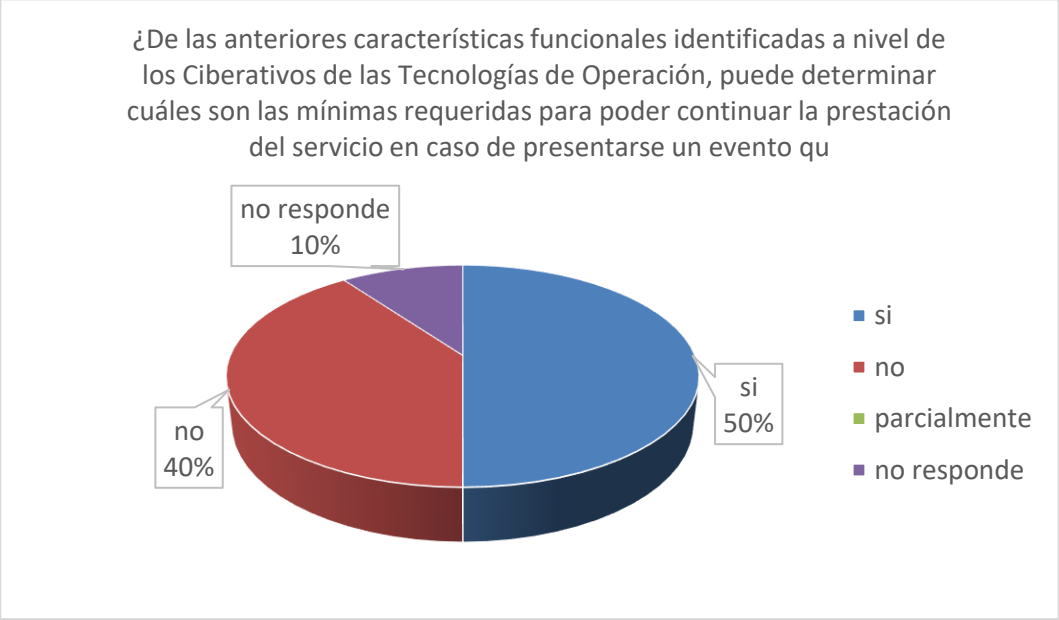
Fuente: Elaboración propia.

Con respecto a la tecnología, en la Figura 3-3, es claro que el 60% lo desconoce, estableciendo así una línea de preocupación con respecto a las personas que operan, mantienen o tienen algún contacto con el servicio, sin embargo, se puede notar que el 30% si conoce algunas de las características, mismo porcentaje que conoce las funciones del servicio. Dentro de los ciber activos identificados están los SCADAS y las telecomunicaciones.

d. ¿De las anteriores características funcionales identificadas a nivel de los Ciber activos de las Tecnologías de Operación, puede determinar cuáles son las mínimas requeridas para poder continuar la prestación del servicio en caso de presentarse un evento que lo afecte?

Si	No	Parcialmente	No responde
5	4		1
50.0	40.0	-	10.0

Figura 3-4. Tabulación Respuesta pregunta 4



Fuente: Elaboración propia.

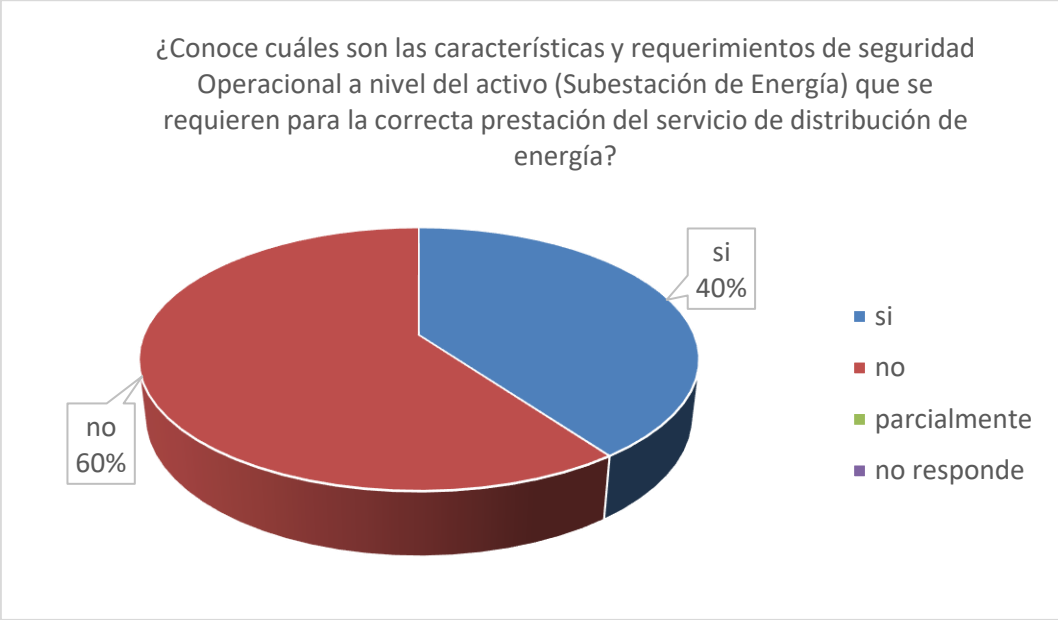
De acuerdo con la Figura 3-4, el 50% puede identificar el papel de cada ciber activo en la operación, mientras que el 40% no. Dentro de las funciones identificadas se encuentran el control que hace los SCADAS, la disponibilidad que debe ser continua, la posibilidad de operación manual ante un evento, entre otras.

- **Bloque de preguntas – Características técnicas:**

e. ¿Conoce cuáles son las características y requerimientos de seguridad Operacional a nivel del activo (Subestación de Energía) que se requieren para la correcta prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
4	6		
40.0	60.0	-	-

Figura 3-5. Tabulación Respuesta pregunta 5



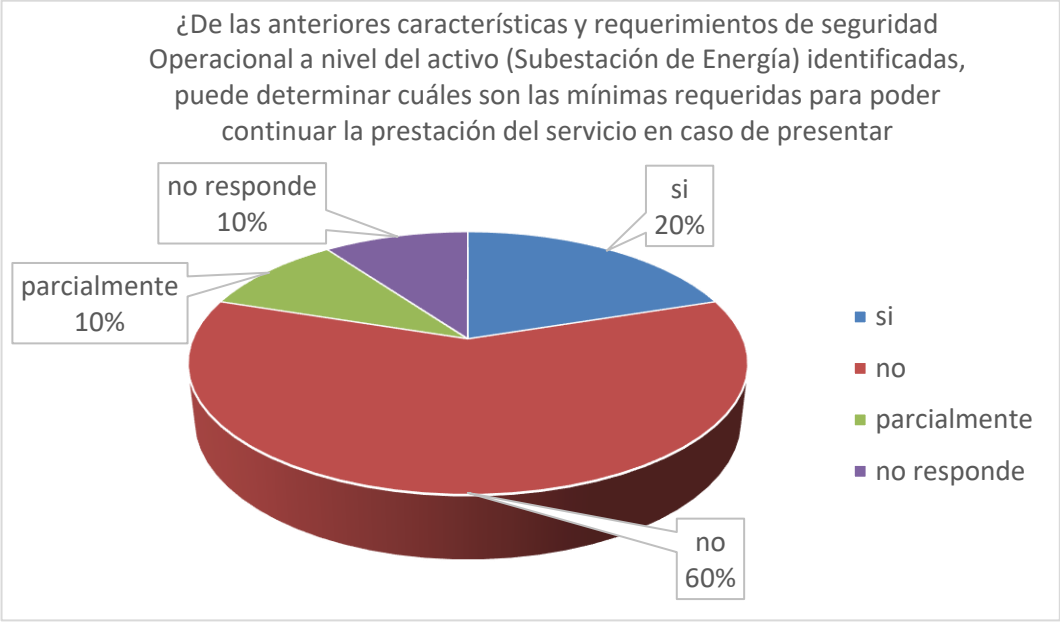
Fuente: Elaboración propia

Con respecto a los requerimientos de seguridad, se genera una alta preocupación y oportunidad, pues el 60% indica no conocerlo, según los resultados de la encuesta en la Figura 3-5. Los que indicaron tener información, establecieron temas con la configuración segura, confiabilidad en los datos, ejecución de procedimientos preventivos y correctivos, entre otros.

f. ¿De las anteriores características y requerimientos de seguridad Operacional a nivel del activo (Subestación de Energía) identificadas, puede determinar cuáles son las mínimas requeridas para poder continuar la prestación del servicio en caso de presentarse un evento que lo afecte?

Si	No	Parcialmente	No responde
2	6	1	1
20.0	60.0	10.0	10.0

Figura 3-6. Tabulación Respuesta pregunta 6



Fuente: Elaboración propia

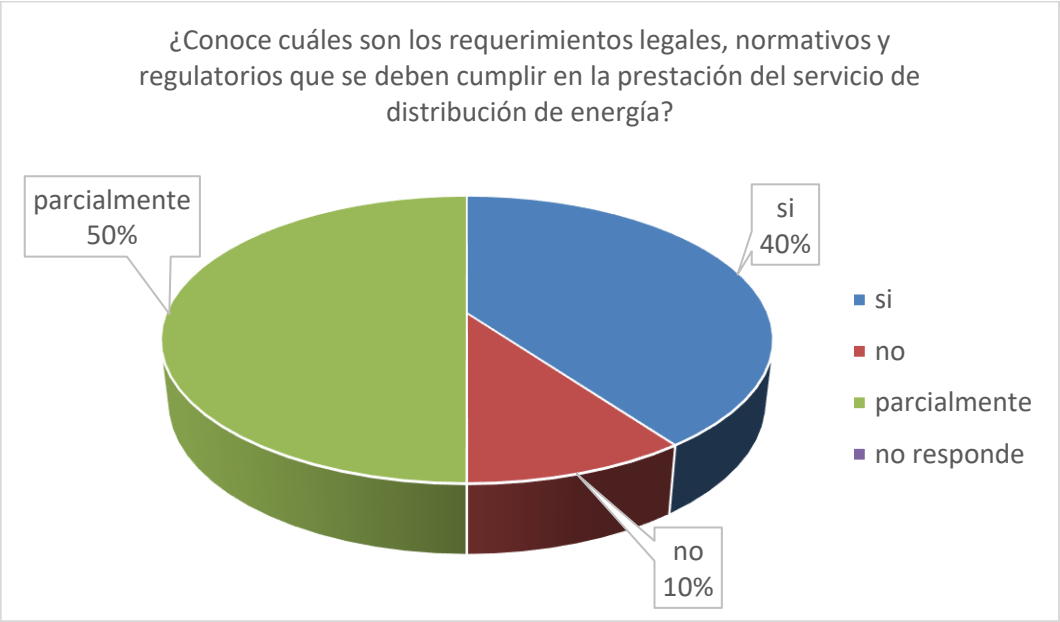
Como se observa en la Figura 3-6 solo el 20 % de las personas consultadas respondieron conocer los requerimientos mínimos desde la Seguridad Operacional con respecto a los planes de restablecimiento, las redundancias asociadas a componentes críticos y el restante 80% respondió no conocerlos o conocerlos parcialmente, esto es preocupante al momento de realizar maniobras en los equipos por los riesgos tanto de seguridad para las personas como para la infraestructura.

- **Bloque de preguntas – Requerimientos externos (legales normativos y regulatorio):**

g. ¿Conoce cuáles son los requerimientos legales, normativos y regulatorios que se deben cumplir en la prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
4	1	5	
40.0	10.0	50.0	-

Figura 3-7. Tabulación Respuesta pregunta 7



Fuente: Elaboración propia

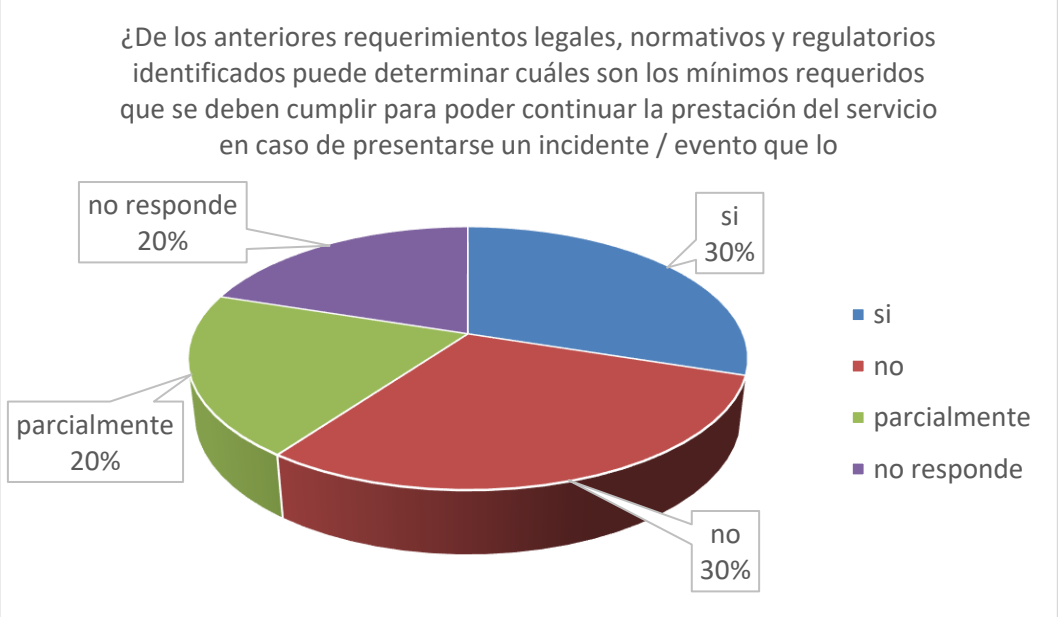
Con respecto al conocimiento de los requerimientos legales, regulatorios y normativos, de acuerdo con las respuestas en la Figura 3-7 es el tema que más se conoce siendo muy conocido por el 40% y parcialmente conocido por el 50% solo un 10% dijo no conocer.

h. ¿De los anteriores requerimientos legales, normativos y regulatorios identificados puede determinar cuáles son los mínimos requeridos que se deben cumplir para poder

continuar la prestación del servicio en caso de presentarse un incidente / evento que lo afecte?

Si	No	Parcialmente	No responde
3	3	2	2
30.0	30.0	20.0	20.0

Figura 3-8. Tabulación Respuesta pregunta 8



Fuente: Elaboración propia

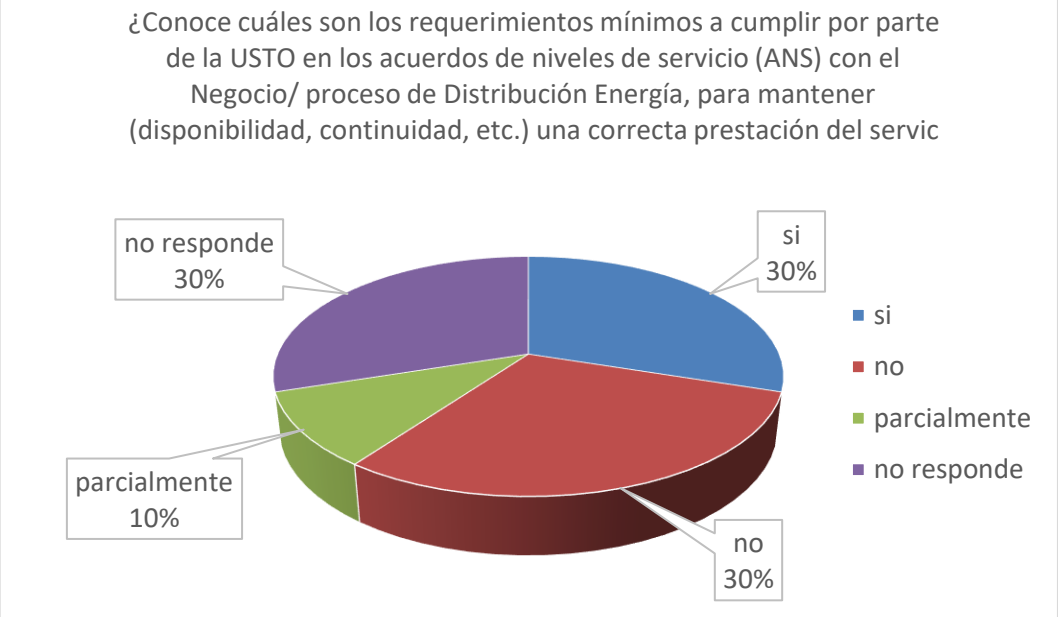
Como se observa en la Figura 3-8, ya en lo que se refiere a los mínimos legales, regulatorios y normativos con relación al restablecimiento ante una interrupción, el conocimiento se reduce a un 50% siendo muy conocido solo por el 20% y parcialmente el 30% y no conoce el 30%. Los elementos mencionados tienen que ver con las garantías de operación al sistema interconectado, la calidad del servicio de energía regulada, los indicadores de calidad y la calidad de la potencia.

- **Bloque de preguntas – Requerimientos internos (ANS, proceso, negocio):**

i. ¿Conoce cuáles son los requerimientos mínimos para cumplir por parte de la USTO en los acuerdos de niveles de servicio (ANS) con el Negocio/ proceso de Distribución Energía, para mantener (disponibilidad, continuidad, etc.) una correcta prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
3	3	1	3
30.0	30.0	10.0	30.0

Figura 3-9. Tabulación Respuesta pregunta 9



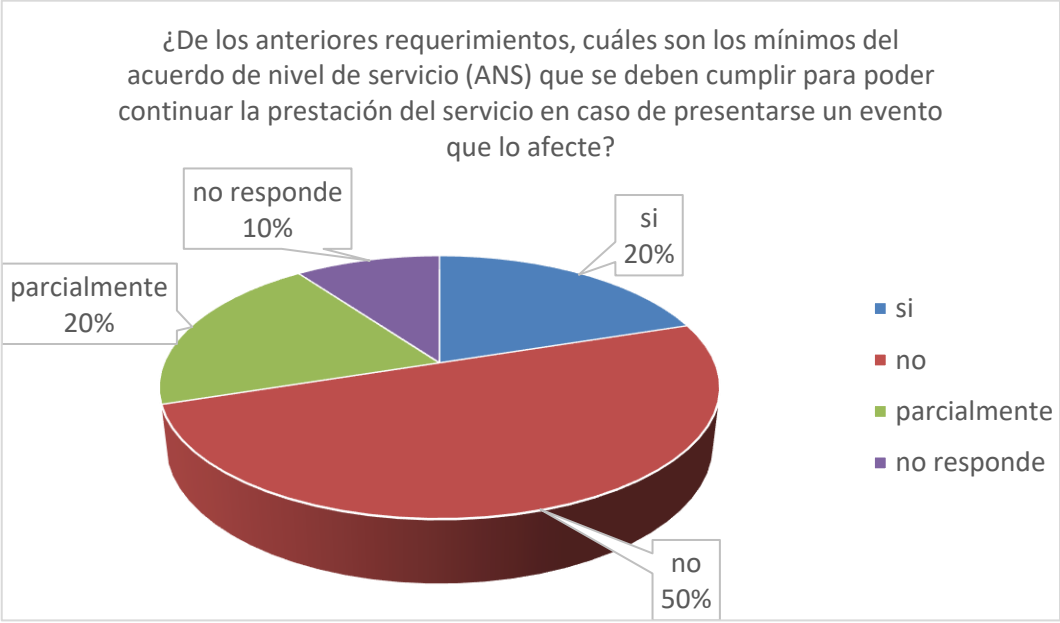
Fuente: Elaboración propia

Según la Figura 3-9, solo el 40% dicen conocer los acuerdos de nivel de servicio con relación en la operación, mantenimiento y soporte de las tecnologías de operaciones 60% restante dicen no conocerlos, esto es delicado al momento de intervenir estas tecnologías porque se puede incurrir en incumplimientos y afectación de los niveles de satisfacción de los interesados.

j. ¿De los anteriores requerimientos, ¿cuáles son los mínimos del acuerdo de nivel de servicio (ANS) que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un evento que lo afecte?

Si	No	Parcialmente	No responde
2	5	2	1
20.0	50.0	20.0	10.0

Figura 3-10. Tabulación Respuesta pregunta 10



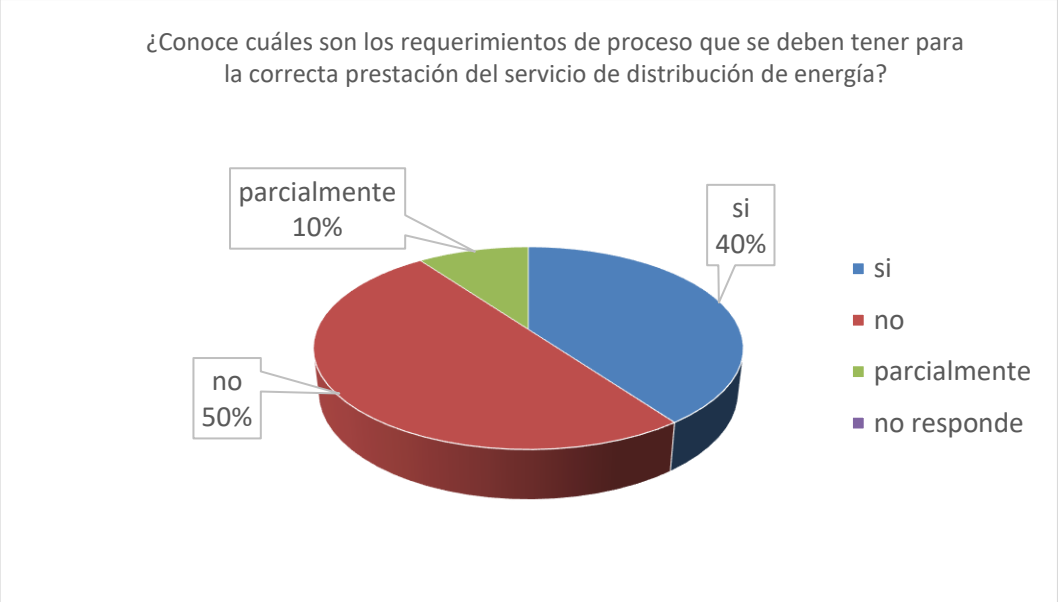
Fuente: Elaboración propia

Como se observa en la Figura 3-10, ya en lo que se refiere a los mínimos requerimientos incluidos en los acuerdos de nivel de servicio a tener en cuenta para el restablecimiento ante una interrupción, el conocimiento se reduce a un 20%, de manera parcial otro 20% y no lo conocen o no responden el 60%. Está claro que un equipo de respuesta debería igualmente conocerlos para actuar de manera coordinada con el equipo de la operación y del soporte de las Tecnologías de Operación.

k. ¿Conoce cuáles son los requerimientos de proceso que se deben tener para la correcta prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
4	5	1	
40.0	50.0	10.0	-

Figura 3-11. Tabulación Respuesta pregunta 11



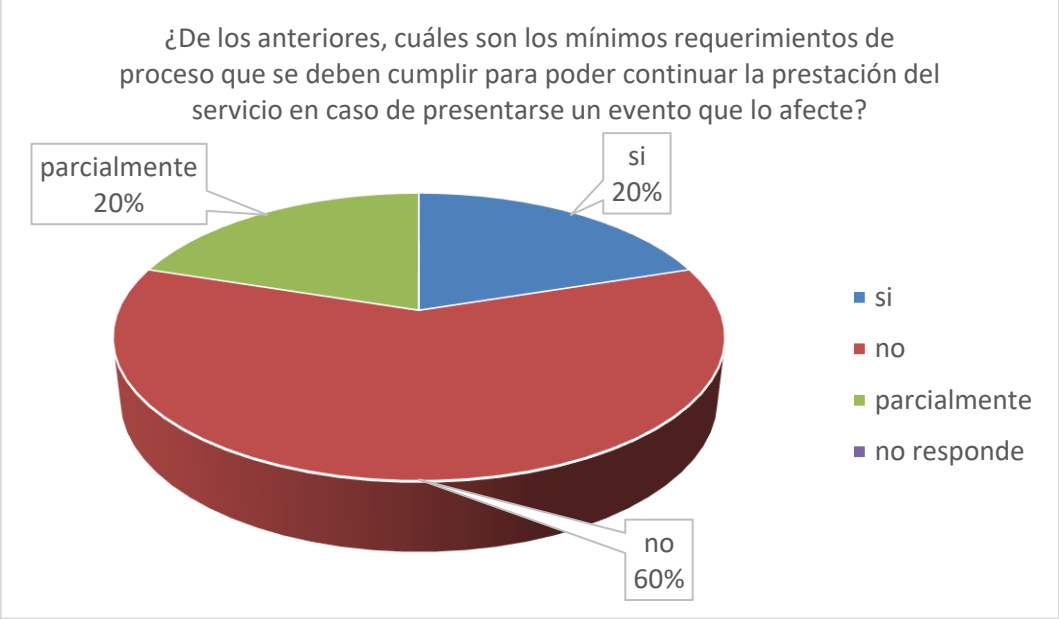
Fuente: Elaboración propia

Según la Figura 3-11, solo el 40% de los encuestados dijeron conocer los requerimientos del proceso para la correcta prestación del servicio en distribución de energía, un 10% dijo conocerlos de manera parcial y el 50% restante respondió no conocerlos. Este es un tema relevante para un equipo de respuesta a incidentes, en la medida que entiende cómo funciona el proceso y cuáles son las exigencias a los activos y ciber activos durante la operación, mantenimiento y soporte de las tecnologías de operaciones, para evitar posibles incumplimientos y afectación de los niveles de satisfacción de los interesados.

l. ¿De los anteriores, ¿cuáles son los mínimos requerimientos de proceso que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un evento que lo afecte?

Si	No	Parcialmente	No responde
2	6	2	
20.0	60.0	20.0	-

Figura 3-12. Tabulación Respuesta pregunta 12



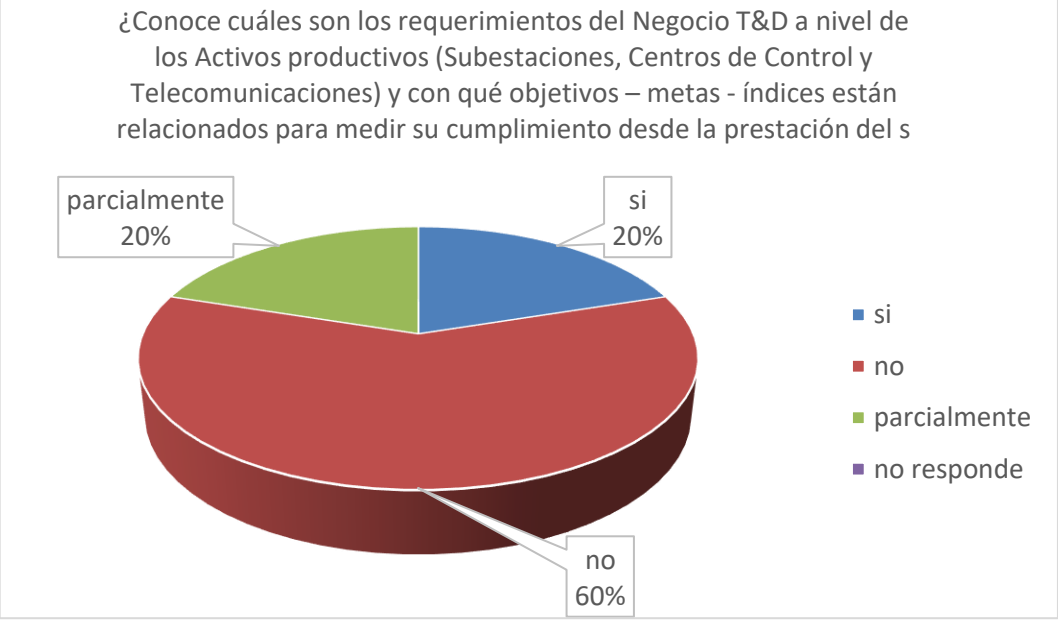
Fuente: Elaboración propia

En la Figura 3-12 se puede observar que, frente a los requerimientos mínimos desde el proceso a nivel de servicio a tener en cuenta para el restablecimiento ante una interrupción, el conocimiento se reduce a un 20%, de manera parcial otro 20% y no lo conocen o no responden el 60%. Está claro que un equipo de respuesta debería igualmente conocerlos para evitar posibles incumplimientos y afectación de los niveles de satisfacción de los interesados.

m. ¿Conoce cuáles son los requerimientos del Negocio T&D a nivel de los Activos productivos (Subestaciones, Centros de Control y Telecomunicaciones) y con qué objetivos – metas - índices están relacionados para medir su cumplimiento desde la prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
2	6	2	
20.0	60.0	20.0	-

Figura 3-13. Tabulación Respuesta pregunta 13



Fuente: Elaboración propia

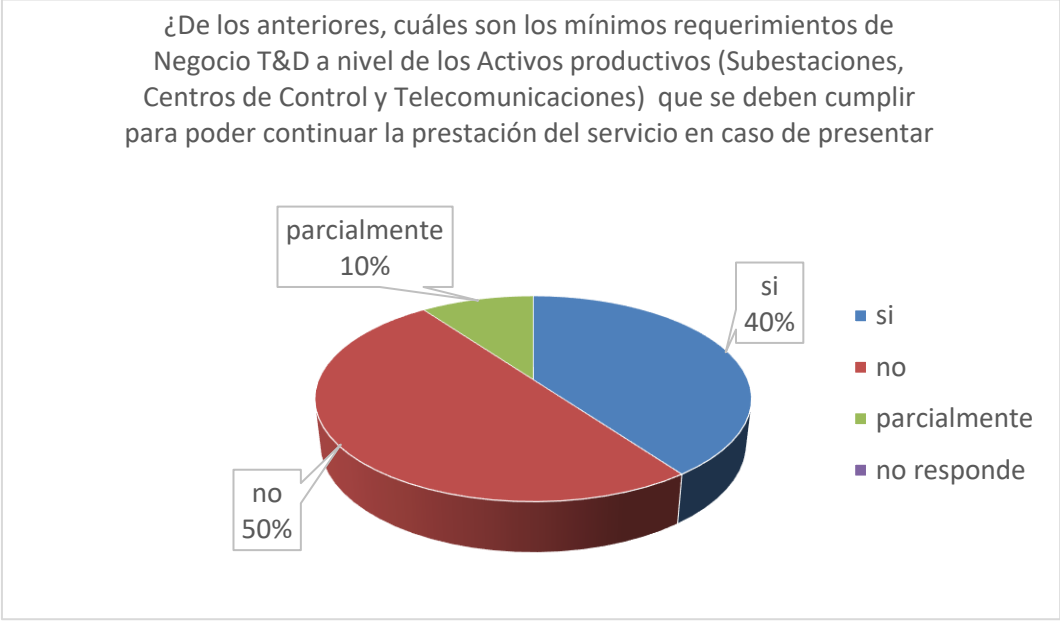
En la Figura 3-13 se observa que solo el 20% de los encuestados dijeron conocer los requerimientos del Negocio en relación con las exigencias a los activos productivos que soportan servicio en distribución de energía, un 20% dijo conocerlos de manera parcial y el 60% restante respondió no conocerlos. Este es un tema relevante para un equipo de respuesta a incidentes, en la medida que entiende las exigencias que desde el negocio se tienen con los activos productivos, los cuales están apalancando el

cumplimiento de metas, objetivos e indicadores claves y como una interrupción puede generar una afectación en su gestión.

n. ¿De los anteriores, cuáles son los mínimos requerimientos de Negocio T&D a nivel de los Activos productivos (Subestaciones, Centros de Control y Telecomunicaciones) que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un Incidente / Evento que lo afecte (Calidad – Continuidad) y reducir al máximo los impacto?

Si	No	Parcialmente	No responde
4	5	1	
40.0	50.0	10.0	-

Figura 3-14. Tabulación Respuesta pregunta 14



Fuente: Elaboración propia

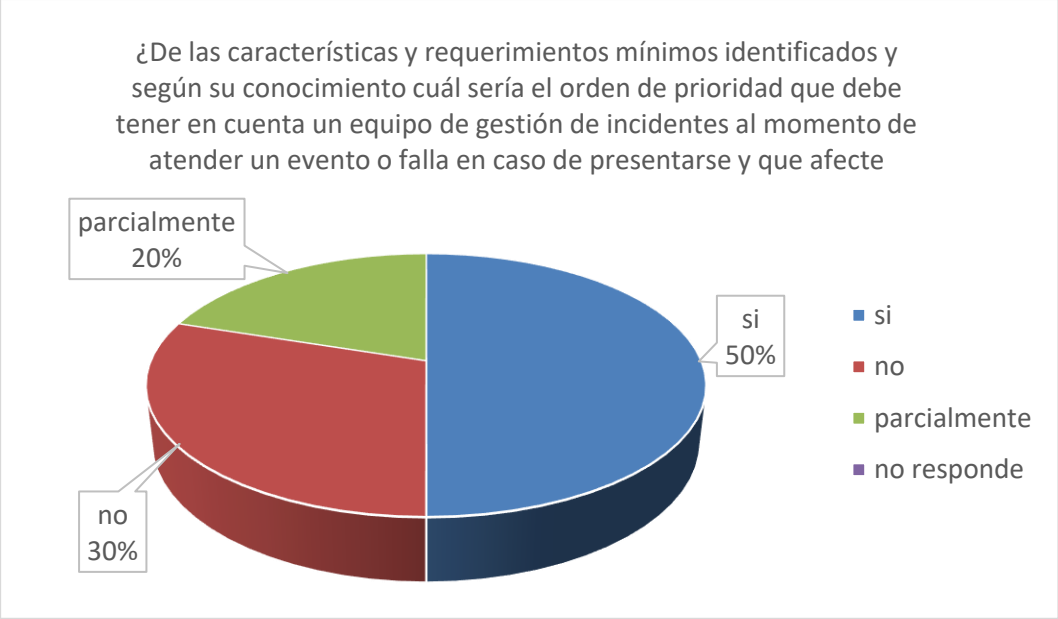
A diferencia de la anterior pregunta, en la Figura 3-14, el 40% respondieron si conocer los requerimientos del Negocio en relación con las exigencias mínimas a los activos productivos desde el punto de vista del servicio a tener en cuenta para el

restablecimiento ante una interrupción, el conocimiento se reduce a un 10%, de manera parcial y a un 50% que dijeron no conocerlos. Está claro que un equipo de respuesta a incidentes debería igualmente conocerlos para evitar posibles incumplimientos y afectación de los niveles de satisfacción de los interesados.

o. ¿De las características y requerimientos mínimos identificados y según su conocimiento cuál sería el orden de prioridad que debe tener en cuenta un equipo de gestión de incidentes al momento de atender un evento o falla en caso de presentarse y que afecte la prestación del servicio de distribución de energía?

Si	No	Parcialmente	No responde
5	3	2	
50.0	30.0	20.0	-

Figura 3-15. Tabulación Respuesta pregunta 15



Fuente: Elaboración propia

Del total de entrevistados, en la Figura 3-15, el 50% manifestó tener el conocimiento para priorizar las características y requerimientos mínimos a tener en cuenta en la

prestación del servicio de distribución energía y cumplir con las exigencias de los Grupos de Interés involucrados, igualmente un 20% dijo hacerlo de manera parcial y un 30% restante respondió que no.

Esta priorización es clave para un equipo de respuesta a incidentes, en la medida que le permite de acuerdo con las circunstancias, determinar el orden de las prioridades que deberá concertar con el equipo de operación del negocio afectado y lograr una respuesta efectiva.

Análisis de la entrevista

Para concluir la presentación de resultados y con el fin de conocer cuáles son las características y requerimientos mínimos para el servicio de distribución de energía, se relacionan a continuación los principales comentarios generados por los participantes y que están asociados a los tipos de requerimientos y características definidos por ellos:

a. Características técnicas que se requieren para la correcta prestación del servicio de distribución de energía:

- Continuidad y calidad atributos que son regulados por la CREG bajo la denominación de DES - FES, SAIDI - SAIFI que básicamente corresponden a los indicadores de duración acumulada mensual de las interrupciones del servicio y de la frecuencia de estas.
- La calidad de la potencia o del suministro corresponde a la estabilidad del suministro eléctrico (en términos de pureza de la onda senoidal es decir sin armónicos) y a la estabilidad del voltaje y frecuencia.
- Disponibilidad de la información de campo para su correcta medición, supervisión y control (TO)

b. Las Características técnicas mínimas requeridas para poder continuar la prestación del servicio en caso de presentarse un evento son:

- Niveles de tensión adecuados para no causar daños a terceros en electrodomésticos u oscilaciones que ocasionen perdidas en diferentes procesos por paros de maquinaria.
- Los anterior se garantiza con la disponibilidad de las herramientas tecnológicas en el Centro de control SCADA para supervisar y maniobrar y DMS para identificación al detalle de la posible afectación.
- Alta disponibilidad del SCADA y el DMS y habilidad de actuación desde la supervisión por el personal que hace parte de la operación para actuar bajo el conocimiento de las exigencias normativas
- Confiabilidad y seguridad, ya que con la primera llegado el caso de requerirse se cuenta con la posibilidad de hacer transferencias o tener respaldo para alimentar la carga, llegado el caso que se den las condiciones técnicas para hacerlo. Por otro lado, la segunda me permite atender la demanda con los estándares básicos que permitan proteger tanto de la seguridad de las personas como de los equipos.

c. Las Características funcionales mínimas a nivel de los Ciber activos de las Tecnologías de Operación para subestaciones:

- Ver norma IEC61850 que detalla los componentes de automatización de subestaciones y describe los componentes y características de la discretización e interoperabilidad de las unidades de medida con funciones de protección y control con sus comunicaciones en el nivel del proceso
- Las funcionalidades mínimas requeridas para garantizar la continuidad del servicio son los subsistemas y macro componentes relacionadas con la supervisión y control en tiempo real.
- Específicamente las SAS en campo, las comunicaciones operativas, el SCADA central (DAS, Imagen del proceso, Funciones de tiempo real, interfaces de operador) En este caso se exceptúan los componentes de históricos, enlaces y servicios a terceros (aplicaciones corporativas) y en general las aplicaciones del EMS y del DMS.

- El SCADA y el DMS deben estar siempre disponibles, porque si bien es cierto, en algún momento por falla coincidente de red corporativa y SCADA se puede operar, hay un impacto alto en el modo de actuación para mantener la continuidad de servicio en caso de una falla en la infraestructura, nos volvemos más lentos para una correcta toma de decisión.
- Las características funcionales mínimas del proceso primario, es decir necesarias para la transformación de la energía a los niveles de voltaje que se requieren en el activo crítico, esto es; 1) Procesamiento de señales, mandos de control de los elementos electromecánicos del patio y elementos de supervisión primaria de las variables de la subestación, 2) Dependiendo de los protocolos de comunicación que se usen en la subestación, serán necesarias o no las redes ethernet o seriales que posibilitan el control automatizado o manual de algunos de los equipos, y 3) Los equipos para subestaciones eléctricas deben tener la posibilidad de actuar manualmente de ser necesario para dar continuidad al servicio, por lo que estas características electromecánicas o manuales también deben estar disponibles.

d. Las características y requerimientos mínimos de Seguridad Operacional a nivel del activo (Subestación de Energía) son:

- A nivel de técnico contar con la correcta configuración de los Ciber activos y elementos de una subestación eléctrica, así como la información y el estado de estos, lo cual permitiría tomar decisiones y acciones a nivel de mantenimientos predictivos y correctivos de forma oportuna, esto haría parte del componente tecnológico.
- A nivel de la operación se debe contar con todos los lineamientos y procedimientos para una operación local-remota de forma segura. Allí se encuentran consignados todos los mecanismos de protección de la infraestructura y del personal humano que actúa en ella. Esto siempre teniendo en cuenta los resultados de los análisis de riesgos basados en consecuencias. La revisión periódica también es clave como elemento indispensable para detectar fallas durante el proceso.
- A nivel de las protecciones deben estar debidamente configuradas o seteados que cumplan con los estándares que correspondan (acuerdos CNO, acuerdo con el CND,

código de redes, entre otras regulaciones), y mantener Redundancia en los sistemas de protección para proteger tanto la vida humana de quien operan como también la vida útil de los equipos o activos. Adicionalmente, deben existir guías de operación claros y homologados que contengan la forma de operar y maniobrar los equipos, así como también de su operación bajo contingencias, por lo cual también se debe contar con operación local o remota.

- En cuanto a las comunicaciones, los datos deben ser muy confiables y con ello la tasa de errores debe ser baja en cuanto a sus datos, reflejando siempre una información confiable del proceso.

e. En cuanto a los Requerimientos externos (legales normativos y regulatorio) que le aplican en términos del servicio son:

- A nivel regulatorio en Colombia están las normatividades emitidas por la CREG (Comisión de regulación de Energía y GAS), en el cual se establecen las normas y regulaciones para la prestación del suministro de energía. También se encuentran los lineamientos del CNO (Consejo Nacional de Operación). Allí se establecen acuerdos de obligatorio cumplimiento para todos los agentes del sector.
- Igualmente se encuentran relacionados:
  - Constitución del 91, Artículo 3, Artículo 365.
  - Ley 142 del 94
  - Ley Eléctrica 143 del 94
  - CONPES 3701, 3854, 3955
  - MinTIC, Guías de seguridad
  - Plan defensa, Plan nacional de protección de infraestructuras críticas
- En cuanto a Los requerimientos mínimos ante un incidente de seguridad, se hace especial énfasis a:
  - Las garantías de operación al sistema interconectado nacional en cuanto a; 1) Capacidad de transporte, 2) Calidad de tensión, y 3) Cumplimiento de los ANS (Acuerdos de Niveles de Servicio) estos hacen parte de las condiciones generales de la prestación del servicio.

- A pesar de que exista una contingencia o evento, la calidad del servicio de la energía está regulada y debe cumplir con unos indicadores de calidad indicados en la regulación CREG 015 del 2018, en la cual se consignan el número de aperturas por permisibles y su frecuencia, entre otras.
- La Calidad de la Potencia de acuerdo con lo establecido en la Resolución 024 de 2005 y sus modificatorias.

f. Los Requerimientos internos (ANS, proceso, negocio) son:

- La atención oportuna en caso de presentarse fallas en algunos componentes de una subestación, por ejemplo. El monitoreo constante y garantizar la continuidad en las comunicaciones con el Centro de Control de Energía. Contar con el recurso humano capacitado y disponible para atender cualquier requerimiento o incidente, estos tienen componentes de tiempo y efectividad en la atención correspondiente, las cuales varían dependiendo del evento.
- Velar por la continuidad de las tecnologías (SAS en las estaciones, comunicaciones, sistemas del CC) que permiten la supervisión y control de la infraestructura del servicio a los clientes de distribución, cumpliendo indicadores acordados de atención ante fallos en cualquier de sus componentes y cumpliendo los requisitos de disponibilidad determinados por el Regulador (CREG) para su remuneración y los acuerdos del CNO.
- Para la categorización de Requerimientos y prioridades en la atención de los eventos e incidentes se cuenta con la siguiente clasificación.
  - Prioridad 1: Eventos que tienen una afectación parcial importante o total de la operación.
  - Prioridad 2: Son los requerimientos asociados a todas las novedades que representen una eventual o actual afectación de la operación de la RTU, sistemas de comunicaciones, equipos de control y protección y/o las variables del proceso.
  - Prioridad 3: son los requerimientos que se hacen a las Unidades durante el desarrollo habitual de la operación.
- Se deben priorizar las acciones que minimicen la indisponibilidad de los subsistemas o componentes de mayor impacto a la supervisión y control. principalmente los de

prioridad 1 o atención inmediata, asociados a la Disponibilidad del SCADA y de las aplicaciones (DMS).

g. Requerimientos del proceso que se deben tener para la correcta prestación del servicio de distribución de energía:

- Contar con la comunicación disponible para operar o maniobrar el equipo o activo que se requiera y de acuerdo con las condiciones del sistema o cuando lo requiera el proceso.
- Además, de la agilidad de actuación de los equipos con tiempos de actuación acorde a:
  - Las alarmas sonoras y visuales disponibles que les permitan a los operadores del centro de control tomar o desencadenar las acciones respectivas.
  - Buena calidad de los datos para con ello poder tener la información necesaria a la hora de tomar decisiones para la supervisión o maniobra. Además, los datos históricos son un insumo importante para la operación, ya que permiten realizar análisis posoperativos respectivos.
  - Contar con planes de contingencia para el restablecimiento de las comunicaciones y de los sistemas para la operación remota, así como de los aplicativos o software que soportan la operación tanto en condiciones normales como ante fallas.
  - La correcta prestación del servicio de los sistemas de transmisión tanto nacional como local.
  - Disponibilidad de Tele medición y telecontrol de los elementos de corte y maniobra instalados en el SDL, según Resolución 015 de 2018 y sus modificatorias.
  - Infraestructuras del servicio e instrumentación asociada cumplan funcionalmente con su cometido en los tiempos y calidad previstas. Se requieren mantenimientos preventivos para validar su correcto funcionamiento.
- Ahora bien, los mínimos requerimientos del proceso que se deben cumplir para poder continuar la prestación del servicio en caso de presentarse un evento son:
  - Disponibilidad de Tele medición y telecontrol de los elementos de corte y maniobra instalados en el SDL, según Resolución 015 de 2018 y sus modificatorias.

- Los planes de restablecimiento o contingencia para restablecer si así se requiere. Sin embargo, debido a la regulación vigente es sumamente importante todos los elementos o aspectos del ítem anterior.
- En continuidad, es tener personal en el centro de control capacitado que pueda coordinar una maniobra con personal en terreno en caso de una falla cuando no hay herramientas y logren validar condiciones seguras.

h. Los requerimientos del Negocio T&D a nivel de los Activos productivos (Subestaciones, Centros de Control y Telecomunicaciones) son:

- Para los Ciber activos los requisitos funcionales son básicamente que estos actúen con base para lo que fueron adquiridos, estos deben cumplir con la normatividad colombiana, y características operacionales y de seguridad. Que permitan ser supervisados y operados desde un componente centralizado.
- A nivel de negocio actualmente se están midiendo desde CMI con el SAIDI, este aplicado para todos los negocios relacionados con la prestación del servicio de energía. Así que los requerimientos es que cumplamos la meta, y todos los esfuerzos que cada negocio identifique en pro de mejorar sus procesos, apalancara este cumplimiento. Este indicador mide el tiempo de afectación por usuario y de acuerdo con ello se pagan unas compensaciones. Es un todo, que si no funciona un eslabón de la cadena se impacta por defecto el tiempo de atención de un evento.
- Todo esto basado en la regulación vigente, que es la CREG015 del 2018 en cuento a indicadores de calidad del servicio. Sin embargo, es importante contar con activos sanos que permitan la maniobrabilidad del sistema, además de contar con respaldo para alimentar la carga por otras fuentes de alimentación llegado el caso de requerirse (en el Anexo 3: Consolidado Inf Ftes Sec Req Servicio SD E se puede consultar los requisitos de la resolución 015 de 2018).
- En cuanto a los requerimientos mínimos que debe tener en cuenta un equipo de gestión de incidentes al momento de atender un evento o falla que afecte la prestación del servicio de distribución de energía, las personas entrevistadas comentaron lo siguiente:

- Una subestación debe hacer parte de una cadena de enlaces de un proceso por el que se transmite y distribuye energía, no es un ente que actúe en un proceso aislado, por lo tanto, se deben mantener todos los equipos en correcto funcionamiento porque es un sistema enlazado, aunque no haya redes de comunicación, por lo tanto, una recopilación de evidencia no puede parar el proceso, debe idearse la forma de recopilarla mientras se vuelve a activar el proceso de distribución de energía.
- Se debe conocer el proceso del que se es parte para mantener presente que es un proceso critico de la sociedad, la economía y el orden público, que debe estar listo y funcionando en el menor tiempo posible.
- Se debe tener presente que el proceso de generación, trasmisión y distribución de energía trabajan sinérgicamente y necesitan el uno del otro, por lo que es necesario que todos trabajen correctamente y en un tiempo prudencialmente corto.
- Los procesos de las subestaciones son procesos de tiempo real, es necesario tener cuidado con las latencias retardos, bloqueos o comportamientos indeseados que pueden tener algunas herramientas de seguridad cibernética que deban ser utilizadas.
- La curva de experiencia y aprendizaje el personal del sector eléctrico es lenta y larga, no se las van a saber todas y no lo van a comprender todo en un mes, deben aceptar las recomendaciones de los empleados especializados.
- Los responsables de los activos son quienes tienen la última palabra en la implementación de acciones que puedan afectar el funcionamiento de los ciber activos y el activo crítico.
- La indisponibilidad de las subestaciones cuesta dinero, los servicios de disponibilidad de energía de generadores que pase por las subestaciones cuesta mucho dinero, y por los activos en funcionamiento pagan por dinero, por lo tanto, allí el tiempo es dinero.
- Los activos cibernéticos no pueden ser retirados de la subestación como evidencia, puede ser realmente difícil reemplazar un equipo del sistema automatizado de subestaciones eléctricas por sus características especializadas.

- La persona que está en la supervisión debe identificar qué es lo que está pasando en el sistema y que analíticamente pueda establecer un camino de decisión que guie su actuación.
- Se debe mantener en todo momento una comunicación asertiva: sea con personal en campo, en la subestación u otros grupos de interés para coordinar el tipo de falla de herramientas, sistema o prestación del servicio.
- Tener a la mano y utilizar en lo posible el manejo de las herramientas de simulación que le permitan acotar un poco más el daño para restablecer más rápidamente es importante.
- Coordinar de forma permanente el estableciendo condiciones de seguridad,
- Y por último resolver la falla.

3.1.2 Actividad 2. Recolección de Información Secundaria

Con respecto al referenciamiento de las fuentes secundarias consultadas, los resultados se presentan en el siguiente orden:

a. Constitución Política de Colombia de 1991 - Tratados Internacionales
b. Ley 142 de 1994, es la Ley de Servicios Públicos Domiciliarios en Colombia
c. Ley 143 de 1994 Por la cual se establece el régimen para la generación, interconexión,
d. Ley 1581 de 2012 Protección de Datos Personales
e. Ley 1712 de 2014 de Transparencia y de Acceso a la Información
f. CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL (CONPES) organismo asesor del gobierno colombiano en lo que respecta al desarrollo económico y social del país (3701, 3854, 3995)
g. Comisión de Regulación de Energía y Gas -CREG (097, 070, 015, 025, 080, 038)
h. Consejo Nacional de Operación del Sector Eléctrico (CNO) (788, 1241, 1043, 1347)
i. Ministerio de Defensa - Comando Conjunto Cibernético (CCOC)(Plan Nacional de Protección y Defensa de Infraestructura Critica Cibernética, plan sectorial, Plan de Protección Específico de Infraestructura Crítica Cibernética, Plan Sectorial de Protección y Defensa para el Sector Electricidad de Colombia PSPSE V1.0,)

En la Tabla 3-2 se presenta para cada fuente de información, un resumen de los aspectos más relevantes con relación a los servicios públicos y cómo le puede aportar a los requerimientos mínimos para tener en cuenta en el servicio con foco en la disponibilidad. Igualmente, en el Anexo 3: Consolidado Inf Ftes Sec Req Servicio SD E podrán mirar en más detalle la información de cada fuente consultada.

Tabla 3-2. Consolidado de normas y leyes que le aportan al servicio de energía

Norma o ley	Resumen o aporte a la ciberseguridad en TO y/o disponibilidad del servicio de energía.
1. Constitución Política de Colombia de 1991 - Tratados Internacionales	La ley regulará el control de calidad de bienes y servicios ofrecidos y prestados a la comunidad, así como la información que debe suministrarse al público en su comercialización. Serán responsables, de acuerdo con la ley, quienes en la producción y en la comercialización de bienes y servicios, atenten contra la salud, la seguridad y el adecuado aprovisionamiento a consumidores y usuarios.
2. Ley 142 de 1994, es la Ley de Servicios Públicos Domiciliarios en Colombia	Garantizar la calidad, prestación continua e ininterrumpida, sin excepción alguna, salvo cuando existan razones de fuerza mayor o caso fortuito o de orden técnico o económico que así lo exijan.
3. Ley 143 de 1994 Por la cual se establece el régimen para la generación, interconexión,	Abastecer la demanda de electricidad de la comunidad bajo criterios económicos y de viabilidad financiera, asegurando su cubrimiento en un marco de uso racional y eficiente de los diferentes recursos energéticos, asegurando una operación eficiente, segura y confiable, manteniendo y operando sus instalaciones, preservando la integridad de las personas, de los bienes y del medio ambiente y manteniendo los niveles de calidad y seguridad establecidos. El servicio de electricidad se regirá por principios de eficiencia, calidad, continuidad, adaptabilidad, neutralidad, solidaridad y equidad. En virtud del principio de calidad, el servicio prestado debe cumplir los

Norma o ley	Resumen o aporte a la ciberseguridad en TO y/o disponibilidad del servicio de energía.
	requisitos técnicos que se establezcan para él. El principio de continuidad implica que el servicio se deberá prestar aún en casos de quiebra, liquidación, intervención, sustitución o terminación de contratos de las empresas responsables del mismo, sin interrupciones diferentes a las programadas por razones técnicas, fuerza mayor, caso fortuito, o por las sanciones impuestas al usuario por el incumplimiento de sus obligaciones y el principio de adaptabilidad conduce a la incorporación de los avances de la ciencia y de la tecnología que aporten mayor calidad y eficiencia en la prestación del servicio al menor costo económico.
4. CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL (CONPES) organismo asesor del gobierno colombiano en lo que respecta al desarrollo económico y social del país (3701, 3854, 3995)	Dentro de estos documentos se trazan como objetivos: 1. El fortalecimiento de la capacidad del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético, y a su vez se definen tres objetivos específicos: a) Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional; b) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa; y 3) Fortalecer el cuerpo normativo y de cumplimiento en la materia. 2. Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades

Norma o ley	Resumen o aporte a la ciberseguridad en TO y/o disponibilidad del servicio de energía.
	socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país. 3. Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital
5. Comisión de Regulación de Energía y Gas -CREG (097, 070, 015, 025, 080, 038)	Estos documentos regulatorios aprueban, reglamentan y definen entre otros asuntos: 1. Los principios generales y la metodología para el establecimiento de los cargos por uso de los Sistemas de Transmisión Regional y Distribución Local, en términos de la calidad del servicio, horas máximas de indisponibilidad, compensaciones por la energía no suministrada, clasificación de las interrupciones, exclusiones e índices de discontinuidad. (097) 2. Establece el reglamento de distribución de energía eléctrica, como parte del reglamento de operación del sistema interconectado nacional y trata temas como, las condiciones de contingencia, información sobre la ocurrencia de eventos en el sistema, incumplimiento de los indicadores de calidad del servicio prestado, características técnicas de los equipos de medida y Sistema de información de la red de distribución (070)

Norma o ley	Resumen o aporte a la ciberseguridad en TO y/o disponibilidad del servicio de energía.
	3. establece la metodología para la remuneración de la actividad de distribución de energía eléctrica en el Sistema Interconectado Nacional y entre otros temas trata; la obligación del reporte de eventos, clasificación de los eventos en el sistema de distribución, indicadores de calidad media tensión y compensación (015) 4. Establecen reglas generales de comportamiento de mercado para los agentes que desarrollen las actividades de los servicios públicos domiciliarios de energía eléctrica y gas combustible, como, por ejemplo; Comportamientos que propenden por la adecuada prestación del servicio público en relación con la gestión de riesgos, y los riesgos en la prestación del servicio. (080) 5. Establece el Código de Redes, como parte del Reglamento de Operación del Sistema Interconectado Nacional y determina entre otros; calidad, seguridad, confiabilidad, requerimientos y especificaciones mínimas de los equipos y requisitos de las protecciones (025).
6. Consejo Nacional de Operación del Sector Eléctrico (CNO) (788, 1241, 1043, 1347)	Estos documentos del Sector eléctrico aprueban e incentivan la adopción de la Guía de Ciberseguridad y las condiciones mínimas de seguridad e integridad para la transmisión de las lecturas desde los medidores hacia el Centro de Gestión de Medidas,
7. Ministerio de Defensa - Comando Conjunto Cibernético (CCOC)	Establecen entre otros asuntos, el plan nacional de protección y defensa de infraestructura critica cibernética, la guía de Elaboración del Plan de Protección

Norma o ley	Resumen o aporte a la ciberseguridad en TO y/o disponibilidad del servicio de energía.
	Específico de Infraestructura Crítica Cibernética, el plan sectorial de protección y defensa para el Sector Electricidad de Colombia

Fuente: Elaboración Propia.

La anterior tabla muestra las leyes y normas que más le aportan a la gestión de incidentes y por el cual se debe regir y cumplir todo lo relacionado con su gestión y como se puede apreciar, la existencia de normas a nivel Colombia establecen un panorama muy positivo en cuanto a la protección de la infraestructura crítica y el apoyo requerido para la creación de un procedimiento para la atención de posibles eventos de seguridad.

En la siguiente Tabla 3-3 se presenta la lista de requerimientos mínimos consolidados para tener en cuenta en la prestación del servicio y en especial en la gestión de incidentes de ciberseguridad, en cuanto a disponibilidad, y su relación con las respuestas obtenidas con base en las preguntas realizadas en la entrevista.

Esta lista de requerimientos surge de los elementos mínimos a tener en cuenta que, desde las entrevistas con los expertos, mencionaron como los más relevantes para una disponibilidad del activo y el servicio de transmisión y distribución, lo cual es ratificado por los énfasis que la regulación, los aspectos legales y sectoriales mencionan.

Tabla 3-3. Matriz de relaciones de Requerimientos Vs Fuentes Primarias Consultadas

	Requerimientos mínimos del servicio de TO en cuanto a disponibilidad							
Fuente Secundaria	**Seguridad**	**Continuidad**	**Resiliencia**	**Recuperación**	**Contingencia**	**Concienciación, formación y entrenamiento**	**Prevención**	**Monitoreo**
Pregunta 1		**x**						**x**
Pregunta 2	**x**	**x**		**x**	**x**		**x**	**x**
Pregunta 3		**x**	**x**		**x**		**x**	**x**
Pregunta 4	**x**	**x**			**x**			
Pregunta 5	**x**	**x**	**x**		**x**		**x**	**x**
Pregunta 6	**x**	**x**	**x**		**x**		**x**	**x**
Pregunta 7	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
Pregunta 8	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
Pregunta 9	**x**	**x**		**x**	**x**	**x**		**x**
Pregunta 10	**x**	**x**		**x**	**x**	**x**		**x**
Pregunta 11	**x**	**x**		**x**	**x**			
Pregunta 12	**x**	**x**			**x**			**x**
Pregunta 13	**x**	**x**		**x**	**x**		**x**	**x**
Pregunta 14	**x**	**x**	**x**	**x**	**x**		**x**	**x**

Fuente: Elaboración Propia

Así mismo, en la Tabla 3-4 se hace la relación de las fuentes secundarias con los requerimientos mínimos:

Tabla 3-4. Matriz de relaciones de Requerimientos Vs Fuentes Secundarias Consultadas

	Requerimientos mínimos del servicio de TO en cuanto a disponibilidad							
Fuente Secundaria	**Seguridad**	**Continuidad**	**Resiliencia**	**Recuperación**	**Contingencia**	**Concienciación, formación y entrenamiento**	**Prevención**	**Monitoreo**
Constitución del 91	**x**							
Ley 142 de 1994		**x**						
Ley 143 de 1994	**x**	**x**	**x**					
Conpes 3701 / 3854 / 3995	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
CREG 097 / 070 / 015 / 025 / 080/ 038	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
CNO 1241 / 1347 / 1043	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
Min Defensa CCOC/ Plan Nal Prot Def ICC / Plan Sect Prot Def ICC / Plan de Prot Esp ICC	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**

Fuente: Elaboración Propia

Como se puede ver en las Tabla 3-3 y Tabla 3-4 en los respectivos cruces, existe una relación directa y se valida que en la operación se tiene en cuenta el marco normativo para su cumplimiento, y que tanto la entrevista como la parte legal son insumos claves para tener presente en el diseño del nuevo procedimiento de gestión de incidentes de ciberseguridad.

A continuación, en la Tabla 3-5, se generó el consolidado de preguntas y referentes secundarios que les aportan a los requerimientos mínimos:

Tabla 3-5. Matriz Consolidada de las Características y Requerimientos mínimos Vs Fuentes Primarias y Fuentes Secundarias

	Preguntas de la Entrevista relacionadas con el Requerimiento							
	2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	3, 5, 6, 7, 8, 14	2, 7, 8, 9, 10, 11, 13, 14	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14	7, 8, 9, 10	2, 3, 5, 6, 7, 8, 13, 14	1, 2, 3, 5, 6, 7, 8, 9, 10, 12, 13, 14
	Características y Requerimientos mínimos del servicio de TO en cuanto a disponibilidad							
Fuente Ref.	Seguridad	Continuidad	Resiliencia	Recuperación	Contingencia	Concienciación, formación y entrenamiento	Prevención	Monitoreo
Constitución Política de Colombia de 1991 - Tratados Internacionales	**x**							
Ley 142 de 1994, es la Ley de Servicios Públicos Domiciliarios en Colombia		**x**						
Ley 143 de 1994 Por la cual se establece el régimen para la	**x**	**x**	**x**					

generación, interconexión,								
CONSEJO NACIONAL DE POLITICA ECONOMICA Y SOCIAL (CONPES) (3701, 3854, 3995)	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
Comisión de Regulación de Energía y Gas -CREG (097, 070, 015, 025, 080, 038)	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
Consejo Nacional de Operación del Sector Eléctrico (CNO) (1241, 1043)	**x**	**x**	**x**	**x**	**x**	**x**		**x**
Ministerio de Defensa - Comando Conjunto Cibernético (CCOC)(Plan Nacional de Protección y Defensa de Infraestructura Critica Cibernética, plan	**x**	**x**	**x**	**x**	**x**	**x**	**x**	**x**

sectorial, Plan de Protección Específico de Infraestructura Crítica Cibernética,								

Fuente: Elaboración propia

Como resultado se obtiene que son 8 las características y requerimientos mínimos (las que se muestran en la tabla anterior) que se deben tener presentes en la gestión de incidentes de ciberseguridad con el propósito de poder lograr la disponibilidad en la prestación de los servicios que soportan las tecnologías de la operación.

Se llega a esta conclusión después de identificar que cada uno de ellos son incluidos en las diferentes leyes y normas que regulan el servicio de transmisión y distribución de energía y cuya relación se cruzó con las respuestas obtenidas a las preguntas realizadas en la entrevista, donde los encuestados con base en su conocimiento y experiencia, también los identifican como requisitos mínimos esenciales evidenciando que no es posible ofrecer una prestación eficiente y continua de los servicios garantizando su disponibilidad sin contar con estos requerimiento mínimos en la operación de TO.

Nota: Desde el Ministerio de Minas y Energía (MME), a través de la CREG se propone que se deberá expedir mediante resolución los requerimientos de disponibilidad, exactitud y precisión, así como las penalizaciones derivadas del incumplimiento de estos requerimientos para las mediciones y variables análogas y digitales de todos los generadores, consumos y demás equipos del SIN que hacen parte del modelo de red utilizado por el CND para el despacho de energía y para la supervisión en tiempo real del sistema. En cualquier caso, la indisponibilidad de las mediciones reportadas al CND no deberán ser superior a 30 minutos sobre una venta de un mes. Para cumplir con lo anterior, se deberá considerar la instalación redundante de equipos alimentación, equipos de medición y sistemas de comunicación.

Es importante mencionar que en la primera semana del Mes de diciembre de 2020, se emitió una comunicación por parte del Ministerio de Minas y Energía (MME) de Colombia en el sentido de trabajar conjuntamente con los agentes del Sector Eléctrico (Generadores, Transmisores y Distribuidores de Energía Eléctrica) un proyecto de resolución " Por la cual se definen criterios de resiliencia, seguridad y confiabilidad para el suministro de energía eléctrica", el cual aborda aspectos relevantes como:

- Identificación de subestaciones estratégicas, requerimientos y remuneración
- Resiliencia

- Supervisión en tiempo real
- Remuneración del servicio complementario de arranque en negro o autónomo de plantas de generación.
- Incorporación de criterios de planificación de la expansión de transmisión
- Programas de capacitación
- Auditorías a los esquemas de protección
- Entre otros

Este proyecto de resolución se encuentra en las etapas finales para su publicación y posterior implementación con unos tiempos acordados para su cumplimiento. Desde el análisis que realizamos a dicho documento se observó que impacta nuestro trabajo de investigación y por lo tanto lo incluimos en las definiciones de los requerimientos mínimos a considerar.

3.2 Fase 2: Actividades claves de la gestión de riesgos, continuidad del negocio, gestión de crisis y resiliencia

De acuerdo con la metodología, para esta fase se obtuvieron los siguientes resultados:

3.2.1 Actividad 1. Referenciamiento de mejores prácticas

Revisión de los marcos de referencia para:

- Gestión de Riesgos.
- Gestión de Continuidad
- Gestión de Crisis
- Gestión de Resiliencia

1) Presentación de algunos marcos de referencia utilizados en Gestión de Riesgos

a. <u>Descripción de normas</u>

- **Octave. Operationally Critical Threat, Asset, and Vulnerability Evaluation**. Se trata de una metodología que orienta a las organizaciones para que dirijan y gestionen de una manera efectiva sus evaluaciones de riesgos a nivel operativo, de manera que se tomen decisiones tomando como base los riesgos, se protejan los activos de información más críticos y por último se comunique de manera efectiva la información específica y fundamental relacionada con la seguridad [71].

- **NIST SP 800 – 30. (National Institute of Standards and Technology)**. La metodología propone recomendaciones y acciones a implementar para realizar una correcta gestión sobre cada riesgo para establecer un sistema de gestión en seguridad de información, el cual es acompañado por el compromiso y responsabilidad del personal relacionado con la empresa en todos los niveles, para lograr cumplir con los objetivos trazados. Esta más orientada y se destaca por ayudar a gestionar riesgos en proyectos de tecnología, logrando una implementación satisfactoria en hardware, bases de datos, software,

telecomunicaciones y redes, esto a través de criterios de seguridad que integra en su estructura entre los que se encuentran confidencialidad, integridad y disponibilidad, como base para valorar la materialización de amenazas y el impacto que ocasionan sobre los elementos que conforman las tecnologías de la información que integran las diferentes empresas en el mundo [72]

- **Mehari. (Método Armonizado de Análisis de Riesgos)**. Esta metodología fue propuesta y desarrollada por el Club Francés de la Seguridad de la Información CLUSIF en el año 1996; es de acceso público y para todo tipo de organizaciones. Se diseñó inicialmente y se actualiza continuamente para ayudar a los CISO (Chief Information Security Officers) en la gestión de las actividades de la seguridad informática, pero también está concebida para auditores CIO o gestores de riesgos. Es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgo, evaluando cuantitativamente, de acuerdo con la situación de la organización, dónde se requiere el análisis; acopla los objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la empresa mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido. Mehari propone un módulo para analizar los intereses implicados por la seguridad y un método de análisis de riesgos con herramientas de apoyo [3] . El principal objetivo de Mehari es proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos ISO/IEC 27005:2008, por medio de un conjunto de herramientas y elementos necesarios para su implementación [73].

- **Magerit**. Se desarrolló por el consejo superior de administración electrónica, esta se basa en dos objetivos fundamentales, primero estudiar cada uno de los riesgos que afectan el sistema de seguridad de la información y su contexto, y el segundo, se basa en las recomendaciones que se enmarcan con el fin de desarrollas las medidas apropiadas de adopción que permiten hacer una evaluación, prevenir reducir y controlar los riesgos que se hayan identificado. [7]. En Magerit, la seguridad es definida como “aquella capacidad de las redes y sistemas de información que permiten soportar, teniendo adecuado margen

de confianza, los incidentes o actividades que de forma malintencionada ponen en compromiso la integridad, disponibilidad, autenticidad y confidencialidad para datos guardados o que son trasmitidos y de cada servicio que se ofrece a través de esas redes o sistemas" [74]

- **ISO 27005:2018**. Esta norma proporciona directrices para la gestión del riesgo en la seguridad de la información en una organización, dando soporte particular a los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma NTC-ISO/IEC 27001. Sin embargo, esta norma no brinda ninguna metodología específica para la gestión del riesgo en la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo, dependiendo por ejemplo del alcance de su SGSI, del contexto de la gestión del riesgo o del sector industrial [75].

- **ISO 31000:2018**. Este documento proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto. Este documento proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específico de una industria o un sector. Este documento puede utilizarse a lo largo de la vida de la organización y puede aplicarse a cualquier actividad, incluyendo la toma de decisiones a todos los niveles [14] (traducción oficial). La norma ISO 31000:2018 establece un conjunto de principios que se deben satisfacer para que la gestión del riesgo sea eficaz; recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada un marco de trabajo cuyo objetivo sea integrar el proceso de gestión del riesgo en los procesos de gobierno, de estrategia y de planificación, de gestión y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización. Esta norma puede ser utilizada por cualquier entidad pública o privada, organizaciones sin ánimo de lucro, asociaciones, grupos o individuos. Los principios básicos de la gestión del riesgo que se describen en la norma ISO 31000 corresponden a: crear y proteger el valor, es una parte integral de todos los procesos de la organización, es parte de la toma de decisiones, trata explícitamente la incertidumbre, es sistémica, estructurada y oportuna, se basa en la mejor información disponible, es adaptable, integra los factores humanos y culturales, es transparente y

participativa, es dinámica, iterativa, responde a los cambios y facilita la mejora continua de la organización. Es así, como el análisis de riesgos informáticos pasa a ser una parte fundamental en la administración de la seguridad, permitiendo algunos beneficios, tal como, identificar los puntos más débiles de la estructura de TI que da soporte a los procesos críticos de la organización. Igualmente, además de ser una guía de selección de medidas de protección de costo adecuado, determina dónde es necesario contar con esquemas de recuperación de desastres y continuidad de negocio y permite realizar políticas de seguridad mejor adaptadas a las necesidades de la organización [11].

b. Selección de la Metodología para el marco de Gestión de Riesgos

Teniendo en cuenta las metodologías anteriormente mencionadas, se realiza una tabla resumen (Tabla 3-6), donde se identifican las principales características, ventajas y desventajas de cada una de las normas.

Tabla 3-6 Matriz comparativa Metodologías de Riesgos, Características, Ventajas y Desventajas

Metodología	Características Principales	Ventajas	Desventajas
OCTAVE	Evalúa cada riesgo de seguridad específico para la información y establece propuesta que permite desarrollar el plan de mitigación. Hace una subdivisión de los activos en dos: 1. Sistemas 2. Personas.	• Comprende procesos relacionados con el análisis, observación y gestión sobre los riesgos • Involucra a los trabajadores en todos los niveles de la organización. • Es muy completa al involucrar cada proceso, departamentos, recursos, activos, las amenazas identificadas, al igual que las salvaguardas como elementos de análisis.	• Solo se puede aplicar en pequeñas y medianas empresas. • No presenta compatibilidad con estándares. • Se basa en demasiados documentos para analizar riesgos. • No define claramente los activos de información • Requiere de conocimientos técnicos para su implementación
MEHARI	Es principalmente un procedimiento de sistema de auditoria que permite la evaluación de riesgos, realiza un completo análisis de los riesgos en los sistemas de información.	• Usa un modelo cuantitativo y cualitativo para el análisis de riesgos. • Evalúa y logra la disminución de riesgos de acuerdo con el tipo de empresa • Particulariza el trabajo • Permite detectar vulnerabilidades mediante las auditorias	• Solo se enfoca en los pilares de confidencialidad, disponibilidad e integridad. • La estimación acerca del impacto de los riesgos sobre los activos se realiza en el proceso de evaluación y gestión.

Metodología	Características Principales	Ventajas	Desventajas
MAGERIT	Realiza la implementación del proceso para la gestión de riesgos tomando como referencia que, cada órgano de administración y control tome decisiones, Integrando cada riesgo que puede llegar a derivarse por el uso de cada tecnología de la información,	• Comprende en su modelo el análisis y la gestión del riesgo. • Es metódica. • Realiza identificación de activos. • No requiere actualización para su uso. • Se encuentra muy bien documentada en lo que se refiere al uso de recursos de información, tipos de activos y sus amenazas.	• Requiere ser muy metodológico para su implementación. • Tiene algunas debilidades a la hora de realizar inventario y establecimiento de políticas. • Se centraliza mucho sobre activos.
NISP SP 800 - 30	En esta se exponen un agregado de sugerencias, recomendaciones y operaciones con miras a la correcta implementación de una gestión de riesgos, la cual sea parte fundamental en todo lo que se realice para la seguridad de la información.	• Bajo costo para su implementación. • Posee herramientas de mitigación y valoración en riesgos. • Proporciona mejora a la administración partiendo de aquellos informes o resultados que se han obtenido del análisis por cada riesgo identificado.	• No tiene contemplados procesos, dependencias o activos como elementos de análisis.

Metodología	Características Principales	Ventajas	Desventajas
ISO 27005:2018	proporciona las directrices para la gestión de riesgos de seguridad de la información, es compatible con los conceptos generales especificados en la norma ISO / IEC 27001 y está diseñado para ayudar a la aplicación satisfactoria de seguridad de la información basado en un enfoque de gestión de riesgos.	• Proporciona una guía para las empresas sobre cómo sortear estas exigencias al mismo tiempo que proporciona un marco de trabajo para gestionar de forma efectiva los riesgos relacionados con la seguridad de la información. • Es complementaria a la ISO/IEC 27001:2013, que proporciona los requisitos de los sistemas de gestión de seguridad, • Se actualizo recientemente la nueva versión de ISO/IEC 27005 para estar en sintonía con ISO/IEC 27001 y de este modo asegurar el cumplimiento de las exigencias de los Sistemas de Gestión certificados y auditados	• La norma ISO 27005 no facilita una metodología concreta de Análisis de Riesgos, sino que describe mediante sus cláusulas el proceso recomendado de análisis incluyendo las fases que lo conforman. • El nuevo estándar no se adentra en la gestión de estos, sino que se queda en un marco declarativo de determinados riesgos, y dicho marco se enlaza con un ciclo PHVA (planificar, hacer, verificar y actuar) para revisar dichos riesgos.

Metodología	Características Principales	Ventajas	Desventajas
ISO 31000:2018	Proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto. proporciona un enfoque común para gestionar cualquier tipo de riesgo, considera el riesgo como un elemento generador de valor porque ayuda a alcanzar los objetivos mediante un pensamiento basado en riesgo para la toma de decisiones.	• Mejora la eficiencia operativa. • Tiene una mejor gobernabilidad interna de la organización. • Aumentar la confianza de las partes externas. • Mejora el rendimiento y la sostenibilidad. • Acentúa la calidad. • Reduce los costes • La disminución de incidentes inesperados. • Mayor control sobre la gestión empresarial y la toma de decisiones.	• La gestión del riesgo está basada en los principios, el marco de referencia y el proceso descritos en este documento, estos componentes podrían existir previamente en toda o parte de la organización, sin embargo, podría ser necesario adaptarlos o mejorarlos para que la gestión del riesgo sea eficiente, eficaz y coherente

Fuente: Elaboración propia.

Teniendo en cuenta el análisis presentado de las metodologías revisadas para la gestión de riesgos y los criterios de comparación establecidos, se elige trabajar conjuntamente en las metodologías ISO 27005:2018 y la ISO 31000:2018 apoyados principalmente en que:

- Usan el mismo framework y esquema de procesos para la gestión de riesgos.
- Permite gestionar los riesgos de manera sistémica, en la organización vinculándose desde el logro de los objetivos y las estrategias definidas y se adapta a la forma de trabajo de la empresa.
- Ayuda a que se tome conciencia por parte de los líderes en los diferentes niveles de gestión de la organización, acerca de los riesgos que desde el nivel estratégico, táctico y operativo existen en la organización y su relación con los procesos, activos, ciber activos, actividades y recursos, que pueden impactar de manera significativa las operaciones y el entorno.
- Es posible alinear los alcances de las 2 metodologías con el nivel estratégico y táctico de la organización con su nivel operativo dándole foco en los activos y ciber activos relacionados con las tecnologías.
- Es posible evidenciar y soportar los requerimientos mínimos del servicio con foco en la disponibilidad del servicio a través de los diferentes elementos que constituyen las normas en su enfoque PHVA.
- Permite que la empresa esté preparada para las diferentes auditorías tanto internas como externa e incluso mantener los estándares de cumplimiento y certificaciones si es del caso.

2) <u>Integración de las Metodología seleccionadas (Riesgos, Continuidad, Crisis y Resiliencia)</u>

Utilizando la estructura de alto nivel definida por ISO y los relacionamientos detallados de las estructuras, procesos y anexos, se puede afirmar que es posible realizar una integración de los estándares ISO/IEC 31000 e ISO/IEC 27005, ver Tabla 3-7, lo que facilitará su relación con los requerimientos mínimos del servicio establecidos en el Objetivo específico 1 de esta investigación, manteniendo la integralidad del abordaje de la gestión de riesgos organizacional partiendo del nivel estratégico y táctico y su relacionamiento a nivel operativo (Tabla 3-7).

Tabla 3-7. Matriz Consolidación Estructura Alto Nivel Vs ISO 31000 – ISO 27005

Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	ISO 31000	ISO 27005
P	Identificación	Contexto Liderazgo Planificación	5.2 Liderazgo y compromiso, 5.4.1 Comprensión de la organización y de su contexto, 5.4.2 Articulación del compromiso con la gestión del riesgo, 5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización, 5.4.4 Asignación de recursos, 5.4.5 Establecimiento de la comunicación y la consulta, 5.5 Implementación, 5.6 Valoración, 6 Proceso, 6.1 Generalidades, 6.2 Comunicación y consulta, 6.3 Alcance, contexto y criterios, 6.3.1 Generalidades, 6.3.2 Definición del alcance, 6.3.3 Contextos externo e interno, 6.3.4 Definición de los criterios del riesgo	6 Descripción general del proceso de gestión del riesgo de seguridad de la información 7 Contexto establecimiento, 7.1 Consideraciones generales, 7.2 Criterios básicos, enfoque de gestión de riesgos 7.2.1, 7.2.2 criterios de evaluación de riesgos, 7.2.3 criterios de impacto, 7.2.4 criterios de aceptación del riesgo, 7.3 Alcance y límites, 7.4 Organización para la gestión del riesgo de seguridad de la información,

Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	ISO 31000	ISO 27005
H	Proteger Detectar Responder	Soporte Operación	6.4 Evaluación del riesgo, 6.4.1 Generalidades, 6.4.2 Identificación del riesgo, 6.4.3 Análisis del riesgo, 6.4.4 Valoración del riesgo, 6.5 Tratamiento del riesgo, 6.5.1 Generalidades, 6.5.2 Selección de las opciones para el tratamiento del riesgo, 6.5.3 Preparación e implementación de los planes de tratamiento del riesgo,	8. evaluación de riesgos 8.1 Descripción general de la evaluación de riesgos de seguridad de información, 8.2 identificación Riesgo, 8.2.1 Introducción a la identificación de riesgos, 8.2.2 Identificación de los activos, 8.2.3 Identificación de las amenazas, 8.2.4 Identificación de los controles existentes, 8.2.5 Identificación de las vulnerabilidades, 8.2.6 Identificación de las consecuencias, 8.3 análisis Riesgo, 8.3.1 metodologías de análisis de riesgos, 8.4 evaluación Riesgo, 9 tratamiento de los riesgos de seguridad Información 9.1 Descripción general del tratamiento del riesgo, de seguridad Información, 10 Información de la aceptación de riesgos de

Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	ISO 31000	ISO 27005
				seguridad, 11 Información de comunicación y consulta de riesgos de seguridad
V	Recuperar	Evaluación Desempeño	6.6 Seguimiento y revisión	12 Información de seguimiento y examen de riesgos de seguridad, 12.1 Seguimiento y revisión de los factores de riesgo
A		Mejora	5.7 Mejora, 5.7.1 Adaptación, 5.7.2 Mejora continua	12.2, control de la gestión de riesgos, revisión y mejora

Fuente: Elaboración propia.

Igualmente se puede decir que la diferencia básica entre las normas analizadas es que ISO/IEC 31000 se enfoca en la Gestión de riesgos de manera integral y genérica, mientras que la ISO/IEC 27005 lo hace a nivel de la gestión de Riesgos en la Seguridad de la información, identificando los activos, las vulnerabilidades, las amenazas y los impactos a los que están expuestos y los controles existentes. Lo interesante de estas diferencias es que se puede integrar la gestión de la seguridad de la información y tecnologías a los objetivos y metas de nivel estratégico de la organización.

En cuanto al marco de gestión de continuidad, crisis y resiliencia, se decidió trabajar por parte del equipo de investigación con los siguientes estándares y referentes de buenas prácticas a nivel internacional:

- ISO 22301:2019 Sistemas de gestión de la continuidad del negocio
- BS 11200:2014 Gestión de crisis. Orientaciones y buenas prácticas
- ISO 22316: Resiliencia organizacional. Principios y atributos.
- BS 65000: Guía para la Resiliencia Organizacional

La ISO 22301:2019 es una normativa internacional para la implementación de Sistemas de Gestión de la Continuidad del Negocio (SGCN). Fue creada después de la gran demanda internacional que obtuvo el estándar británico BS 25999-2 del año 2007. Su principal función es la de proporcionar un marco de actuación para que las empresas puedan mitigar los daños que una situación de crisis puede llegar a causar. busca igualmente minimizar los riesgos y consecuencias que una organización se expone de manera habitual o imprevista, a partir de la creación de planes de continuidad.

Su articulación con la gestión de incidentes permitirá fortalecer la prevención de incidentes de seguridad asociados a escenarios de riesgos disruptivos, a partir de una adecuada evaluación de riesgos, determinación del impacto que su materialización puede causar en el negocio, selección de las estrategias y soluciones de continuidad de negocio, elaboración de Planes de continuidad de negocio complementarios a la gestión de incidentes y Diseño de programas de entrenamiento y pruebas para la mejora continua, entre otros elementos. La BS 11200:2014 Gestión de crisis, es una guía que busca proporcionar a las organizaciones una orientación sobre cómo abordar la gestión de crisis en la organización y ayudar a la

alta dirección a planificar, establecer, operar, mantener y mejorar su capacidad de gestión a partir de la mejora continua.

Su articulación con la gestión de incidentes permite mejorar el alcance de los análisis de escenarios de riesgos determinando cuales pueden desencadenar una situación de crisis en la organización y su entorno asociado, establecer un equipo y capacidades de respuesta sostenible en el tiempo por medio de la implementación de unos procesos y procedimientos diseñados para su gestión, utilización de unos mecanismos de comunicación tanto interna como externa y de un programa de formación, entrenamiento y pruebas para su actualización.

En cuanto a la Resiliencia se cuenta con la BS 65000, es una guía que proporciona una visión general de la capacidad de recuperación de una organización describiendo los fundamentos necesarios para su abordaje e implementación y la ISO 22316, establece los principios, atributos y actividades que una organización debe considerar para mantener y mejorar su resiliencia.

Su aporte en la gestión de incidentes será fortalecer el entendimiento de las capacidades a establecer e implementar en la organización para una adecuada recuperación y transformación desde el aprendizaje e innovación, luego de la materialización de un incidente.

A continuación, la Tabla 3-8, se presentan los elementos claves de cada mejor práctica utilizada para el referenciamiento siguiendo la estructura de alto nivel definida por la ISO alineados con el enfoque PHVA y el marco de NIST.

Tabla 3-8. Referenciamiento de mejores prácticas a nivel de riesgos, continuidad, crisis y resiliencia siguiendo un enfoque PHVA

Etapas - Fases de un Evento / Incidente / Siniestro	**Ciclo de Gestión - PHVA**	**Marco de Referencia NIST**	**Estructura de Alto Nivel ISO**	**Riesgos**	**Continuidad**	**Crisis**	**Resiliencia**
Antes, durante, Después	Planear, Hacer, Verificar, Ajustar	Identificar, Proteger, Detectar, Responder, Recuperar,	Objeto y Campo de Aplicación, Referencias Normativas, Términos y Definiciones, Contexto de la Organización, Liderazgo, Planificación, Apoyo, Operación, Evaluación del Desempeño, Mejora				
Antes	Planeación	Identificación	Contexto de la Organización (Entendimiento de la Organización y su contexto, Necesidades y Expectativas de los Grupos de interés, Alcance del Sistema de	5.4.1 Comprensión de la organización y de su contexto 5.4.2 Articulación del compromiso con la gestión del riesgo 6.1 Generalidades	4.4 Sistema De Gestión De Continuidad De Negocio 6.2.1 Establecer Los De Objetivos Para La Continuidad De Negocio 6.2.2 Determinar Los Objetivos Para La Continuidad De Negocio 4. Contexto De La Organización	3. Crisis Gestión: Base De Conceptos, Principios Y Desarrollo De Una Capacidad 3.1 La Comprensión De Las Crisis Y La Mejor Manera De Administrarlos	4 Principios 4.1 Generalidades 4.2 Principios generales de la resistencia organizativa 4.3 Establecimiento del contexto 4.4 Mandato y compromiso

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
			Gestión, Sistema de Gestión y sus Procesos)	6.2 Comunicación y consulta 6.3 Alcance, contexto y criterios 6.3.1 Generalidades 6.3.2 Definición del alcance 6.3.3 Contextos externo e interno 6.3.4 Definición de los criterios del riesgo	4.1 Comprensión De La Organización Y Su Contexto 4.2 Comprensión De Las Necesidades Y Expectativas De Las Partes Interesadas 4.2.2 Requisitos Legales Y Reglamentarios 4.3 Determinación Del Alcance Del Sistema De Gestión De Continuidad De Negocio 4.3.2 Alcance Del Sistema De Gestión De Continuidad De Negocio 4.3.3 Exclusiones Del Alcance	3.2 Los Posibles Orígenes De La Crisis 3.3Implicaciones De La Naturaleza De Las Crisis	4.5 Principios relacionados con el diseño del marco 4.6 Principios relativos a la aplicación de las medidas 4.7 Principios relacionados con la gestión del cambio, la vigilancia, el examen y el mejoramiento continuo 5.2 Ser informado (conocimiento de la situación)

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
					4.4 Sistema De Gestión De Continuidad De Negocio 6.1.1 Determinación De Los Riesgos Y Las Oportunidades.		5.2 Establecer el contexto 5.2.1 Generalidades 5.2.2 Contexto interno 5.2.3 Contexto externo 5.2.4 Gestión del riesgo
			Liderazgo (Liderazgo y Compromiso, Política, Roles, Responsabilidades, Autoridad y Funciones)	5.4.3 Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización	5.1 Liderazgo y compromiso 5.1.2 Alta dirección 5.1.3 Otros roles directivos 5.2 Política 5.2.1 Establecimiento de la política de continuidad de negocio	5. Liderazgo En La Crisis 5.1 El Cmt (Véase Sección 4) 5.2 Compás 5.3 Comprender Los Desafíos Del	5.3 Mandato y compromiso 5.4 Diseño del marco 5.4.1 Establecimiento de una política de resistencia 5.4.2 Rendición de cuentas

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
					5.2.2 Comunicación de la política de continuidad de negocio de la organización 5.3 Roles, responsabilidades y autoridades 6.2.2 Determinar los objetivos para la continuidad de negocio	Liderazgo En Las Crisis 5.4 Funciones Claves Del Liderazgo 6. Toma De Decisiones Estratégicas En La Crisis 6.1 Toma De Decisiones 6.2 ¿Cómo Se Toman Las Decisiones? 6.3 ¿Por Qué Es Desafiante La Toma	6.2 Propósito e intención 6.3 Cualidades y características del liderazgo 6.4 Comportamientos organizativos (cultura y comportamiento, necesidad de revisar la labor anterior) 5 Fomento de la resiliencia 5.1 General

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
						De Decisiones En Una Crisis? 6.4 Dilemas, Retraso En La Decisión Y Evitación De La Decisión 6.5 Problemas En La Toma De Decisiones 6.6 Toma Eficaz De Decisiones En La Crisis	

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
			Planificación (Acciones para Dirigir y Atender los Riesgos asociados a las Amenazas y Oportunidades, Objetivos y Planificación para alcanzarlos, Planificación de Cambios)	6.4 Evaluación del riesgo 6.4.1 Generalidades 6.4.3 Análisis del riesgo 6.4.4 Valoración del riesgo 6.5 Tratamiento del riesgo 6.5.1 Generalidades 6.5.2 Selección de las opciones para el tratamiento del riesgo	6. Planificación 6.1 Acciones Para Abordar Riesgos Y Oportunidades 6.1.1 Determinación De Los Riesgos Y Las Oportunidades 6.1.2 Abordar Riesgos Y Oportunidades 6.3 Planificación De Los Cambios En El Sistema De Gestión De Continuidad De Negocio 4.4 Sistema De Gestión De Continuidad De Negocio 8.2 Análisis De Impacto En El Negocio Y Evaluación De Riesgos	4.Construcción De La Capacidad Para La Gestión De Crisis 4.1Introducción 4.4Anticipar Y Valorar 4.5 Preparar 4.5.1 Generalidades 4.5.2 Plan De Gestión De Las Crisis 4.5.3 Gestión De La Información Y Conocimiento Situacional 4.5.3.1 Gestión De La Información	5.4.3 Integración en los procesos de organización 6.7 Procesos de gestión empresarial e integración 5.5 Desarrollar la capacidad de adaptación 5.6 Fortalecer la organización 5.6.1 La organización debería implementar medidas específicas que fortalecen su capacidad para hacer

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
				6.5.3 Preparación e implementación de los planes de tratamiento del riesgo	8.2.2 Análisis De Impacto E En El Negocio (Bia, Por Sus Siglas En Inglés) 8.2.3 Evaluación Del Riesgo 8.3 Estrategias Y Soluciones De Continuidad De Negocio 8.3.1 Generalidades 8.3.2.1 Generalidades 8.3.2 Identificación De Estrategias Y Soluciones 8.3.2.2 Protección De Las Actividades Priorizadas	4.5.3.2 Conocimiento Situacional 4.5.3.3 Composición Y Expectativas Del Equipo De Gestión De La Crisis 7.4.3Monitorización De Los Medios De Comunicación 7.5Desarrollo De Una Estrategia Para Las Comunicaciones En La Crisis	frente a acontecimientos perturbadores 5.7 Validar y revisar 6 Evaluación de la capacidad de recuperación de una organización 6.1 Madurez y medición modelo de madurez para la resiliencia organización Nivel de madurez notas

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
Durante	**Hacer**	**Proteger, Detectar, Responder**	**Soporte** (Recursos, Competencias, Conciencia, Comunicación, Información Documentada)	5.4.4 Asignación de recursos 5.4.5 Establecimiento de la comunicación y la consulta 6.2 Comunicación y consulta	7.1.1 Generalidades 7.1.2 Recursos del BCMS 7.2 Competencias 7.4 Comunicación 7.5 Información documentada 7.5.1 Generalidades 7.5.3 Control de la información documentada 7.5.3.1 Acceso a la información documentada 7.5.3.2 Tipos de control 8.4.4.5 Comunicaciones	7.Comunicación En La Crisis 7.1Introducción 7.2Preparación Previa A La Crisis 7.3Gestión De La Reputación Y Las Partes Interesadas 7.4Roles Claves 7.4.1Generalidades 7.4.2Portavoz	5.4.4 Recursos 5.4.5 Establecimiento 5.4.6 Establecimiento de mecanismos externos de comunicación y notificación 6.5 Conocimiento e información

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
			Operación (Planificación y Control Operacional, Planificación y Preparación de Respuesta a Incidentes, Emergencias, Contingencias y Desastres, Determinación de Requerimientos de Productos y Servicios, Diseño y Desarrollo de Productos y Servicios, Control de Productos No Conformes, Producción y Prestación del Servicio, Control de Salidas del Proceso)		8.1 Planificación y control operacional 8.1.1 Generalidades 8.1.2 Gestión de continuidad de negocio 7.3 Toma de conciencia 8.3.4 Requisitos de recursos 8.3.4.1 Generalidades 8.3.4.2 Personas 8.3.4.2.1 Generalidades 8.3.4.2.2 Respuesta al incidente 8.3.4.4 Edificios, lugares de trabajo y servicios asociados 8.3.4.5 Equipo y consumibles 8.3.4.6 Sistemas de las TIC	3.4Recuperación De Una Crisis: Una Parte Integral De La Gestión De La Crisis 4.6Responder (El Cmt En Acción) 4.7Recuperar	5.5 Aplicación de las medidas 5.5.1 Aplicación del marco de gestión de riesgos Al aplicar el marco de resiliencia institucional 5.5.2 Aplicación de las medidas de gestión de riesgos y mejora de la capacidad de recuperación de la organización

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
					8.3.4.7 Transporte y logística 8.3.4.8 Finanzas 8.3.4.9 Socios y cadena de suministro 8.3.5 Implementación de soluciones 8.4.4 Planes de continuidad de negocio 8.4.4.1 Generalidades 8.4.4.2 Cobertura 8.4.4.2.1 Generalidades 8.4.4.2.2 Responder a los incidentes 8.4.4.4 Gestión de incidentes/estratégica		

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
					8.4.4.7 Salvamento y seguridad 8.4.4.8 Reanudación de las actividades priorizadas 8.4.4.9 Sistemas TIC 8.4.5 Recuperación 8.5 Programa de ejercicios 8.5.1 Generalidades 8.5.2 Diseño del programa de ejercicios 8.5.3 Ejecutar los planes de continuidad de negocio		

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
Después	**Verificar**	**Recuperar**	**Evaluación del Desempeño** (Seguimiento, Medición, Análisis, Evaluación del Cumplimiento, Revisión por la Dirección)	6.6 Seguimiento y revisión 6.7 Registro e informe	8.6 Evaluación De La Documentación Y Las Capacidades De Continuidad De Negocio 8.6.1 Generalidades 8.6.2 Medición De La Eficacia 8.6.3 Resultados 9. EVALUACIÓN DEL DESEMPEÑO 9.1 Seguimiento, Medición, Análisis Y Evaluación 9.1.1 Generalidades 9.1.2 Retención De Evidencia 9.1.3 Evaluación Del Desempeño 9.2 Auditoría Interna	8.Entrenamiento, Ejercitación Y Aprendizaje A Partir De Las Crisis 8.1Desarrollo De Las Personas Y Práctica De Las Disposiciones Para La Gestión De La Crisis 8.2Estrategia De Aprendizaje Y Desarrollo 8.3Entrenamiento Para La Gestión De Las Crisis	5.6 Vigilancia y examen del marco

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
					9.2.1 Generalidades 9.2.2 Programa(S) De Auditoría 9.3 Revisión Por La Dirección 9.3.1 Generalidades 9.3.2 Entradas De La Revisión Por La Dirección 9.3.3 Salidas De La Revisión Por La Dirección	8.4Desarrollo De Destrezas 8.5Métodos De Instrucción 8.6Puesta En Práctica De Las Disposiciones Para La Gestión De La Crisis 8.7Tipos De Ejercicios 8.8Actividad De Ejercicio Posterior A La Crisis	
Después	**Ajustar**	**Recuperar**	**Mejora** (No Conformidades y	5.7 Mejora 5.7.1 Adaptación	9.3.3.1 Mejora Del BCMS 9.3.3.2 Conservación De Información Documentada	4.8 Revisar Y Aprender	5.7 Mejora continua y gestión del cambio 6 Atributos

Etapas - Fases de un Evento / Incidente / Siniestro	Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO	Riesgos	Continuidad	Crisis	Resiliencia
			Acciones Correctivas, Mejora Continua)	5.7.2 Mejora continua	10. Mejora 10.1 No Conformidad Y Acción Correctiva 10.1.1 Generalidades 10.1.2 Ocurrencia De La No Conformidad 10.1.3 Conservación De Información Documentada 10.2 Mejora Continua	8.8Actividad De Ejercicio Posterior A La Crisis	6.1 Generalidades 6.6 Aprendizaje 6.8 Evaluación del rendimiento 6,9 Capacidad de adaptación 6.10 Innovación 6.11 Vigilancia 6.12 Capital social, confianza y lealtad

Fuente: Elaboración Propia.

Como se puede observar en los Resultados del referenciamiento de mejores prácticas a nivel de riesgos, continuidad, crisis y resiliencia siguiendo un enfoque PHVA, muchos de los elementos claves son fácilmente identificables con los componentes de la estructura de alto nivel, necesarios para articular con la respuesta corporativa. Sin embargo, en el componente de Operación, no se observan elementos en la norma de referencia.

Igualmente se observa en algunos componentes asociados a la respuesta corporativa de referencia, que las normas analizadas son limitadas en sus aportes. En estos puntos es importante reforzar desde el trabajo de investigación para que en el procedimiento no queden esos vacíos y/o deficiencias.

3.2.2 Actividad 2. Revisar los procedimientos de respuesta a nivel corporativo

A continuación, en relación con la articulación de la respuesta corporativa con los elementos claves identificados en la gestión de riesgos, continuidad, crisis y resiliencia, se realizaron búsquedas en internet y otras fuentes, de algunos tipos de respuesta corporativa a eventos, incidentes y crisis. Estas búsquedas permitieron determinar 9 casos prácticos que han utilizado el mecanismo de respuestas corporativas a eventos, incidentes y crisis de tipo empresarial y como se encontraron en cada uno los elementos de referencia tanto del PHVA, como de las funciones de NIST y de la estructura de alto nivel desarrolladas en este proyecto, insumos importantes para determinar el alcance del Protocolo de respuesta corporativa a crear y proponer. Lo que se espera con estos casos es identificar los elementos claves presentes en cada uno de los casos de referencia para tener identificados los insumos mínimos a tener en cuenta en el protocolo de respuesta corporativa (Tabla 3-9).

a. Listado de los casos de referencia analizados:

- Caso 1 “Diseño de un modelo de ciberseguridad para dispositivos móviles en el sector empresarial”.
- Caso 2 “Desde un enfoque de controles basado en la ISO 27002:2013.”

- Caso 3 “Desde un enfoque de continuidad del negocio basado en las normas de referencia ISO 22301, 22313, 22317, NIST 800 – 34”.
- Caso 4 “Desde la implementación del NIST CYBERSECURITY FRAMEWORK”.
- Caso 5 “Desde la Implementación de un plan de prevención, preparación y respuesta ante emergencia, de acuerdo con el Ministerio de Trabajo a través Decreto 1072 de 2015”.
- Caso 6 “Desde la gestión estratégica del riesgo y su importancia en las buenas prácticas empresariales”.
- Caso 7 “Desde una guía para el manejo de respuesta empresarial ante situaciones de Crisis”.
- Caso 8 “Desde una propuesta de investigación a la respuesta organizativa a la adversidad: fusión de las corrientes de investigación sobre gestión de crisis y resiliencia”.
- Caso 9 “Desde las guías, a partir de la BS 11200: 2014 – GTC DE 029/16 – Investigaciones de Crisis y Gestión de Crisis”.

Tabla 3-9. Relacionamiento de los Elementos de la Estructura de Alto Nivel con los Casos de Respuesta Corporativa analizados siguiendo un enfoque PHVA

Ciclo de Gestión - PHVA	Marco de Referencia NIST	Estructura de Alto Nivel ISO Riesgos – Continuidad – Crisis - Resiliencia	Caso 1	Caso 2	Caso 3	Caso 4	Caso 5	Caso 6	Caso 7	Caso 8	Caso 9
P	Identificación Proteger	Contexto (C) Liderazgo (L) Planificación (P)	C L P	L P	L P	c P	P	L P	L P	L P	c P
H	Detectar Responder	Operación (O) Soporte (S)	S O	S O	O	O	S O	O	S O		S O
V	Recuperar	Evaluación Desempeño (E)	E	E	E	E	E	E	E		E
A		Mejora (M)	M	M		M		M			M

C: Contexto S: Soporte L: Liderazgo P: Planificación O: Operación E: Evaluación Desempeño M: Mejora

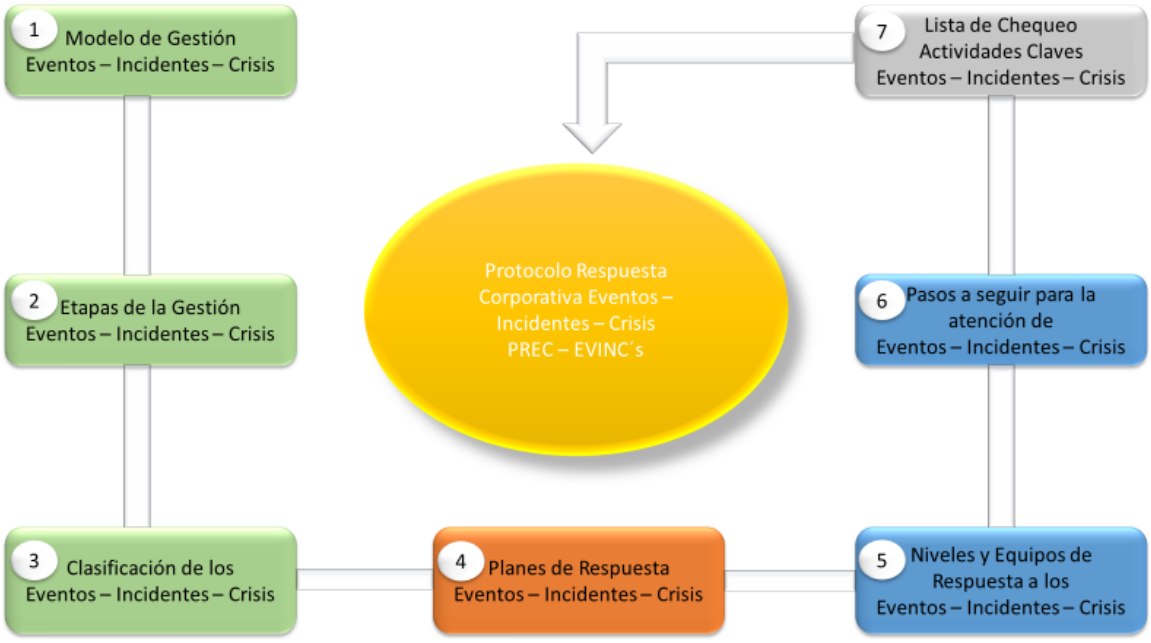
Fuente: Elaboración Propia.

En el Anexo 5: Matriz Rel Elem Claves con Resp Corp se presenta la matriz de relacionamiento de los elementos claves vs la respuesta corporativa que permiten observar la explicación de cómo responde a cada elemento identificado de la estructura de alto nivel, insumo clave para el objetivo específico 4 de este trabajo de investigación.

Esta matriz evidencia cómo la respuesta corporativa a eventos, incidentes y crisis, de los 9 casos analizados, mantiene una alineación con los diferentes elementos de la estructura de alto nivel, que a su vez nos permitirá relacionar los elementos claves de riesgos, continuidad, crisis y resiliencia, insumo fundamental para el procedimiento de gestión de incidentes y su alineación con la organización.

A partir de los resultados y como parte de la investigación, se propone un protocolo de respuesta corporativa (Figura 3-16) que permite la atención de los eventos, incidentes y crisis de acuerdo a una gradualidad de los efectos y consecuencias, siguiendo un modelo de gestión, con unas etapas definidas que a partir de una clasificación se pudieran activar unos planes y recursos, teniendo en cuenta una estructura temporal de gestión crisis y unos pasos definidos para su atención, recuperación y vuelta a la normalidad.

Figura 3-16. Mapa conceptual del Protocolo de Respuesta Corporativa de Eventos – Incidentes - Crisis



Fuente Elaboración propia

Como se observa en el mapa conceptual (Figura 3-16), el protocolo de respuesta corporativa de eventos, incidentes y crisis (PREC – EVINC´s), propuesto desde esta investigación, se compone de los siguientes elementos:

1) Modelo de Gestión (E-I-C): Muestra las fases y etapas por las que se debe transitar para gestionar de manera pertinente la ocurrencia de cualquier evento, incidente o crisis en la organización, sin importar el origen de la situación.

2) Fases y Etapas de la Gestión (E-I-C): Son básicamente los momentos que, desde la gestión de cualquier evento, incidente o crisis en la organización, sin importar el origen de la situación, se debe seguir para su atención. Se conocen como la fase de la Precrisis (antes de la ocurrencia), se compone de las etapas de Planeación y Preparación, luego está la fase de la Crisis (durante la ocurrencia), se compone de las etapas de Alerta y Respuesta, y está la fase de la Pos crisis (posterior a la ocurrencia) y se compone de las etapas de seguimiento y vuelta a la normalidad.

3) Clasificación de los Eventos, Incidentes y Crisis: Corresponde a la clasificación que de acuerdo con la intensidad y gradualidad de los efectos que los eventos, incidentes y crisis pueden generar en la empresa y su entorno. Se clasifican así; 1) Nivel de Gravedad Leve, 2) Nivel de Gravedad Moderada, medio y 3) Nivel de gravedad Alta o critica.

4) Planes de Respuesta (E-I-C): Se conocen así a los diferentes planes, protocolos, guías y recursos necesarios para la atención de un evento, incidente o crisis. De acuerdo con el nivel de gradualidad de los efectos, se deberán activar en la organización

5) Niveles y Equipos de respuesta (E-I-C): Se conocen así a los tres niveles de la organización y equipos de trabajo disponibles para su atención y gestión. Esta el Nivel 1 Operativo, ubicado en la instalación afectada con equipos de respuesta de tipo local. Esta el Nivel 2 Táctico, ubicado en la organización afuera del área o dependencia afectada y se compone de los equipos de apoyo y soporte de la organización. Y ésta el Nivel 3 Estratégico, compuesto por el Equipo Directivo o Alta Dirección, se le conoce también como el Equipo Gerencial de Crisis.

6) Pasos para seguir en la Gestión (E-I-C): Se llama así a las actividades básicas que se deben emprender en la atención de todo Evento, Incidente o Crisis en la organización. Busca dar claridad a todos los involucrados en la actuación a seguir. Los pasos son en su orden; PASÓ 1 - Comunicar Evento, PASÓ 2 - Activar cadena de llamadas, PASÓ 3 - Evaluar situación, PASÓ 4 - Atención del evento y PASÓ 5 - Cierre del evento.

7) Lista de Chequeo (E-I-C): Como su nombre lo indica son una lista de actividades mínimas a tener en cuenta en las diferentes fases, etapas y pasos dentro de la gestión ante la ocurrencia de un evento, incidente o crisis en una organización.

b. Descripción de los componentes

En el Anexo 6: Protocolo Respuesta Corporativa Eventos Incidentes Crisis se detalla cada uno de los componentes del modelo.

3.3 Fase 3: Gestión de incidentes de seguridad

En esta fase se establecieron las etapas para tener en cuenta dentro del procedimiento de gestión de incidentes, con lo cual, se revisaron las buenas prácticas existentes a nivel de modelos de gestión de respuesta a nivel de TI y TO.

3.3.1 Actividad 1. Revisar los modelos de respuesta de incidentes de seguridad – ciberseguridad

En ese sentido, se realizó un referenciamiento a nivel nacional e internacional de los modelos, estándares y buenas prácticas en gestión de incidentes de ciberseguridad a nivel de TI y TO, con el fin de poder caracterizar las principales etapas a tener en cuenta en la respuesta a incidentes y de esta manera realizar la articulación de los requerimientos mínimos del servicio con los elementos a potenciar desde el marco de referencia de gestión de riesgos, continuidad, crisis y resiliencia con la respuesta de nivel corporativo ante eventos tecnológicos.

Después de consultar las fuentes secundarias y analizar la información relacionada con el tema objeto de la investigación, se seleccionaron los siguientes referentes internacionales que dan una visión general y son los que le pueden aportar a este proyecto de investigación, brindando los insumos para diseñar el nuevo procedimiento integrado de gestión de incidentes de ciberseguridad alineado con la respuesta corporativa:

a. NIST Cybersecurity Framework: Marco para la mejora de la seguridad cibernética en infraestructuras críticas Versión 1.1, publicado 16/04/2018.
b. Estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide, Agosto 2012
c. MINTIC: Guía para la Gestión y clasificación de Incidentes de Seguridad de la Información, 6/11/2016.
d. INCIBE: Guía Nacional de Notificación y Gestión de Ciber incidentes, publicado el 21/02/2020

e. ISO/IEC 27035 – 1 y 2: Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad – parte 1, principios y parte 2, directrices para planificar y prepararse para la respuesta a incidentes, 11/01/2016.

Para tener un mejor contexto de cada referente se extracta de su contenido lo que está directamente relacionado con la gestión de incidentes de ciberseguridad a nivel de TI y TO, con el fin de poder caracterizar las principales etapas para tener en cuenta en el diseño del nuevo procedimiento, objeto de esta investigación.

a. NIST Cybersecurity Framework: Marco para la mejora de la seguridad cibernética en infraestructuras críticas Versión 1.1, publicado 16/04/2018.

Este Marco ofrece una forma flexible de abordar la seguridad cibernética, lo que incluye el efecto de la seguridad cibernética en las dimensiones físicas, cibernéticas y de personas. Este es aplicable a organizaciones que dependen en la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en tecnología de la 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 puede ayudar a las organizaciones a abordar la seguridad cibernética ya que afecta la privacidad de los clientes, empleados y otras partes.

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 seguridad cibernética. Estos componentes se explican a continuación.

Como el foco es la gestión de incidentes de ciberseguridad, no se entra a explicar los niveles de implementación ni los perfiles del marco y a continuación si se entra en más detalle con el núcleo del marco que nos permite ver cómo está estructurado, que actividades lo

componen y nos brinda información para hacer el comparativo con los otros referentes relacionados con la temática de la investigación.

El Núcleo del Marco: El Núcleo del Marco proporciona un conjunto de actividades para lograr resultados específicos de seguridad cibernética y hace referencia a ejemplos de orientación en cómo lograr dichos resultados. El Núcleo no es una lista de verificación de las acciones a realizar. Este presenta los resultados clave de seguridad cibernética identificados por las partes interesadas como útiles para gestionar el riesgo de seguridad cibernética. El Núcleo consta de cuatro elementos: Funciones, Categorías, Subcategorías y Referencias Informativas.

Figura 3-17. Estructura núcleo del framework de ciberseguridad de la NIST

Fuente: Framework for Improving Critical Infraestructure Cibersercurity V 1.1

Elementos del Núcleo del Marco trabajan juntos en la siguiente manera:

- Las Funciones organizan actividades básicas de seguridad cibernética en su nivel más alto. Estas funciones son: Identificar, Proteger, Detectar, Responder y Recuperar. Las funciones también se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en

seguridad cibernética. Por ejemplo, las inversiones en planificación y ejercicios apoyan la respuesta oportuna y las acciones de recuperación, lo que resulta en un impacto reducido en la prestación de servicios.

- Las Categorías son las subdivisiones de una Función en grupos de resultados de seguridad cibernética estrechamente vinculados a las necesidades programáticas y actividades particulares. Los ejemplos de categorías incluyen "Gestión de activos", "Gestión de identidad y control de acceso" y "Procesos de detección".

- Las Subcategorías dividen aún más una Categoría en resultados específicos de actividades técnicas o de gestión. Proporcionan un conjunto de resultados que, aunque no son exhaustivos, ayudan a respaldar el logro de los resultados en cada Categoría. Algunos ejemplos de subcategorías incluyen "Los sistemas de información externos se catalogan", "Los datos en reposo se protegen" y "Las notificaciones de los sistemas de detección se investigan".

- Las Referencias Informativas son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada Subcategoría. Las referencias informativas presentadas en el Núcleo del Marco son ilustrativas y no exhaustivas. Se basan en la orientación intersectorial a la que se hace referencia con más frecuencia durante el proceso de desarrollo del Marco.

b. Estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide, Agosto 2012

Esta publicación busca ayudar a las organizaciones a mitigar los riesgos de los incidentes de seguridad informática al proporcionar pautas prácticas para responder a los incidentes de manera efectiva y eficiente. Incluye pautas para establecer un programa de respuesta a incidentes efectivo, pero el enfoque principal del documento es detectar, analizar, priorizar y manejar incidentes. Se anima a las organizaciones a adaptar las pautas y soluciones recomendadas para cumplir con sus requisitos específicos de seguridad y misión.

La respuesta a incidentes de seguridad informática se ha convertido en un componente importante de los programas de tecnología de la información (TI). Los ataques relacionados con la ciberseguridad no solo se han vuelto más numerosos y diversos, sino también más dañinos y disruptivos. Con frecuencia surgen nuevos tipos de incidentes relacionados con la seguridad. Las actividades preventivas basadas en los resultados de las evaluaciones de riesgos pueden reducir el número de incidentes, pero no todos los incidentes se pueden prevenir. Por lo tanto, es necesaria una capacidad de respuesta a incidentes para detectar incidentes rápidamente, minimizar las pérdidas y la destrucción, mitigar las debilidades que fueron explotadas y restaurar los servicios de TI. Con ese fin, esta publicación proporciona pautas para el manejo de incidentes, en particular para analizar datos relacionados con incidentes y determinar la respuesta adecuada a cada incidente.

Debido a que realizar la respuesta a incidentes de manera efectiva es una tarea compleja, establecer una capacidad de respuesta a incidentes exitosa requiere una planificación y recursos sustanciales. Monitorear continuamente los ataques es esencial. El establecimiento de procedimientos claros para priorizar el manejo de incidentes es fundamental, al igual que la implementación de métodos efectivos para recopilar, analizar y reportar datos. También es vital construir relaciones y establecer medios de comunicación adecuados con otros grupos internos (por ejemplo, recursos humanos, legales) y con grupos externos (por ejemplo, otros equipos de respuesta a incidentes, aplicación de la ley).

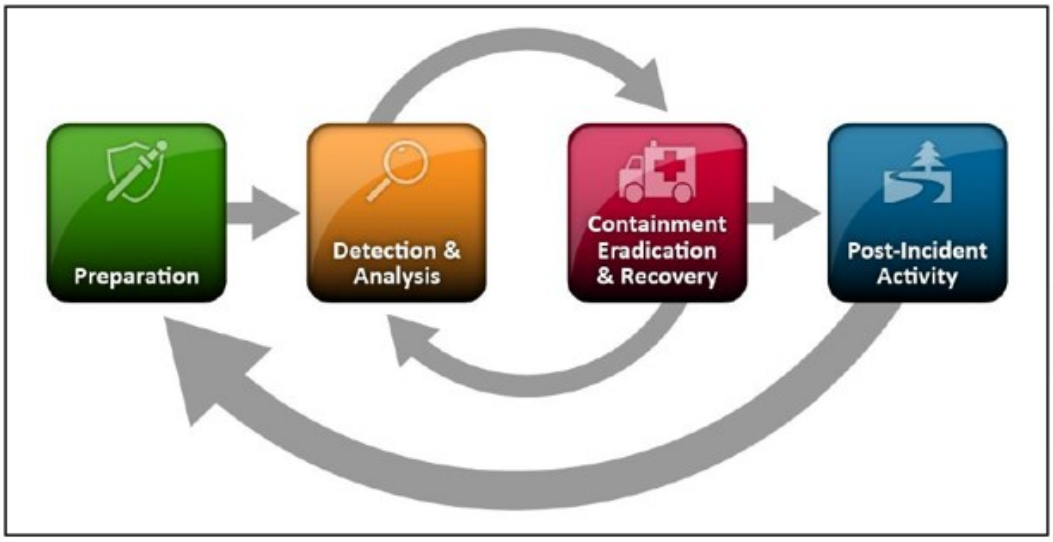
El establecimiento de una capacidad de respuesta a incidentes debe incluir las siguientes acciones:

- Crear una política y un plan de respuesta a incidentes
- Desarrollar procedimientos para realizar el manejo y reporte de incidentes
- Establecer pautas para comunicarse con partes externas con respecto a incidentes
- Seleccionar una estructura de equipo y un modelo de dotación de personal

- Establecer relaciones y líneas de comunicación entre el equipo de respuesta a incidentes y otros grupos, tanto internos (por ejemplo, departamento legal) como externos (por ejemplo, agencias de aplicación de la ley)
- Determinar qué servicios debe proporcionar el equipo de respuesta a incidentes

Esta Figura 3-18 muestra las principales fases del proceso de respuesta a incidentes: preparación, detección y análisis, contención, erradicación y recuperación, y actividad posterior al incidente:

Figura 3-18. Ciclo de vida de la respuesta a incidentes



Fuente: Estándar NIST.SP.800-61r2

Uno de los aspectos más importantes de la coordinación de la respuesta a incidentes es el intercambio de información, donde diferentes organizaciones comparten información sobre amenazas, ataques y vulnerabilidades entre sí para que el conocimiento de cada organización beneficie a la otra.

El intercambio de información sobre incidentes con frecuencia es beneficioso para ambas partes porque las mismas amenazas y ataques suelen afectar a varias organizaciones simultáneamente.

c. MINTIC: Guía para la Gestión y clasificación de Incidentes de Seguridad de la Información, 6/11/2016

Para el desarrollo de esta guía, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre por parte del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide), tomando como base los lineamientos recomendados en Norma la ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes.

Esta guía entrega los lineamientos básicos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para que se puedan integrar los incidentes de seguridad sobre los activos de información, independiente del medio en el que se encuentren.

CARACTERÍSTICAS DE UN MODELO DE GESTIÓN DE INCIDENTES

Esta guía de gestión de incidentes de seguridad de la información plantea una serie de actividades para dar cumplimiento con el ciclo de vida de la gestión y respuesta a un incidente de seguridad (Figura 3-19).

Figura 3-19. Ciclo de vida para la respuesta a Incidentes de seguridad de la información, NIST

Fuente: Guía gestión de incidentes de seguridad de la información – MINTIC

Para definir las actividades de esta guía se incorporaron componentes definidos por el NIST alineados con los requerimientos normativos de la NTC–ISO–IEC 27035-2013.

d. INCIBE: Guía Nacional de Notificación y Gestión de Ciberincidentes, publicado el 21/02/2020

El objeto del presente documento es el de generar un marco de referencia consensuado por parte de los organismos nacionales competentes en el ámbito de la notificación y gestión de incidentes de ciberseguridad.

Se conoce como gestión de ciber incidentes a un conjunto ordenado de acciones enfocadas a prevenir en la medida de lo posible la ocurrencia de ciber incidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible. El proceso de gestión de incidentes consta de diferentes fases y, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea, como se muestra en la Figura 3-20.

Figura 3-20: Fases de la gestión de un ciber incidente

Fuente: Guía nacional de notificación y gestión de ciber incidentes – INCIBE

e. ISO/IEC 27035 – 1 y 2:

ISO/IEC 27035 – 1 y 2: Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad – parte 1, principios y parte 2, directrices para planificar y prepararse para la respuesta a incidentes, 11/01/2016

ISO / IEC 27035-1, Principios de gestión de incidencias (este documento), se presentan los conceptos básicos y las fases de la gestión de incidentes de seguridad de la información, y cómo mejorar la gestión de incidencias. Esta parte combina estos conceptos con los principios de un enfoque estructurado para detectar, informar, evaluar y responder a los incidentes, y la aplicación de las lecciones aprendidas.

Esta norma plantea 5 fases para lograr los objetivos de la gestión de incidentes de seguridad de la información, las cuales se describen a continuación:

- Planificación y Preparación: Para que un plan de gestión de incidentes de seguridad de la información sea eficiente y eficaz para ponerlo en funcionamiento, una organización debe completar una serie de actividades preparatorias y de planeación que debe realizar para enfrentar los incidentes que se puedan materializar.

- Detección y Reporte: La segunda fase de la gestión de incidente de seguridad de la información implica la detección, recolección de información asociada con las ocurrencias de eventos de seguridad de la información y la existencia de vulnerabilidades de seguridad de información por medios manuales o automáticos. En esta fase, eventos y vulnerabilidades podrían todavía no ser clasificados como incidentes de seguridad de la información. La notificación de eventos de seguridad en línea con las políticas de seguridad de la información de la organización permite el análisis posterior si es necesario.

- Evaluación y Decisión: La tercera fase de la gestión de incidentes de seguridad de información consiste en la evaluación de la información asociada con las ocurrencias de eventos de seguridad de la información y la decisión de si para clasificar los eventos como incidentes de seguridad de la información.

- Respuestas: La cuarta fase de gestión de incidentes de seguridad de la información consiste en responder a los incidentes de seguridad de información de acuerdo con las acciones determinadas en la evaluación y la fase de decisión. Dependiendo de las decisiones, las respuestas podrían hacerse de inmediato, en tiempo real o casi en tiempo real, y algunas respuestas podrían implicar investigación de seguridad de la información.

- Lecciones aprendidas: La quinta fase de gestión de incidentes de seguridad de la información se produce cuando los incidentes de seguridad de la información han sido resueltos. Esta fase consiste en lecciones de aprendizaje de cómo se han manejado los incidentes (y las vulnerabilidades).

ISO / IEC 27035-2, directrices para planificar y prepararse para la respuesta a incidentes, describe cómo planificar y prepararse para la respuesta a incidentes. Esta parte comprende el “Plan” y preparar las fases “lecciones aprendidas” del modelo presentado en la norma ISO / IEC 27035-1.

Análisis de las normas

Después de analizar más en detalle los 5 referentes anteriores, se llega a la siguiente conclusión:

- La guía para la gestión y clasificación de incidentes de seguridad de la información de MINTIC, se elaboró recogiendo los aspectos importantes de mejores prácticas y documentos de uso libre del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide) y tomó como base los lineamientos

recomendados en la norma ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes.

- La guía nacional de notificación y gestión de Ciber incidentes de INCIBE, en sus fases está muy alineada con el Framework de NIST y el estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide, aunque el nombre de sus fases los relacione diferente, su propósito es el mismo.

- El NIST Cybersecurity Framework: Marco para la mejora de la seguridad cibernética en infraestructuras críticas Versión 1.1, Es un marco más general, integrador y ofrece una forma flexible de abordar la seguridad cibernética, lo que incluye el efecto de la seguridad n las dimensiones físicas, cibernéticas y de personas. Este es aplicable a organizaciones que dependen en la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en tecnología de la 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 puede ayudar a las organizaciones a abordar la seguridad cibernética ya que afecta la privacidad de los clientes, empleados y otras partes. Por lo que aporta a la gestión desde el ciclo PHVA, este será la base de referencia para diseñar y complementar el nuevo procedimiento de gestión de incidentes de ciberseguridad, alineado e integrado con la respuesta corporativa.

- El estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide su énfasis está en cómo mitigar los riesgos de los incidentes de seguridad informática al proporcionar pautas prácticas para responder a los incidentes de manera efectiva y eficiente. Incluye pautas para establecer un programa de respuesta a incidentes efectivo, pero el enfoque principal del documento es detectar, analizar, priorizar y manejar incidentes una vez se haya identificado o materializado. Este estándar nos brinda insumos para complementar la propuesta de diseño del nuevo procedimiento de gestión de incidentes de ciberseguridad, alineado e integrado a la respuesta corporativa.

- La norma ISO/IEC 27035 – 1 y 2: Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad – parte 1, principios y parte 2, directrices para planificar y prepararse para la respuesta a incidentes, nos dan la orientación desde la gestión y la respuesta de los incidentes de seguridad, relacionando y describiendo las actividades que hay que llevar a cabo para una eficaz y eficiente gestión de estos.

- Los referentes seleccionados y que le aportan al trabajo de investigación son el framework de NIST V1.1 por si visión global (PHVA), integradora y que contempla tecnologías de la operación, el estándar NIST SP 800-61 rev 2 y la norma ISO/IEC 27035 – 1 y 2, por su complemento en la preparación y respuesta ante los incidentes de ciberseguridad.

Nota: Las fuentes de INCIBE y MINTIC, se descartaron en la validación de resultados por la siguiente razón: La guía nacional de notificación y gestión de Ciber incidentes de INCIBE, en sus fases está muy alineada con el Framework de NIST y el estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide, aunque el nombre de sus fases los relacione diferente, su propósito es el mismo y la guía para la gestión y clasificación de incidentes de seguridad de la información de MINTIC, se elaboró recogiendo los aspectos importantes de mejores prácticas y documentos de uso libre del NIST (National Institute of Standards and Technology – (Computer Security Incident Handling Guide) y tomó como base los lineamientos recomendados en la norma ISO IEC 27001 – 2013 Numeral 16 de la misma, para la gestión de incidentes. Por esta razón se decidió continuar con el Framework de NIST, el estándar NIST SP 800-61 Rev. 2 y el estándar ISO/IEC 27035 -1-2.

Finalmente se realizó un comparativo donde se señala una breve descripción del propósito de cada uno de los 3 referentes seleccionados, sus etapas, sus ventajas, sus desventajas y el aporte que le brinda al diseño del nuevo procedimiento integrado de gestión de incidentes de ciberseguridad y respuesta corporativa. Ver la Tabla 3-10:

Tabla 3-10. Cuadro comparativo principales etapas de la gestión de incidentes

Cuadro comparativo principales etapas de la gestión de incidentes					
Referente	**Descripción**	**Fase**	**Ventajas**	**Desventajas**	**Aporte al nuevo procedimiento**
NIST Cybersecurity Framework: Marco para la mejora de la seguridad cibernética en infraestructuras críticas Versión 1.1, publicado 16/04/2018	Ofrece una forma flexible de abordar la seguridad, lo que incluye el efecto de la seguridad cibernética en las dimensiones físicas, cibernéticas y de personas.	Funciones: • Identificar • Proteger • Detectar • Responder • Recuperar	Este es aplicable a organizaciones que dependen en la tecnología, ya sea que su enfoque de seguridad cibernética sea principalmente en tecnología de la 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 puede ayudar a las organizaciones a abordar la seguridad cibernética ya que afecta la	Ninguna	Como marco su enfoque es desarrollar la capacidad de gestión de la seguridad cibernética en las organizaciones con su visión global e integradora, alineado con las diferentes metodologías existente para la gestión y respuesta a los incidentes de ciberseguridad y en especial a los de las tecnologías de la operación.

Cuadro comparativo principales etapas de la gestión de incidentes					
Referente	**Descripción**	**Fase**	**Ventajas**	**Desventajas**	**Aporte al nuevo procedimiento**
			privacidad de los clientes, empleados y otras partes. Las cinco funciones básicas que define el no están destinadas a formar una ruta serial o conducir a un estado final estático deseado. Por el contrario, las funciones deben realizarse concurrente y continuamente para formar una cultura operativa que aborde el riesgo dinámico de seguridad cibernética. Las funciones también se alinean con las metodologías existentes		Como su estructura está basada en el ciclo PHVA y su desarrollo pasa por todas estas fases, el aporte para este proyecto de investigación es que se convierte en el referente fundamental y estructural para definir el diseño del nuevo procedimiento de gestión de incidentes de ciberseguridad, alineado e integrado a la respuesta corporativa.

Cuadro comparativo principales etapas de la gestión de incidentes					
Referente	**Descripción**	**Fase**	**Ventajas**	**Desventajas**	**Aporte al nuevo procedimiento**
			para la gestión de incidentes y ayudan a mostrar el impacto de las inversiones en seguridad cibernética. Por ejemplo, las inversiones en planificación y ejercicios apoyan la respuesta oportuna y las acciones de recuperación, lo que resulta en un impacto reducido en la prestación de servicios.		
Estándar NIST SP 800-61 rev 2: Computer Security Incident	Esta guía busca ayudar a las organizaciones a mitigar los riesgos de los incidentes de seguridad informática al	• Preparación • Detección y Análisis. • Contención, erradicación	Brindan un acercamiento y orientación de cómo afrontar y gestionar los incidentes de seguridad una vez se hayan	Su foco y énfasis está sólo en la respuesta de los incidentes que están ocurriendo o	Desde el enfoque de la gestión basados en el ciclo PHVA, existe una equivalencia entre las fases de ambas guías,

Cuadro comparativo principales etapas de la gestión de incidentes					
Referente	**Descripción**	**Fase**	**Ventajas**	**Desventajas**	**Aporte al nuevo procedimiento**
Handling Guide, Agosto 2012	proporcionar pautas prácticas para responder a los incidentes de manera efectiva y eficiente.	y recuperación. • Actividad post incidente.	identificado o materializado, es decir, la gestión o manejo reactivo a los incidentes de seguridad informática, así como un acercamiento al plan, políticas y procedimientos que deberán ser llevados a cabo por el equipo de respuesta según su estructura organizativa y funcional. Son útiles en su totalidad cuando se trata de un incidente de seguridad que ha ocurrido o está ocurriendo.	han ocurrido, siendo un enfoque totalmente reactivo. Algunos procedimientos de las guías de referencia son parcialmente eficientes cuando se trata realizar la gestión bajo el ciclo PHVA en lo relacionado con la prevención, es decir en el antes de que ocurra el o los incidentes.	con un avance en el desarrollo de la fase del Hacer, aportando las mejores prácticas en relación con la conveniencia y acercamiento para complementar la propuesta al diseño del nuevo procedimiento de gestión de incidentes de ciberseguridad, alineado e integrado a la respuesta corporativa.
ISO/IEC 27035 – 1 y 2:	Se presentan los conceptos básicos y las fases de la gestión de incidentes de seguridad de la información, y cómo mejorar la gestión de incidencias. Esta parte combina estos conceptos con los principios de un enfoque estructurado para detectar, informar, evaluar y responder a los incidentes, y la aplicación	• Planificación y preparación. • Detección y reporte. • Evaluación y decisión. • Respuestas • Lecciones aprendidas			

Cuadro comparativo principales etapas de la gestión de incidentes					
Referente	**Descripción**	**Fase**	**Ventajas**	**Desventajas**	**Aporte al nuevo procedimiento**
	de las lecciones aprendidas.				

Fuente: Elaboración Propia

Con base en la tabla anterior, se concluye que el marco de ciberseguridad de NIST que está disponible y se enfoca en las organizaciones cuyos servicios son soportados en las tecnologías de la operación de infraestructuras críticas, se convierte en la línea base para tomar como punto de partida los elementos que harán parte del nuevo procedimiento de gestión de incidentes y tomando como complemento los ofrecidos en el estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide, Agosto 2012 y la ISO/IEC 27035 – 1 y 2: Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad. Además de esto, también se tendrá en cuenta los resultados arrojados en los objetivos específicos 1 y 2 desarrollados en este proyecto.

Para una mejor ilustración se hace una alineación y equivalencia de los referentes seleccionados con el ciclo de vida de la gestión (PHVA) y en qué fase le aportan cada uno de ellos al diseño del nuevo procedimiento de gestión de incidentes de ciberseguridad, alineado e integrado a la respuesta corporativa. Ver la siguiente Tabla 3-11:

Tabla 3-11. Alineación y equivalencia de los referentes seleccionados con el ciclo de vida de la gestión (PHVA)

Referente	Planear	Hacer	Verificar	Actuar
NIST Cybersecurity Framework	Identificar Detectar	Proteger Responder	Recuperar	Recuperar
Estándar NIST SP 800-61 rev 2	Preparación Detección y Análisis.	Contención, erradicación	Recuperación	Actividad post incidente
ISO/IEC 27035 – 1 y 2:	Planificación y preparación. Detección y reporte. Evaluación y decisión.	Evaluación y decisión Respuestas	Evaluación y decisión	Lecciones aprendidas

Fuente: Elaboración Propia

Para una mejor ilustración en más detalle ver la siguiente Tabla 3-12:

Tabla 3-12. Principales etapas de la gestión de incidentes bajo el ciclo PHVA

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
P L A N E A R	**Identificar:** Desarrollar una comprensión organizacional para administrar el riesgo de seguridad cibernética para sistemas, personas, activos, datos y capacidades	a) Gestión de activos. b) Entorno empresarial c) Gobernanza. d) Evaluación de riesgos. e) Estrategia de gestión de riesgos. f) Gestión de riesgos de la cadena de suministros.	**Preparación:** Establecer una capacidad de respuesta a incidentes para que la organización esté lista para responder a incidentes, también prevenir incidentes al garantizar que los sistemas, redes y aplicaciones sean lo suficientemente	a) Mecanismos de coordinación. b) Información de contactos. c) Equipo, Lugar y herramientas de respuesta.	**Planificación y Preparación:** Para que un plan de gestión de incidentes de seguridad de la información sea eficiente y eficaz para ponerlo en funcionamiento, una organización debe completar una serie de actividades preparatorias, a saber.	a) Formular y producir una política de gestión de incidentes de seguridad de la información y adquirir compromiso de la dirección. b) Actualizar las políticas de seguridad de la información, incluidos los relacionados con la gestión de riesgos. c) Definir y documentar un plan de seguridad de la información. d) Establecer el equipo de respuesta a incidentes (IRT), con el correspondiente programa de formación diseñado, desarrollado y proporcionado su personal. e) Establecer y mantener relaciones y conexiones apropiadas con las organizaciones internas y externas. f) Establecer, implementar y operar los mecanismos técnicos, organizativos y operativos.

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
			seguros. Aunque el equipo de respuesta a incidentes no suele ser responsable de la prevención de incidentes, es fundamental para el éxito de los programas de respuesta a incidentes.			g) Diseño y desarrollo de un programa de formación capacitación y entrenamiento para el evento de seguridad de la información. h) Probar el uso del plan de gestión de incidentes de seguridad de la información, sus procesos y procedimientos.

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
	Proteger: Desarrollar e implementar medidas de seguridad adecuadas para garantizar la entrega de servicios críticos. La función Proteger admite la capacidad de limitar o contener el impacto de un posible evento de seguridad cibernética.	a) Gestión de identidad y control de acceso. b) Conciencia y capacitación. c) Seguridad de datos. d) Procesos y procedimientos de protección de la información. e) Mantenimiento. f) Tecnología de protección.	**Detección y análisis:** Los incidentes pueden ocurrir de innumerables formas, por lo que no es factible desarrollar instrucciones paso a paso para manejar cada incidente. Las organizaciones deben estar generalmente preparadas para manejar cualquier incidente, pero	a) Vectores de ataque. b) Señales de un incidente. c) Fuentes precursores e indicadores. d) Análisis. e) Documentación. f) Priorización. g) Notificación del incidente.	**Detección y Reporte: I**mplica la detección, recolección de información asociada con las ocurrencias de eventos de seguridad de la información y la existencia de vulnerabilidades de seguridad de información por medios manuales o automáticos.	a) Monitorear la actividad del sistema y la red de la organización, si proceden a iniciar la sesión. b) Detectar y reportar la ocurrencia de un evento o la existencia de una vulnerabilidad de seguridad de la información. c) Recopilar información sobre un evento de seguridad de información o su vulnerabilidad. d) Garantizar que todas las actividades, los resultados y las decisiones conexas se registran adecuadamente para su posterior análisis. e) Garantizar que las pruebas digitales se recogen y almacenan de forma segura. f) Asegurarse de que un régimen de control de cambios es seguido para permitir eventos de seguridad de la información.

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
			deben enfocarse en estar preparadas para manejar incidentes que utilizan vectores de ataque comunes. Los diferentes tipos de incidentes merecen diferentes estrategias de respuesta.			

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
H A C E R	**Detectar:** Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de seguridad cibernética. La Función Detectar permite el descubrimiento oportuno de eventos de seguridad cibernética.	a) Anomalías y eventos. b) Vigilancia continua de seguridad. c) Procesos de detección.	**Contención, erradicación y recuperación:** La contención es importante antes de que un incidente sobrepase los recursos o aumente el daño. La mayoría de los incidentes requieren contención, por lo que es una consideración importante en las primeras etapas del manejo de cada	a) Elegir la estrategia de contención. b) Recolección y manejo de la evidencia. c) Identificación de host atacante. d) Acciones de erradicación.	**Evaluación y Decisión:** Consiste en la evaluación de la información asociada con las ocurrencias de eventos de seguridad de la información y la decisión para clasificar los eventos como incidentes de seguridad de la información.	a) Recopilar información que puede incluir pruebas y mediciones acerca de la detección de un evento de seguridad informática. b) Realizar una evaluación para determinar si el evento es un posible o confirmado incidente de seguridad o información de una falsa alarma. c)Asegurar que todas las partes involucradas, en particular el IRT, registran adecuadamente todas las actividades, los resultados y las decisiones conexas para su posterior análisis. d)Asegúrese de que el régimen de control de cambios se mantiene para cubrir el seguimiento de incidentes y de notificación de incidentes, y para mantener la base de datos de seguridad de información actualizada.

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
			incidente. Una vez que se ha contenido un incidente, la erradicación puede ser necesaria para eliminar los componentes del incidente. En la recuperación, los administradores restauran los sistemas para que funcionen normalmente, confirman que los sistemas están			

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
			funcionando normalmente y (si corresponde) corrigen vulnerabilidades para evitar incidentes similares.			
	Responder: Desarrollar e implementar actividades apropiadas para tomar medidas con respecto a un incidente detectado de seguridad	a) Planificación de respuesta. b) Comunicaciones. c) Análisis. d) Mitigación. e) Mejoras.			**Respuestas:** Consiste en responder a los incidentes de seguridad de información de acuerdo con las acciones determinadas en la evaluación y la fase de decisión.	a) Investigar los incidentes según se requiera y con respecto a la clasificación de incidentes y la escala de calificación de seguridad de la información. b) Revisión por parte del IRT para determinar si el incidente de seguridad de la información está bajo control, y si es así, realice la respuesta requerida. Si el incidente no está bajo control o que va a tener un impacto severo en las operaciones de la organización, realizar actividades de respuesta de crisis a

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
	cibernética. La función Responder respalda la capacidad de contener el impacto de un posible incidente de seguridad cibernética				Dependiendo de las decisiones, las respuestas podrían hacerse de inmediato, en tiempo real o casi en tiempo real, y algunas respuestas podrían implicar investigación de seguridad de la información.	través de la escalada a la función de manejo de crisis. c) Asignar recursos internos e identificar los recursos externos con el fin de responder a un incidente. d) Asegurar que todas las partes involucradas, en particular el IRT, registren adecuadamente todas las actividades para su posterior análisis. e) Asegurar de que la evidencia digital se recoge y almacena de forma segura demostrable. f) Asegurar de que el régimen de control de cambios se mantiene para cubrir las actualizaciones de seguimiento y notificación de incidentes. g) Comunicar la existencia del incidente de seguridad de la información y compartir todos los detalles pertinentes con otras personas u organizaciones

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
V E R I F I C A R Y A C T U A R	**Recuperar:** Desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restablecer cualquier capacidad o servicio que se haya visto afectado debido a un incidente de seguridad cibernética.	a) Planificación de recuperación. b) Mejoras. c) Comunicaciones.	**Actividad posterior al incidente:** Una de las partes más importantes de la respuesta a incidentes es también la que se omite con mayor frecuencia: aprender y mejorar. Cada equipo de respuesta a incidentes debe evolucionar para reflejar nuevas amenazas, tecnología	a) Lecciones aprendidas. b) Datos de incidentes anteriores similares. c) Retención de evidencia.	**Lecciones aprendidas:** Cuando los incidentes de seguridad de la información han sido resueltos. Esta fase consiste en lecciones de aprendizaje de cómo se han manejado los incidentes (y las vulnerabilidades).	a) Identificar las lecciones aprendidas de los incidentes de seguridad de la información y las vulnerabilidades. b) Revisar, identificar y hacer mejoras en la aplicación de control de seguridad de la información (controles nuevos o actualizados). c) Revisar, identificar y hacer mejoras a las revisiones evaluaciones y gestión de riesgos de seguridad de información existentes. d) Revisar la eficacia de los procesos, procedimientos, formatos y estructura de la organización e) Sobre la base de las lecciones aprendidas, identificar y hacer mejoras en el plan de gestión de incidentes de seguridad de la información y la documentación. f) Comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza (si la organización así lo desea).

Principales etapas de la gestión de incidentes bajo el ciclo PHVA						
Referentes	**NIST Cybersecurity Framework**		**Estándar NIST SP 800-61 rev 2**		**ISO/IEC 27035 – 1 y 2:**	
PHVA	**Fase**	**Actividades**	**Fase**	**Actividades**	**Fase**	**Actividades**
			mejorada y lecciones aprendidas.			g) Determinar si la información del incidente, vectores de ataque y vulnerabilidades asociadas pueden ser compartidos con organizaciones asociadas para ayudar en la prevención de los mismos incidentes que se produzcan en sus entornos. h Realizar una evaluación exhaustiva del rendimiento y la eficacia de IRT sobre una base periódica.

Fuente: Elaboración Propia

La tabla anterior resume el propósito del objetivo específico 3 que es el de caracterizar las principales etapas para tener en cuenta en la respuesta a incidentes, resultado que sirve como insumo para construir el diseño del nuevo procedimiento de gestión de incidentes de ciberseguridad, alineado e integrado a la respuesta corporativa.

Además, integrar los resultados de los objetivos específicos 1 y 2 para obtener el producto final que es el resultado del objetivo específico 4. Por esta razón la actividad 2: Construir el diseño integrado de gestión de incidentes de ciberseguridad y respuesta corporativa del objetivo específico 3, se desarrolla en el objetivo específico 4 donde se integran los resultados obtenidos en los objetivos específico 1, 2 y 3 para luego validar el procedimiento con un estudio de caso que está dentro del alcance del objetivo 4.

3.4 Fase 4: Construcción y Validación

Objetivo específico 4: Validar el procedimiento de Gestión de Incidentes de Ciberseguridad a través de un ejercicio de simulación o juego de roles dentro de un caso de estudio.

3.4.1 Actividad 1. Construir el diseño integrado de gestión de incidentes de ciberseguridad y respuesta corporativa

En esta actividad se diseñó y construyó el procedimiento gestión de incidentes y su articulación con la respuesta corporativa, partiendo de los requerimientos mínimos del servicio, mapeándolos sobre los procesos de gestión de incidentes, teniendo como marco el ciclo PHVA y los elementos de la estructura de alto nivel.

Teniendo como base del análisis la ficha de requerimientos mínimos del servicio, los elementos claves de la gestión de riesgos, continuidad, crisis y resiliencia, las Características mínimas de los tipos de respuesta a nivel corporativo ante la ocurrencia de eventos tecnológicos y las etapas de la gestión y atención de los incidentes de ciberseguridad, se logró llegar a la siguiente propuesta para el procedimiento de Gestión de Incidentes de Ciberseguridad.

Procedimiento Gestión de Incidentes de Ciberseguridad en las Tecnologías de Operación diseñado

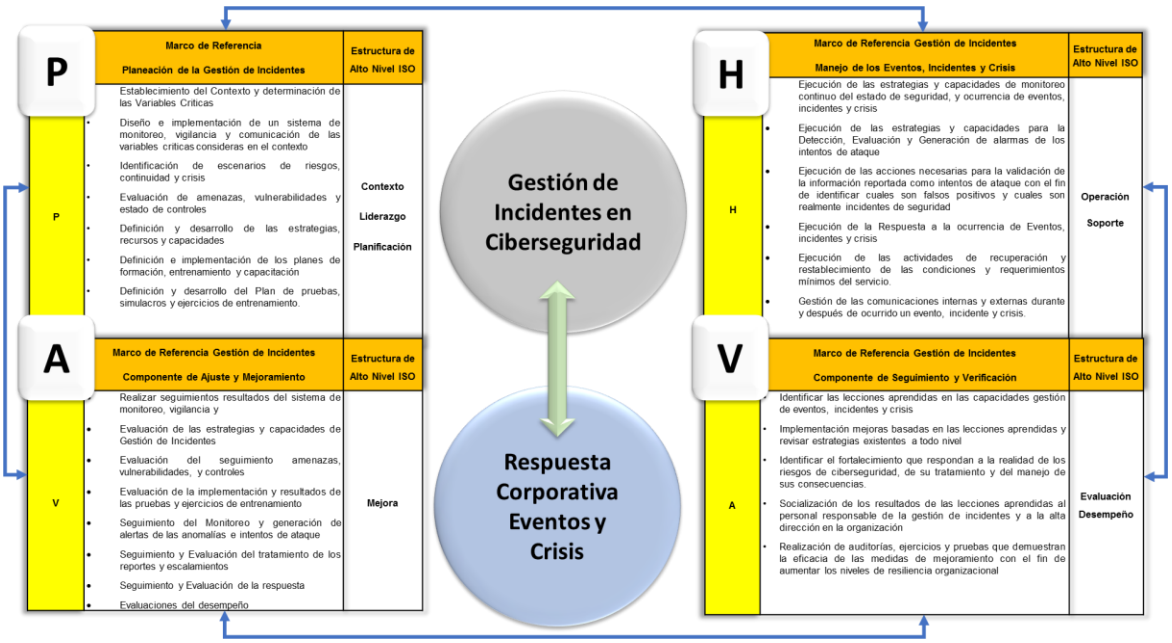
En esta actividad se diseñó y construyó el procedimiento gestión de incidentes y su articulación con la respuesta corporativa, partiendo de los requerimientos mínimos del servicio, mapeándolos sobre los procesos de gestión de incidentes, teniendo como marco el ciclo PHVA y los elementos de la estructura de alto nivel Teniendo como base del análisis la ficha de requerimientos mínimos del servicio, los elementos claves de la gestión de riesgos, continuidad, crisis y resiliencia, las Características mínimas de los tipos de respuesta a nivel corporativo ante la ocurrencia de eventos tecnológicos y las etapas de la gestión y atención de los incidentes de ciberseguridad, se logró llegar a la siguiente propuesta para el **procedimiento de Gestión de Incidentes de Ciberseguridad.**

Para su diseño y construcción se tuvieron en cuenta los siguientes aspectos:

1) Partir de las actividades del Framework de NIST para facilitar la articulación
2) A cada actividad asociarle los elementos de las normas de referencia escogidas tanto de Gestión de Incidentes como de riesgos, continuidad, crisis y resiliencia que podrían fortalecer las acciones definidas
3) Reconocer el énfasis que desde un enfoque sistémico siguiendo PHVA, era importante tener en cuenta para un procedimiento de gestión de incidentes
4) Definir las actividades que dentro de la planeación, ejecución, verificación y ajuste era importante tener para una gestión de incidentes
5) Identificar los elementos de la estructura de alto nivel que servirán para la articulación de la respuesta corporativa posteriormente.

A continuación, se presenta la Tabla 3-13 que permite observar el resultado de los elementos de la propuesta a desarrollar:

Tabla 3-13. Propuesta para el Diseño y construcción del Procedimiento Gestión de Incidentes (NIST) fortalecido con los elementos claves de las normas de referencia en riesgos, continuidad, crisis y resiliencia con enfoque PHVA y articulado a la respuesta corporativa



Fuente: Elaboración Propia

Cada uno de los 4 componentes de detallan a continuación (PHVA):

1) Componente Planeación de la Gestión de Incidentes (Planear)

Descripción: Identificación, análisis y evaluación del contexto empresarial tanto interno como externo con el fin de comprender el estado actual y cambios en la gestión de riesgos, la capacidad de aseguramiento de las operaciones ante posibles interrupciones, los niveles de respuesta a la generación de eventos, incidentes y crisis y las capacidades de recuperación, adaptación y transformación que la organización realiza a nivel de los activos y ciber activos que soportan la prestación de servicios, con el fin de realizar la planeación de la gestión de incidentes que permita gestionar el riesgo de ciberseguridad (Tabla 3-14 y Figura 3-21).

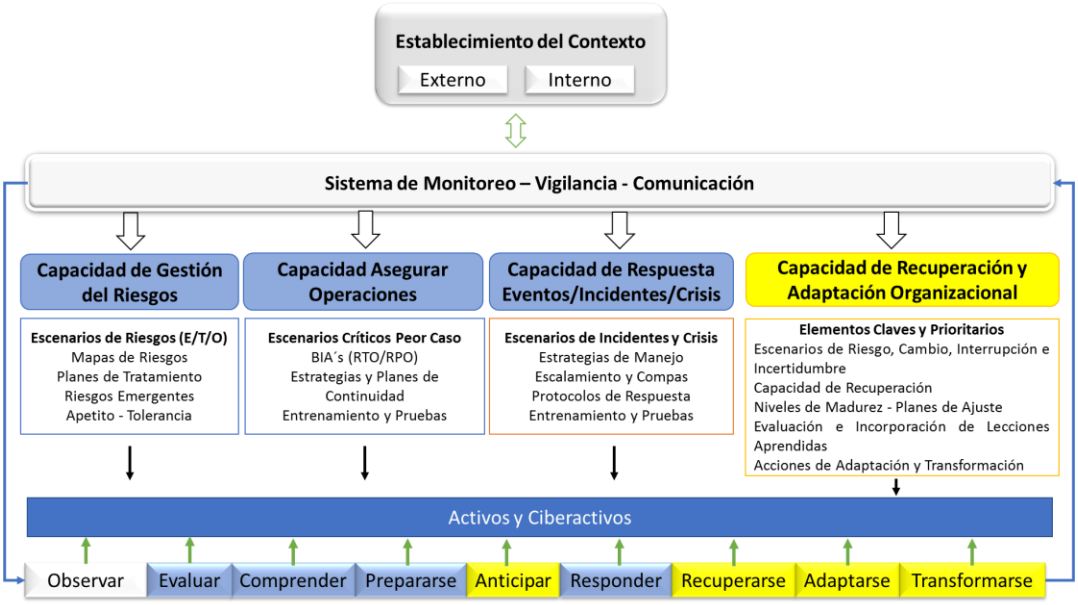
Tabla 3-14. Componente Planeación Gestión de Incidentes

Ciclo de Gestión - PHVA	Planeación de la Gestión de Incidentes	Estructura de Alto Nivel ISO
P	• Establecimiento del Contexto y determinación de las Variables Criticas con foco en la gestión de incidentes a nivel de los activos y ciber activos de la organización • Diseño e implementación de un sistema de monitoreo, vigilancia y comunicación de las variables criticas consideras en el contexto, y su impacto en la gestión de riesgos, aseguramiento de las operaciones, en la gestión de eventos, incidentes y crisis, y en la capacidad de recuperación de la Organización con foco en los activos y ciber activos. • Identificación de Activos/Ciber activos objeto de la gestión de incidentes • Identificación de escenarios de riesgos, continuidad y crisis con énfasis en los activos y ciber activos objeto de la gestión. • Evaluación de amenazas, vulnerabilidades y estado de controles a nivel de los activos y ciber activos objeto de la gestión • Definición, desarrollo de las estrategias, recursos, capacidades de prevención, protección, respuesta y recuperación para su ejecución y la entrega de recomendaciones para el cierre de brechas existentes • Definición e implementación de los planes de formación, entrenamiento y capacitación al personal involucrado en la gestión de incidentes	• Contexto • Liderazgo • Planificación

Ciclo de Gestión - PHVA	Planeación de la Gestión de Incidentes	Estructura de Alto Nivel ISO
	• Definición y desarrollo del Plan de pruebas, simulacros y ejercicios de entrenamiento para responder y recuperarse ante los eventos, incidentes y crisis.	

Fuente: Elaboración propia

Figura 3-21: Actividades de la Planeación de la gestión de Incidente



Fuente: Elaboración propia

A continuación, se presenta los siguientes aspectos e insumos:

<u>Aspectos para tener en cuenta:</u>

1) El Direccionamiento, metas e indicadores del nivel estratégico, táctico y operativo de los negocios y áreas involucradas.
2) Políticas, lineamientos y reglas de negocio existentes que apliquen.

3) Metodologías, guías, procedimientos e instructivos que se requieren tener en cuenta o alinear y ajustar
4) Estado del arte en relación con las amenazas, vulnerabilidades, controles y temas emergentes
5) Niveles de gestión de riesgos, continuidad, crisis y resiliencia existente
6) Requerimientos mínimos del servicio/productos (Negocio, Proceso, Activos, Legal, normativo y regulatorio)
7) Requerimientos, necesidades y expectativas de los grupos de Interés
8) Protocolos de respuesta corporativa existentes para la atención de eventos, y crisis en la organización y su articulación con la gestión de incidentes
9) Estado de los niveles de concienciación, formación, entrenamiento y ejercicios de pruebas del personal que interviene los activos y ciber activos de la organización.

Salida del componente de Planeación de la Gestión de Incidentes

- Señales y tendencias del contexto (Externo e Interno) con relación a los activos y ciber activos foco de la gestión
- Estado del arte de las amenazas, vulnerabilidades y controles a nivel de la ciberseguridad en los activos y ciber activos de las Tecnologías existentes en la organización (TI y TO)
- Identificación de los escenarios de riesgos, continuidad y crisis asociados a los activos y ciber activos de las Tecnologías existentes en la organización (TI y TO) foco de la gestión
- Determinación de los elementos claves, críticos y prioritarios de la organización a proteger (Inventario) en relación con los activos y ciber activos existentes actuales, en proceso y futuros
- Identificación de las capacidades de recuperación y los niveles de madures en resiliencia organizacional existentes en la organización con relación a los activos y ciber activos
- Diseño del Plan, Procedimiento y Guía táctica para la gestión de eventos e incidentes

- Aseguramiento de los recursos necesarios para la gestión de incidentes en términos del desarrollo e implementación de estrategias, con el fin de hacer frente a los riesgos de ciberseguridad y al manejo de sus consecuencias.
- Asignación del Equipo de gestión y respuesta a eventos e incidentes, roles y responsabilidades
- Mecanismo de articulación del equipo de gestión y respuesta a eventos e incidentes con el protocolo de respuesta corporativa existente
- Determinación del alcance de la gestión de incidentes en la organización; 1) Procesos, 2) Infraestructura Critica, 3) Componentes de TI, 4) Productos y/o Servicios, 5) Proyectos y 6) Contratos que involucran las Tecnologías.
- Políticas, lineamientos y reglas de negocio para la articulación y operatividad de la gestión de incidentes en la organización.
- Planes de tratamiento en la gestión de riesgos y estrategias de continuidad, crisis y resiliencia con foco en la gestión de incidentes
- Identificación y capitalización de las lecciones aprendidas de la atención de otros eventos, incidentes y crisis ya materializados o de los ejercicios de simulación y simulacros llevados a cabo.
- Diseño e implementación de un sistema de monitoreo, vigilancia y comunicación de las variables criticas consideras en el contexto, y su impacto en la gestión de riesgos, aseguramiento de las operaciones, en la gestión de eventos, incidentes y crisis, y en la capacidad de recuperación de la Organización con foco en los activos y ciber activos.
- Diseño de un programa de formación, capacitación y entrenamiento para la gestión de eventos, incidentes y crisis al personal para el equipo de gestión de incidentes y sus aliados a niveles estratégicos, tácticos y operativos de la organización.

2) Componente Manejo de los Eventos, Incidentes y Crisis (Hacer)

Descripción: Ejecución de los planes, estrategias y capacidades organizacionales en cuanto al monitoreo continuo de la seguridad de información y de ciberseguridad, Detección,

evaluación y alarmas de anomalías a nivel de los activos y ciber activos, Validación de la información, Atención, respuesta y recuperación ante los posibles eventos, incidentes y crisis, así como de la gestión de comunicaciones internas y externas durante y después de ocurrido un evento, incidente y crisis (Tabla 3-15 y Figura 3-22).

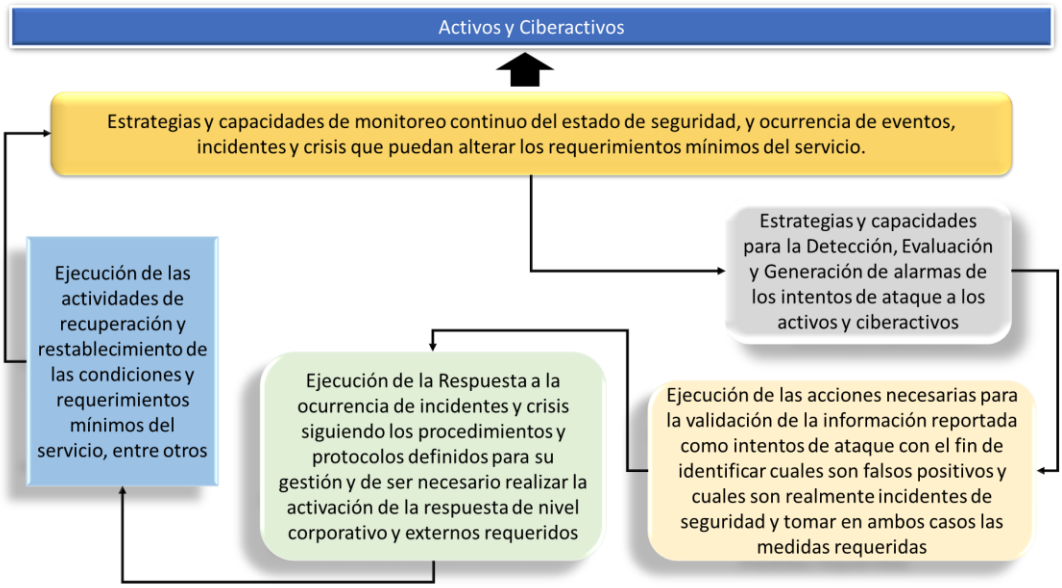
Tabla 3-15. Componente Manejo de los Eventos, Incidentes y Crisis

Ciclo de Gestión - PHVA	Manejo de los Eventos, Incidentes y Crisis	Estructura de Alto Nivel ISO
H	• Ejecución de las estrategias y capacidades de monitoreo continuo del estado de seguridad, y ocurrencia de eventos, incidentes y crisis que puedan alterar los requerimientos mínimos del servicio. • Ejecución de las estrategias y capacidades para la Detección, Evaluación y Generación de alarmas de los intentos de ataque a los activos y ciber activos. • Ejecución de las acciones necesarias para la validación de la información reportada como intentos de ataque con el fin de identificar cuáles son falsos positivos y cuales son realmente incidentes de seguridad y tomar en ambos casos las medidas requeridas. • Ejecución de la Respuesta a la ocurrencia de Eventos, incidentes y crisis siguiendo los procedimientos y protocolos definidos para su gestión y de ser necesario realizar la activación de la respuesta de nivel corporativo y externos requeridos. • Ejecución de las actividades de recuperación y restablecimiento de las condiciones y requerimientos mínimos del servicio, entre otros.	• Operación • Soporte

Ciclo de Gestión - PHVA	Manejo de los Eventos, Incidentes y Crisis	Estructura de Alto Nivel ISO
	• Gestión de las comunicaciones internas y externas durante y después de ocurrido un evento, incidente y crisis.	

Fuente: Elaboración propia

Figura 3-22: Actividades de la Ejecución de la gestión de Incidente



Fuente: Elaboración Propia

A continuación, se presenta los siguientes aspectos e insumos:

<u>Aspectos para tener en cuenta:</u>

1) Metodologías, guías, procedimientos e instructivos que se tiene definidos e implementados en la organización para su utilización.
2) Los Análisis de riesgos y controles implementados
3) Diseño de las estrategias de continuidad, crisis y resiliencia
4) Protocolos de respuesta corporativa existentes para la atención de eventos, y crisis en la organización y su articulación con la gestión de incidentes.
5) Sistema de monitoreo, vigilancia y comunicaciones con foco en la gestión de incidentes.

Salida del componente Manejo y Recuperación de los Eventos, Incidentes y Crisis

- Definición, desarrollo e implementación de las estrategias de continuidad, crisis y resiliencia.
- Definición y ejecución del programa de formación, entrenamiento y capacitación al personal involucrado en la gestión de incidentes.
- Definición e implementación de los procedimientos de respuesta y recuperación articulados con la respuesta corporativa.
- Informes de las evaluaciones e investigaciones en la gestión de incidentes realizadas
- Plan de pruebas, simulacros y ejercicios de entrenamiento para responder y recuperarse ante los eventos, incidentes y crisis implementado.
- Equipo de gestión y respuesta a eventos e incidentes, roles y responsabilidades formado, capacitado y entrenado.
- Implementación del sistema de monitoreo continuo del estado de seguridad, y ocurrencia de eventos, incidentes y crisis que puedan alterar los requerimientos mínimos del servicio
- Gestión de las comunicaciones durante y después de la ocurrencia de eventos, incidentes y crisis

3) Componente Seguimiento y verificación de la Gestión de Incidentes (Verificar)

Descripción: Realizar los seguimientos y verificaciones continuas con el propósito de asegurar y mejorar la calidad y la eficacia del diseño, implementación y los resultados de la gestión de incidentes y de esta manera contribuir con el desarrollo de las capacidades para gestionar los riesgos, asegurar las operaciones, la respuesta, recuperación y comunicación (Tabla 3-16 y Figura 3-23).

El seguimiento y las verificaciones continuas deberían tener lugar en todas actividades y resultados que se lleven a cabo en la gestión de incidentes. La organización debería a partir de los resultados de los seguimientos y verificaciones, realizar las adaptaciones del procedimiento de gestión de incidentes en función de los cambios del contexto externos e internos y sus impactos en las capacidades actuales de gestión de riesgos, aseguramiento de las operaciones, manejo y respuesta a los eventos, incidentes y crisis, y finalmente de su capacidad de recuperación.

Los Seguimientos y verificaciones pueden adoptar la forma de auditorías internas o externas, o de autoevaluaciones. La frecuencia y el tiempo de la revisión pueden verse influidos por leyes y reglamentos, según el tamaño, la naturaleza y la condición jurídica de la organización. También pueden verse influidos por los requisitos de las partes interesadas.

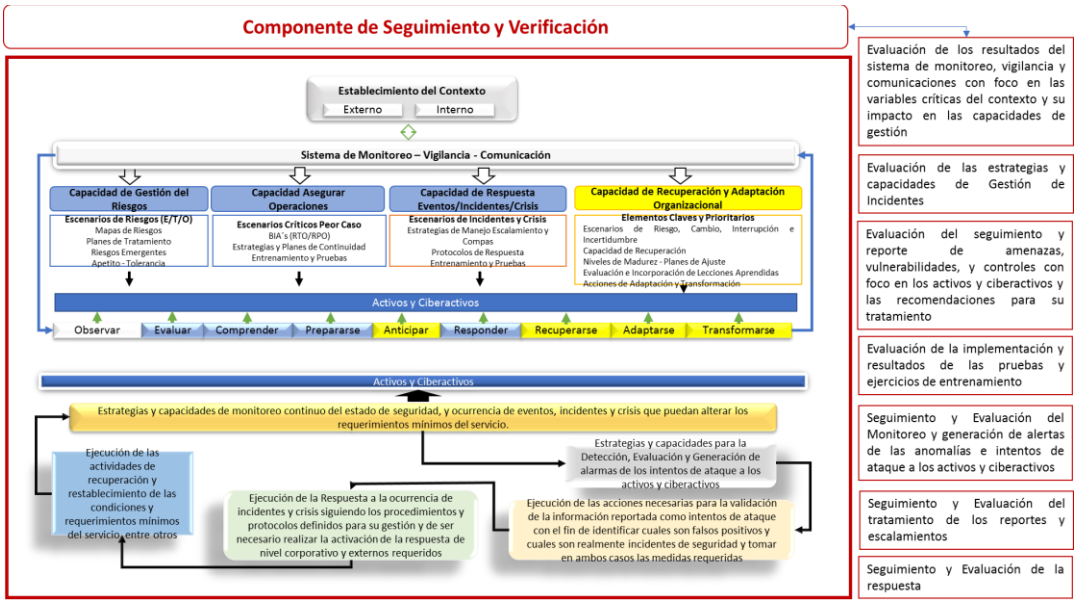
Tabla 3-16. Componente Seguimiento y verificación de la Gestión de Incidentes

Ciclo de Gestión - PHVA	Componente de Seguimiento y Verificación	Estructura de Alto Nivel ISO
V	• Realizar seguimientos y verificaciones continuas a las Evaluación de los resultados del sistema de monitoreo, vigilancia y comunicaciones con foco en las variables críticas del contexto y su impacto en las capacidades de gestión	• Evaluación • Desempeño

Ciclo de Gestión - PHVA	Componente de Seguimiento y Verificación	Estructura de Alto Nivel ISO
	• Evaluación de las estrategias y capacidades de Gestión de Incidentes • Evaluación del seguimiento y reporte de amenazas, vulnerabilidades, y controles con foco en los activos y ciber activos y las recomendaciones para su tratamiento • Evaluación de la implementación y resultados de las pruebas y ejercicios de entrenamiento • Seguimiento y Evaluación del Monitoreo y generación de alertas de las anomalías e intentos de ataque a los activos y ciber activos • Seguimiento y Evaluación del tratamiento de los reportes y escalamientos • Seguimiento y Evaluación de la respuesta • Evaluaciones del desempeño en la gestión de incidentes de ciberseguridad de la organización a través de los indicadores definidos	

Fuente: Elaboración propia

Figura 3-23: Actividades del Seguimiento y Verificación de la gestión de Incidente



Fuente: Elaboración propia

A continuación, se presenta los siguientes aspectos e insumos:

<u>Aspectos para tener en cuenta:</u>

1) Planes de tratamiento
2) Plan de pruebas, ejercicios y simulacros
3) Plan de auditorías
4) Evaluaciones e investigaciones sobre los incidentes de seguridad ocurridos.
5) Reportes de monitoreo y vulnerabilidades
6) Requerimientos, normatividad y aspectos legales que pueden aplicar
7) Actividades y requerimientos de terceros involucrados en la organización
8) Métricas y Acuerdos de Nivel de Servicio con los clientes internos y externos asociados a la gestión de incidentes

<u>Salida del componente del verificar de la Gestión de Incidentes.</u>

- Resultados de los seguimientos y verificaciones al sistema de monitoreo, vigilancia y comunicaciones con foco en las variables críticas del contexto y su impacto en las capacidades de gestión
- Ejecución, evaluación y entrega de resultados del Plan de pruebas, simulacros y ejercicios de entrenamiento para responder y recuperarse ante los eventos, incidentes y crisis.
- Ejecución, evaluación y entrega de resultados de las auditorias y evaluaciones del procedimiento de gestión de incidentes
- Resultados de los seguimientos y verificaciones de los análisis de amenazas, vulnerabilidades y controles realizados en el marco de la gestión de incidentes
- Resultados de los seguimientos y verificaciones de las estrategias y capacidades definidas e implementadas vs los riesgos en ciberseguridad
- Resultados de los seguimientos y verificaciones del cierre de brechas de ciberseguridad en los activos y ciber activos en términos de eficacia
- Resultados de los seguimientos y verificaciones del Monitoreo y generación de alertas de las anomalías e intentos de ataque a los activos y ciber activos y su gestión
- Resultados de los seguimientos y verificaciones de la activación y desempeño de la respuesta y recuperación de los eventos, incidentes y crisis materializados
- Resultados de los seguimientos y verificaciones del desempeño a través de las Métricas y Acuerdos de Nivel de Servicio pactados con los clientes internos y externos asociados a la gestión de incidentes
- Comunicar y compartir los resultados de las evaluaciones, investigaciones y auditorías realizadas a las partes involucradas en la gestión de incidentes.

4) Componente Ajuste y Mejoramiento Continuo de la Gestión de Incidentes (Actuar)

Descripción: Propender de forma permanente por el mejoramiento continuo de Ajuste de la idoneidad, cambio y eficacia de las diferentes capacidades, habilidades y estrategias en relación con la gestión de incidentes y su adecuada integración con los procesos que apoyan la operación en la organización. Para lograrlo es necesario que la organización

utilice los resultados de los diferentes seguimientos y verificaciones con el propósito de Identificar, documentar y socializar las lecciones aprendidas, realizar los mejoramientos y ajustes que correspondan en relación con la gestión de incidentes (Tabla 3-17 y Figura 3-24).

Esto con el fin de mejorar las capacidades de anticipar, responder, recuperarse, adaptarse y transformarse de acuerdo con las dinámicas y exigencias del entorno y su realidad operacional.

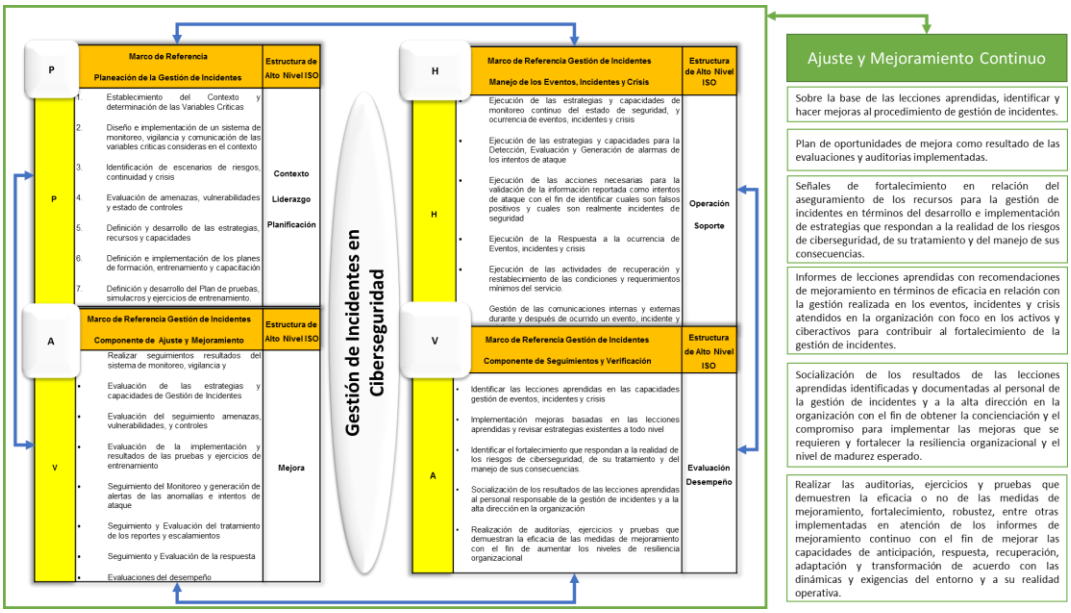
Tabla 3-17: Componente Ajuste y Mejoramiento Continuo de la Gestión de Incidentes

Ciclo de Gestión - PHVA	**Marco de Referencia Gestión de Incidentes Componente de Ajuste y Mejora Continua**	**Estructura de Alto Nivel ISO**
A	• Identificar las lecciones aprendidas en el desarrollo de actividades y capacidades en la gestión de eventos, incidentes y crisis • Implementación de las mejoras basadas en las lecciones aprendidas y revisar estrategias existentes a todo nivel • Identificar las necesidades de fortalecimiento necesarios para la gestión de incidentes en términos de las estrategias y capacidades que respondan a la realidad de los riesgos de ciberseguridad, de su tratamiento y del manejo de sus consecuencias. • Socialización de los resultados de las lecciones aprendidas identificadas y documentadas al personal responsable de la gestión de incidentes y a la alta dirección en la organización	• Mejora

Ciclo de Gestión - PHVA	Marco de Referencia Gestión de Incidentes Componente de Ajuste y Mejora Continua	Estructura de Alto Nivel ISO
	• Realización de auditorías, ejercicios y pruebas que demuestran la eficacia o no de las medidas de mejoramiento con el fin de aumentar los niveles de resiliencia organizacional	

Fuente: Elaboración propia

Figura 3-24: Actividades del Ajuste y Mejoramiento Continuo de la gestión de Incidente



Fuente: Elaboración propia

A continuación, se presenta los siguientes aspectos e insumos:

<u>Aspectos para tener en cuenta:</u>

1) Relación de los hallazgos y resultados de los seguimientos y verificaciones en relación con los niveles de ciberseguridad en los activos y ciber activos con el fin

de desarrollar acciones que permitan su implementación y rendición de cuentas en su cumplimiento.

2) Los objetivos de los negocio, estrategias y políticas, así como de los requerimientos mínimos del servicio que puedan verse impactados con la gestión de incidentes y puedan incluso afectar el cumplimiento regulatorio o los acuerdos de niveles de servicio existentes con los clientes y usuarios.
3) Asignación de los recursos, estrategias y capacidades para la gestión de incidentes con el fin de hacer frente a los riesgos de ciberseguridad y al manejo de sus consecuencias.
4) Revisiones de los eventos, incidentes y crisis atendidos en la organización con relación a los activos y ciber activos con el fin de conocer cómo fue la evaluación de la respuesta y recuperación, así como de los planes, procedimientos ejecutados, y herramientas utilizadas, con el fin de identificar puntos pendientes de mejoramiento.

Salida del componente del actuar de la Gestión de Incidentes.

- Sobre la base de las lecciones aprendidas, identificar y hacer mejoras al procedimiento de gestión de incidentes.
- Plan de oportunidades de mejora como resultado de las evaluaciones y auditorías implementadas.
- Señales de fortalecimiento en relación del aseguramiento de los recursos necesarios para la gestión de incidentes en términos del desarrollo e implementación de estrategias que respondan a la realidad de los riesgos de ciberseguridad, de su tratamiento y del manejo de sus consecuencias.
- Informes de lecciones aprendidas con recomendaciones de mejoramiento en términos de eficacia en relación con la gestión realizada en los eventos, incidentes y crisis atendidos en la organización con foco en los activos y ciberactivos para contribuir al fortalecimiento de la gestión de incidentes.
- Socialización de los resultados de las lecciones aprendidas identificadas y documentadas al personal responsable de la gestión de incidentes y a la alta dirección en la organización con el fin de obtener la concienciación y el

compromiso para las implementar las mejoras que se requieren y fortalecer la resiliencia organizacional y el nivel de madurez esperado.

- Realización de auditorías, ejercicios y pruebas que demuestran la eficacia o no de las medidas de mejoramiento, fortalecimiento, robustez, entre otras implementadas en atención de los informes de mejoramiento continuo con el fin de mejorar las capacidades de anticipar, responder, recuperarse. Adaptarse y transformarse de acuerdo con las dinámicas y exigencias del entorno y su realidad operacional

3.4.2 Actividad 2. Construir los instrumentos de validación

A continuación, se presenta el referenciamiento (Tabla 3-18) realizado a 3 prácticas para llevar a cabo ejercicios de simulación, vigentes en el mercado.

Tabla 3-18. Matriz de relaciones de los Referentes para los Ejercicios de Simulación y Simulacros

		Referentes Ejercicios de Simulación y Simulacros			
	Elementos a tener en cuenta para una Simulación	Consolidado	BQA	CD & A	Csirt Sector Electrico
1	Introducción	BQA	x		
2	Justificación	Csirt Sector Electrico - CD & A		x	x
3	Alcance	Csirt Sector Electrico - CD & A		x	x
4	Objetivos	Csirt Sector Electrico - BQA - CD & A	x	x	x
5	Enfoque	BQA - CD & A	x	x	
6	Tipo de ejercicio	BQA - CD & A	x	x	
7	Prerequisitos	Csirt Sector Electrico - CD & A		x	x
8	Supuestos	Csirt Sector Electrico			x
9	Identificar elemento crítico a evaluar	BQA - CD & A	x	x	
10	Definición de participantes y roles para el ejercicio.	Csirt Sector Electrico - BQA - CD & A	x	x	x
11	Facilitador	Csirt Sector Electrico - BQA - CD & A	x	x	x
12	Observador	Csirt Sector Electrico - BQA - CD & A	x	x	x
13	Evaluador	Csirt Sector Electrico - BQA - CD & A	x	x	x
14	Jugadores	Csirt Sector Electrico - BQA - CD & A	x	x	x
15	Guion (Trama)	Csirt Sector Electrico - BQA - CD & A	x	x	x
16	Escenario	Csirt Sector Electrico - BQA - CD & A	x	x	x
17	Línea de Tiempo	CD & A		x	
18	Eventos Principales (Hitos) Piezas Injects	Csirt Sector Electrico - CD & A		x	x
19	Mapa del Ejercicio	CD & A		x	
20	Análisis de Riesgos y plan de controles	CD & A		x	
21	Listas de Verificación	BQA - CD & A	x	x	
22	Ficha del Ejercicio	CD & A		x	
23	Ejecución de la Simulación	Csirt Sector Electrico - BQA - CD & A	x	x	x
24	Evaluación de la Simulación	Csirt Sector Electrico - BQA - CD & A	x	x	x
25	Lecciones aprendidas - Incorporación de mejoras y ajustes	Csirt Sector Electrico - BQA - CD & A	x	x	x

Fuente: Elaboración Propia

Como se puede observar cada referente le aporta al consolidado de referencia para la Guía, pero desde su alineación y claridad la fuente de BQA está más aterrizada a las necesidades empresariales de manera general y en lo especifico de la Ciberseguridad la fuente del Csirt del Sector

Con los elementos identificados en el referenciamiento de buenas prácticas, fue posible diseñar una Guía para llevar a cabo el Ejercicio de Simulación de un Caso de Estudio y tomar de cada referente lo que consideramos era relevante para la guía.

En el Anexo 8: Guía para llevar a cabo ejercicios de Simulación y Simulacros. Se encuentra el detalle de los siguientes ítems de la Guía desarrollada.

GUÍA PARA EL DISEÑO, EJECUCIÓN Y EVALUACIÓN EJERCICIOS DE SIMULACIÓN

1) Introducción
2) Justificación
3) Alcance
4) Objetivos
5) Enfoque
6) Tipo De Ejercicio
7) Prerrequisitos
8) Supuestos
9) Identificar Elemento Crítico A Evaluar
10) Definición De Participantes Y Roles Para El Ejercicio.
11) Facilitador
12) Observador
13) Evaluador
14) Jugadores
15) Guion (Trama)
16) Escenario
17) Línea De Tiempo
18) Eventos Principales (Hitos)
19) Mapa Del Ejercicio

20) Análisis De Riesgos Y Plan De Controles
21) Listas De Verificación
22) Ficha Del Ejercicio
23) Ejecución De La Simulación
24) Evaluación De La Simulación
25) Lecciones Aprendidas - Incorporación De Mejoras Y Ajustes

Con esta Guía se diseñaron los formatos que sirvieron para la validación del Procedimiento Gestión de Incidentes de Ciberseguridad en las Tecnologías de Operación, dichos formatos hacen parte de un ejercicio de simulación que se construyó, como se indicó, a través de un caso de estudio con el propósito de obtener los resultados de la actividad propuesta.

3.4.3 Actividad 3. Realizar el ejercicio de simulación

A continuación, se presenta el Caso de Estudio

1) Introducción

El proceso de responder a incidentes de ciberseguridad es crítico para el éxito de una organización que trabaja en el ciberespacio, esto incluye entender cómo funciona una organización bajo estrés.

Para esto es fundamental realizar ejercicios como las simulaciones utilizando estudios de caso que permitan verificar entre otras cosas la validez de los procedimientos, guías, protocolos e instructivos, en su coherencia y articulación con la respuesta corporativa como es el objetivo del trabajo de investigación.

2) Justificación

La simulación es un ejercicio que permite una reflexión colaborativa basada en eventos diseñados para evaluar procesos e interacción de las personas en la organización que

deben responder a un ciberataque a través de procedimientos, roles, articulación, coordinación, entre otros.

Para el caso de esta investigación el objetivo 4 planteado en el proyecto de investigación tiene que ver precisamente con la aplicación de un Caso de Estudio a través de un ejercicio de simulación que permita Validar el procedimiento de Gestión de Incidentes de Ciberseguridad y su articulación con la respuesta corporativa.

3) Alcance

El Caso de Estudio que se utilizó tuvo un alcance en los procesos productivos de Transmisión y Distribución de Energía Eléctrica de una empresa ficticia específicamente en los activos y ciberactivos de un Centro de Control y una Subestación de Distribución Energía, donde se observó la viabilidad de la implementación del Procedimiento Gestión de Incidentes, su articulación con el Protocolo de Respuesta Corporativa y los hallazgos obtenidos en su ejecución.

4) Objetivos de la Simulación

General: Validar la aplicación del nuevo procedimiento gestión de incidentes de ciberseguridad articulado con la respuesta a nivel corporativo y estratégico siguiendo el protocolo elaborado, ambos en el marco de la investigación y obtener las observaciones y recomendaciones de los participantes, como insumo para las conclusiones del trabajo de grado.

Objetivo específico:

1. Verificar el paso a paso para el diseño del ejercicio de simulación en el marco de la gestión de incidentes.
2. Validar si es posible implementar el procedimiento gestión de incidentes articulado con el protocolo de respuesta corporativa a eventos – incidentes – crisis, en el marco de los planes de prevención, preparación, respuesta y recuperación en la organización.

3. Obtener las conclusiones y recomendaciones por parte de los participantes del ejercicio de la simulación con miras a realizar los ajustes y mejoras en próximos ejercicios de simulación.

5) Enfoque

Realización de un Caso de Estudio con foco en ciberseguridad, que permita tanto, la evaluación del procedimiento gestión de incidentes, como de la articulación y escalamiento de la respuesta técnica/operativa con la respuesta de nivel corporativo que permita evidenciar las capacidades de gestión de eventos, incidentes y crisis organizacional.

6) Tipo de ejercicio

Ejercicio de simulación tipo exploratorio con fines de diagnóstico, orientados a probar la capacidad de gestión desde el análisis de las situaciones en el marco de la simulación, donde se busca la aplicación de criterios para toma de decisiones operativas, tácticas y estratégicas.

El ejercicio será avisado a los participantes con anterioridad de su ejecución y será en “Frio” (Paralelo) sin actuar sobre el proceso normal que no será afectado ni por la simulación ni por la acción de la respuesta.

7) Prerrequisitos

Requisitos previos que se deben garantizar para la realización del ejercicio de simulación, en un ambiente controlado y seguro en su ejecución.

- Requerimientos del ejercicio alineados con los requerimientos del procedimiento y protocolo a evaluar.
- Conocimiento previo de los asistentes de los procedimientos, protocolos, guías e instructivos a evaluar durante el ejercicio.

- Requisitos de seguridad previos a la realización de los ejercicios donde aplique tanto para las personas como para las instalaciones, procesos y servicios involucrados.
- Realización de un análisis de riesgos y determinación de controles para su implementación antes y durante la realización del ejercicio.
- Contar con los responsables designados para el ejercicio.
- Tener completos y disponibles los insumos de la planificación y preparación del ejercicio.
- Disponer de los recursos necesarios para su ejecución y evaluación.

8) Supuestos

Elementos para tener en cuenta en la narrativa del guion y la construcción de los escenarios a simular:

- Evento: ciberataque hacia la plataforma tecnológica (TO) que hace parte de la operación del servicio, generando una indisponibilidad, tales como un ransomware, un DoS/DDoS, inyección de código, entre otros.
- Modo (explotación de vulnerabilidades por atacantes internos y externos) y lugar (Empresa de Transmisión y Distribución Energía Eléctrica - Centro de Control - Subestación de Energía).
- Tiempo de ocurrencia (época de verano - fin de semana).
- Condiciones de la ocurrencia de los hechos (reducción del personal al interior del centro de control y subestación, con personal disponible en turno, se tiene en ejecución unos trabajos de mantenimiento programado con personal contratista al interior de la subestación).
- Respuestas esperadas para los eventos (activación del procedimiento Gestión de Incidentes y de la Respuesta Corporativa a través del protocolo definido)
- Estado de los controles (parciales en seguridad física y parciales en seguridad lógica).
- Tipos y alcance de las afectaciones (personas internas de la empresa y usuarios del servicio de energía, procesos de transmisión y distribución de energía eléctrica),

equipos asociados a las comunicaciones del centro de control, y del SCADA local de la subestación).

- Impactos que considerar (reputacional, información, discontinuidad del servicio, pérdidas financieras, legales, personas y comunidad).

9) Identificar Elemento Crítico a Evaluar

La implementación del Procedimiento Gestión de Incidentes y del escalamiento del nivel de respuesta técnico – operativo (áreas de la organización afectadas e involucradas y equipo de incidentes) con el Nivel de Respuesta Corporativo y Gerencial (equipo de crisis), su comunicación y toma de decisiones en la atención y recuperación del incidente y del manejo de crisis de la empresa.

10) Definición de Participantes y Roles para el Ejercicio

- Facilitador: Fredy Gómez
- Observador: Héctor Valencia
- Evaluador: Juan Guillermo Grajales, Héctor Valencia, Fredy Gómez
- Jugadores:
    - Personal Operación - Operador del Centro de Control y Subestaciones
    - Personal Equipo Respuesta a Incidentes – Csirt
    - Personal Nivel Táctico – Respuesta Corporativa – Logística, Seguros, Seguridad, Legal, Comunicaciones
    - Personal Nivel Estratégico

15) Guion (Trama)

Para el diseño del ejercicio se tomaron como referente varias situaciones del momento actual del país; 1) la situación de la pandemia por COVID 19, 2) el aumento del trabajo remoto 3) las dificultades de movilidad a las instalaciones y restricciones en los sitios de trabajo, 4) el aumento del consumo de energía en general, 5) la situación geopolítica de la

región, 6) la situación sociopolítica del país con la aparición de movilizaciones y 7) un año preelectoral.

A continuación, se diseña un guion que pretende ser una abstracción de la realidad a partir de la materialización de eventos adversos reflejados en varios riesgos de la empresa, del proceso y de los activos asociados, como; 1) fallas en la seguridad digital, y 2) errores u omisiones, y que tienen como consecuencia la interrupción de la prestación del servicio de energía eléctrica en varias regiones del país del sagrado corazón de Jesús.

El análisis multicausal de eventos adversos que se pueden desencadenar a partir de la materialización de los riesgos potenciales mencionados permitirá a los participantes del ejercicio la toma de decisiones desde los niveles operativos, táctico y estratégico, siguiendo los procedimientos de operación, gestión de incidentes y la respuesta corporativa asociada.

16) Escenario

Nos encontramos en el país del sagrado corazón de Jesús, es el año 2021 del 22 de Junio afectado por las altas temperaturas producto de la variabilidad climática, la temperatura promedio oscila entre los 25 y 30 grados centígrados, se vienen implementando nuevas políticas de operación en el país y el sector de energía asociados a los efectos de la pandemia del COVID 19, ejemplo de esta situación son las restricciones de movilidad supervisadas por la fuerza pública en todo el territorio, la implementación de las burbujas en los sitios de trabajo para evitar la proliferación de los contagios que lleven al cierre de conglomerados y el cambio a la modalidad de trabajo remoto en casa, intensificado con los mínimos desplazamientos a instalaciones.

Es un año complejo adicionalmente a estar próximos a una nueva elección presidencial, los efectos de la pandemia y las decisiones del gobierno para su manejo, han generado grandes movilizaciones y manifestaciones en general, las cuales han sido aprovechadas por actores políticos y grupos delincuenciales llevando a choques con las fuerzas del orden, lo que ha generado campañas masivas de desinformación en redes sociales, alimentando un

sentimiento de solidaridad por los abusos de la fuerza y la violación de los derechos humanos. Esto ha permitido que tanto grupos de hacktivistas realicen ataques a paginas oficiales del gobierno como de la mención de amenazas por parte de otros países de la región a la infraestructura critica de los sectores productivos como represalias a los abusos.

En este contexto se presenta el **escenario de ciberataque al centro de control que involucra a la subestación de maría auxiliadora con los apagones a las regiones de la luz, la estrella y la cascada, por un deslastre de carga**.

17) Eventos Principales (Hitos)

El ejercicio transcurrirá de manera gradual, con la aparición de eventos que permitirán la participación de los jugadores de acuerdo con los roles y a las funciones asignadas en los procedimientos y protocolos objeto de la verificación en la simulación.

Cada jugador de acuerdo con los roles y funciones asignadas deberán en cada evento, responder a las siguientes preguntas:

- ¿Cómo debería actuar de acuerdo con la información que acaba de llegar?
- ¿Qué decisiones debería tomar?
- ¿Debo comunicar?, ¿A quién lo debo hacer?, ¿Qué y cómo lo voy a comunicar?
- ¿Debo interactuar con otros jugadores?, ¿Qué dice el procedimiento o Protocolo?

Los eventos objeto de la simulación son en su orden:

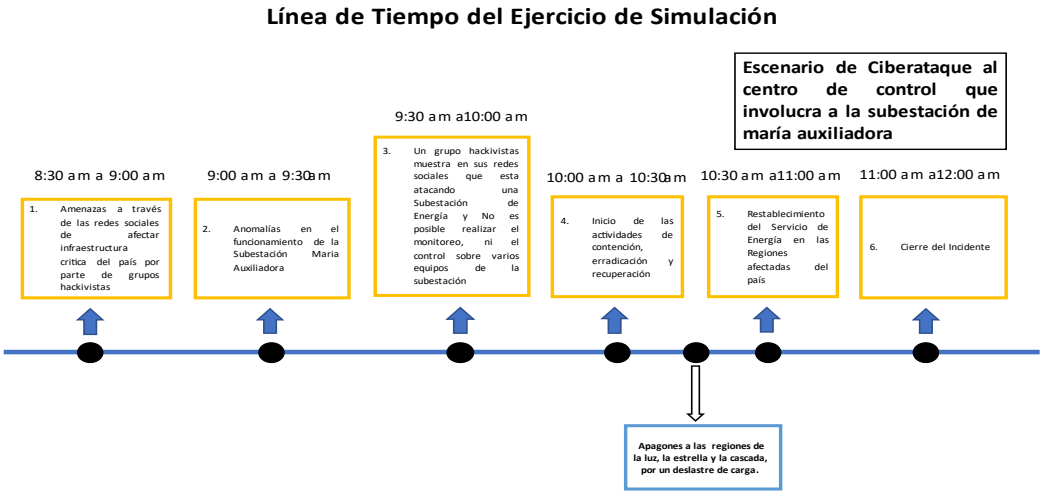
a. Amenazas a través de las redes sociales de afectar infraestructura critica del país por parte de grupos hacktivistas
b. Anomalías en el funcionamiento de la Subestación Maria Auxiliadora
c. Un grupo hacktivistas muestra en sus redes sociales que está atacando una Subestación de Energía y no es posible realizar el monitoreo, ni el control sobre varios equipos de la subestación.

d. Inicio de las actividades de contención, erradicación y recuperación
e. Restablecimiento del Servicio de Energía en las Regiones afectadas del país
f. Cierre del incidente

18) Líneas de tiempo

En la siguiente Figura 3-25 se hace una relación de la línea de tiempo del evento.

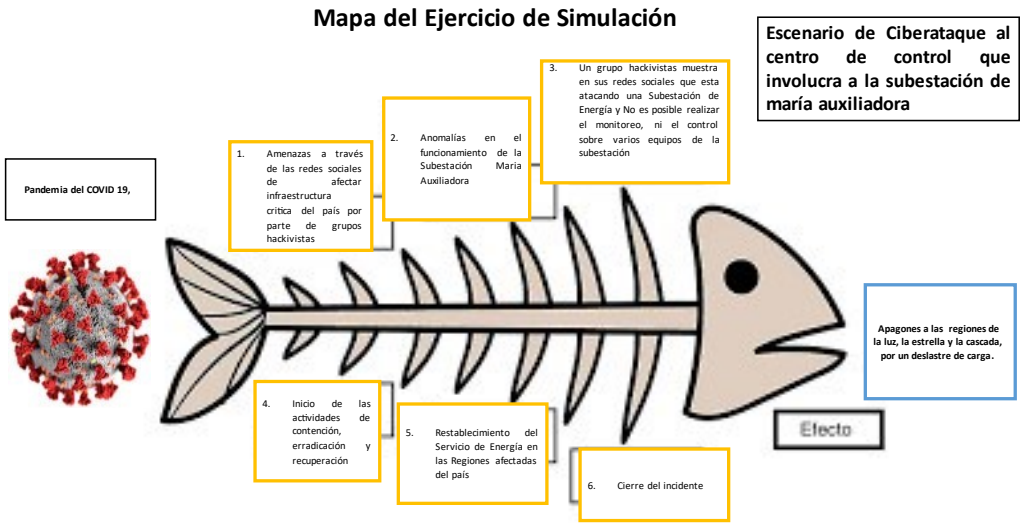
Figura 3-25 Línea de Tiempo del Ejercicio de Simulación



Fuente: Elaboración propia.

19) Mapa del ejercicio

Figura 3-26. Mapa del Ejercicio de Simulación



Fuente: Elaboración Propia

La Figura 3-26 del mapa del ejercicio como se observa, muestra de manera general todos los elementos presentes en el ejercicio de simulación, con el objetivo de que el facilitador pueda identificar que el desarrollo se esté llevando de la manera adecuada y le sirva a la vez para las observaciones y conclusiones del ejercicio

20) Análisis de Riesgos y Plan de Controles

El ejercicio de simulación será realizado en los procesos de transmisión y distribución de energía eléctrica, en los activos de la empresa el DESTELLO E.S.P. ubicada en la Meseta con los activos del Centro de Control XYZ y la Subestación Maria Auxiliadora.

En este punto es importante tener en cuenta la manera cómo será llevado a cabo dicho ejercicio de simulación que para este caso será de tipo exploratorio con fines de diagnóstico, orientados a probar la capacidad de gestión desde el análisis de las situaciones en el marco de la simulación, donde se busca la aplicación de criterios para toma de

decisiones operativas, tácticas y estratégicas en relación con la operación, la gestión de incidentes y la respuesta corporativa asociada.

El ejercicio será avisado a los participantes con anterioridad de su ejecución y será en “Frio” (Paralelo) sin actuar sobre el proceso normal que no será afectado ni por la simulación ni por la acción de la respuesta.

Los riesgos que se identifican están asociados a las ayudas didácticas que serán utilizados para ambientar el escenario hipotético como son los videos, mensajes de texto, la utilización simulada de redes sociales con mensajes ficticios de los atacantes.

En ese punto los controles identificados estarán asociado a:

- Los videos, mensajes y otros asociados a la ambientación didáctica, no serán compartidos con nadie diferente del equipo de planeación y preparación del ejercicio
- Los videos, mensajes y otros asociados estarán almacenados en un sitio seguro para evitar su acceso no autorizado.
- La utilización de estos será solo en el momento de la ejecución de la simulación y previo a su proyección se harán las advertencias y observaciones para que no se divulguen por fuera del ejercicio y de los participantes.
- Las comunicaciones que se utilicen al interior de los jugadores involucrados en el ejercicio en relación con los eventos que se están presentando hipotéticamente, solo será entre estos participantes y no deberán salir a otros medios o personas para evitar desinformación y pánico ante hechos no reales.

21) Lista de verificación

En la Tabla 3-19 se entregan los resultados obtenidos del análisis del evento.

Tabla 3-19. Lista de Verificación de Elementos Claves de la Simulación

Lista de Chequeo de la simulación				
Tipo y nombre del ejercicio	**Simulación de respuesta ante un ataque cibernético a la infraestructura tecnológica en la Empresa Destello E.S.P.**			
Lugar	Reunion Teams - Salon social Urbanización Veleros	**Fecha**	22 de Junio de 2021	
Responsable	Fredy Humberto Gómez - Hector Valencia V.	**Hora**	8:00am a 12:00 m	
Aspectos generales				**Estado**
Propósito	Verificar los elementos minimos necesarios para llevar a cabo el ejercicio de simulación			
Areas Participantes	Operación - Equipo Gestión Incidentes - Equipo Respuesta Corporativo (Comunicaciones, Logistica, Legal, Seguros - Equipo Respuesta Crisis (Gerente General, Directivo Transmisión y Distribución)			Ok
Fecha de la simulación	22 de Junio de 2021 de 8:00am a 12:00pm			Ok
Descripción del lugar o lugares donde se va a realizar	Reunion virtual en la plataforma Teams y Salon Social Urbanización			Ok
Alarma de inicio del ejercicio	Se conoce en las redes sociales, y por organismos de control de un comunicado de un grupo hackivista anonymous con un video indicando que están inconformes con la administración de los dirigentes de la ciudad y que se tiene control de la red de energía advirtiendo que si al finalizar el día no se presenta renuncia del alcalde empezará a darse apagones en toda la ciudad, el departamento y el país.			Ok
Señal de finalización	EL equipo de respuesta a incidentes, informara que el incidente esta contenido y recuperado y que se puede iniciar con la fase de actividades posteriores			Ok
Recursos humanos	1 facilitador, 1 observador, 2 evaluadores, 1 integrante del equipo de respuesta a incidentes, 1 integrante de la respuesta corporativa y 1 integrante del Equipo de Crisis			Ok
Otros recursos	PC´s, Pantallas de Proyección (Tv), Tablero y Marcadores, Telefono, Celulares			Ok
Facilitador	Fredy Humberto Gómez Orjuela			Ok
Observadores	Hector Valencia Valencia			Ok
Evaluador	Fredy Humberto Gómez Orjuela - Hector Valencia Valencia			Ok
Jugadores	Personal Operación - Operador del Centro de Control y Subestaciones, Personal Equipo Respuesta a Incidentes – Csirt, Personal Nivel Táctico – Respuesta Corporativa – Logística, Seguros, Seguridad, Legal, Comunicaciones y Personal Nivel Estratégico – Respuesta Equipo de Crisis – Gerente General			Ok
Guion	Terminado y Disponible			Ok
Eventos	Identificados, redactados			Ok
Linea de Tiempo	Establecida			Ok
Mensajes	Identificados, redactados			Ok
Videos - Mensajes Redes Sociales y otros de ayuda didactica para la ambientación del Ejercicio	Terminado y Disponible			Ok

Fuente: Elaboración Propia

22) Ficha Del Ejercicio

Tabla 3-20. Ficha Técnica del Ejercicio de Simulación

1. Ficha técnica de la simulación			
Tipo y nombre del ejercicio	**Simulación de respuesta ante un ataque cibernético a la infraestructura tecnológica en la Empresa Destello E.S. P.**		
Areas involucradas	Operación - Equipo Gestión Incidentes - Equipo Respuesta Corporativo (Comunicaciones, Logistica, Legal, Seguros - Equipo Respuesta Crisis (Gerente General, Directivo Transmisión y Distribución)		
Lugar	Reunion Teams - Salon social Urbanización Veleros.	**Fecha**	22 de Junio de 2021
Responsable	Fredy Humberto Gómez - Hector Valencia V.	**Hora**	8:00am a 12:00 m
Aspectos generales			
Propósito	Validar la aplicación del nuevo procedimiento gestión de incidentes de ciberseguridad articulado con la respuesta a nivel corporativo y estratégico siguiendo el protocolo elaborado, ambos en el marco de la investigación y obtener las observaciones y recomendaciones de los participantes, como insumo para las conclusiones del trabajo de grado.		
Objetivos específicos	1.Verificar el paso a paso para el diseño del ejercicio de simulación en el marco de la gestión de incidentes. 2.Validar si es posible implementar el procedimiento gestión de incidentes articulado con el protocolo de respuesta corporativa a eventos – incidentes – crisis, en el marco de los planes de prevención, preparación, respuesta y recuperación en la organización. 3.Obtener las conclusiones y recomendaciones por parte de los participantes del ejercicio de la simulación con miras a realizar los ajustes y mejoras en próximos ejercicios de simulación.		
Modalidad del simulacro	Ejercicio de simulación tipo exploratorio con fines de diagnóstico, orientados a probar la capacidad de gestión desde el análisis de las situaciones en el marco de la simulación, donde se busca la aplicación de criterios para toma de decisiones operativas, tácticas y estratégicas. El ejercicio será avisado a los participantes con anterioridad de su ejecución y será en "Frio" (Paralelo) sin actuar sobre el proceso normal que no será afectado ni por la simulación ni por la acción de la respuesta.		
Areas Participantes	Operación - Equipo Gestión Incidentes - Equipo Respuesta Corporativo (Comunicaciones, Logistica, Legal, Seguros - Equipo Respuesta Crisis (Gerente General, Directivo Transmisión y Distribución)		
Fecha de la simulación	22 de Junio de 2021 8:00am a 12:00 m		
Descripción del lugar o lugares donde se va a realizar	Reunion Teams - Salon social Urbanización.		
Descripción breve y detallada de la situación incluyendo los eventos que se simularán y su ubicación gráfica	Para el diseño del ejercicio se tomaron como referente varias situaciones del momento actual del país; 1) la situación de la pandemia por COVID 19, 2) el aumento del trabajo remoto 3) las dificultades de movilidad a las instalaciones y restricciones en los sitios de trabajo, 4) el aumento del consumo de energía en general, 5) la situación geopolítica de la región, 6) la situación sociopolítica del país con la aparición de movilizaciones y 7) un año preelectoral. En este contexto se presenta el escenario de ciberataque al centro de control que involucra a la subestación de maría auxiliadora con los apagones a las regiones de la luz, la estrella y la cascada, por un deslastre de carga.		
Alarma de inicio del ejercicio	Se conocen de amenazas a través de las redes sociales de afectar infraestructura critica del país por parte de grupos hacktivistas		
Señal de finalización	Se inician acciones de contención de eventos de ciberseguridad y el Restablecimiento del Servicio de Energía en las Regiones afectadas del país		
Consecuencias	Apagones a las regiones de la luz, la estrella y la cascada, por un deslastre de carga.		
Observaciones			

Fuente: Elaboración Propia

23) Ejecución de La Simulación

Tabla 3-21. Formato de Ejecución de la Simulación

Ejecución de la Simulación				
Tipo y nombre del ejercicio	**Simulación de respuesta ante un ataque cibernético a la infraestructura tecnológica en la Empresa Destello E.S. P.**			
Instituciones involucradas	Operación - Equipo Gestión Incidentes - Equipo Respuesta Corporativo (Comunicaciones, Logística, Legal, Seguros - Equipo Respuesta Crisis (Gerente General, Directivo Transmisión y Distribución)			
Lugar	Reunión Teams - Salón social Urbanización XXX.	**Fecha**	22 de junio de 2021	
Responsable	Fredy Humberto Gómez - Héctor Valencia V.	**Hora**	8:00am a 12:00m	
GUION				
Hora	**Evento**	**Acción Por Tomar**	**Duración**	**Responsable**

8:00 a.m.	Inicio de reunión y bienvenida al ejercicio de simulación	1. Iniciar la reunión de Teams 2. Validar la asistencia de los jugadores y de los demás participantes de la simulación	10 minutos	Fredy Humberto Gómez - Héctor Valencia V.
8:11 a.m.	Realizar presentación del ejercicio de simulación	1. Realizar presentación del ejercicio de simulación	10 minutos	Fredy Humberto Gómez - Héctor Valencia V.
8:21 a.m.	Se asumen los roles de la simulación	1. Presentar el Contexto	4 minutos	Fredy Humberto Gómez - Héctor Valencia V.
8:30 am - 9:00 am	Se inicia con el Primer evento	Presentar el video del evento 1	5 minutos	Fredy Gómez Héctor Valencia V.
Se publica un video tipo Anonymous indicando que está inconforme con la administración del alcalde y que se tiene control de la red de energía y que si al finalizar el día no se presenta renuncia del alcalde empezará a darse apagones en toda la ciudad, el departamento y el país.				
ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo		**ACCIONES REALIZADAS en atención del evento**		**OBVSERVACIONES**

Procedimiento Gestión Incidentes • **Iniciar el procedimiento de gestión de incidentes de Ciberseguridad** ○ Evaluación de la posible amenaza desde el Sistema de Monitoreo del Entorno y desde los escenarios de riesgos identificados y valorados en su impacto. ○ Identificación de los Activos y Ciber activos que se pueden ver expuestos por la amenaza anunciada. ○ Determinar posibles vulnerabilidades que pueden ser explotadas y el estado de controles asociados. ○ Identificación de los planes y estrategias definidas para la gestión del potencial incidente. ○ Ejecución de las estrategias y capacidades de monitoreo continuo del estado de seguridad, y ocurrencia de eventos, incidentes y crisis que puedan alterar los requerimientos mínimos del servicio.	• Al inicio no son claros los roles y el arranque se hace lento. • En el transcurso del análisis y toma de decisiones se plantea la instalación temprana de un Puesto de Mando Unificado con el fin de buscar los recursos especializados para el manejo de una eventual emergencia y contingencia. • Se decide activar el equipo de repuesta a incidentes con el fin de evaluar la realidad de la amenaza y el potencial de daño del grupo que lo genera. • Se revisa la situación actual tanto del Centro de Control como de las Subestaciones asociadas y el estado de controles. • Se decide esperar la evaluación para nuevas acciones. • Se comunica la situación a la sala de seguridad y al personal de operación de	El Puesto de Mando Unificado (PMU) es un organismo temporal encargado de la coordinación, organización y control durante la fase de emergencia posterior al impacto; su creación facilita las labores de salvamento, administración y atención en salud de los lesionados, la evacuación de los afectados y la racionalidad del recurso humano y técnico. Para el evento en concreto de la simulación, no es necesario realizar esta activación, porque es un tema que requiere primero de la validación y segundo de la evaluación del posible impacto dada las características de este. El paso inicial como lo menciona el procedimiento gestión de incidentes es el de activar al equipo de respuesta como se hizo y con ellos realizar la validación de la

○ Ejecución de las estrategias y capacidades para la Detección, Evaluación y Generación de alarmas de los intentos de ataque a los activos y ciber activos. ○ Ejecución de las acciones necesarias para la validación de la información reportada como intentos de ataque con el fin de identificar cuáles son falsos positivos y cuales son realmente incidentes de seguridad clasificarlo y tomar en ambos casos las medidas requeridas. ○ Gestión de las comunicaciones internas y externas durante y después de la ocurrencia de eventos, incidentes y crisis.		las áreas que potencialmente se pueden ver afectadas.	veracidad y capacidad del posible atacante, determinar los activos potencialmente involucrados y las posibles consecuencias, y es en ese punto donde se analiza si un PMU es necesario y en qué momento montarlo. Por lo demás se cumplió en la mayoría las actividades esperadas.	
9:00 am - 9:30 am	Se inicia con el segundo evento	Presentar el evento 2	3 minutos	Fredy Gómez - Héctor Valencia V.
Anomalías en el funcionamiento de la Subestación Maria Auxiliadora.				
ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo		**ACCIONES REALIZADAS en atención del evento**	**OBVSERVACIONES**	

Procedimiento Gestión Incidentes ○ Declaración del Incidente de Seguridad. ○ Ejecución de la Respuesta a la ocurrencia de Eventos, incidentes y crisis siguiendo los procedimientos y protocolos definidos para su gestión. ○ Realizar la activación de la respuesta de nivel corporativo y externos requeridos. ○ Gestión de las comunicaciones internas y externas durante y después de la ocurrencia de eventos, incidentes y crisis. **Protocolo de Respuesta Corporativa** ○ Clasificación de los Eventos, Incidentes y Crisis de acuerdo con la intensidad y gradualidad de los efectos que los eventos, incidentes y crisis pueden generar en la empresa y su entorno. ○ Planes, protocolos, guías y recursos necesarios para la atención de un evento,	• Una vez se evalúa la amenaza se llega a la conclusión que es real y que el grupo tiene el potencial para llevarla a cabo. • Sumado a la situación de anormalidad en la Subestación se decide declarar el evento inicial como un Incidente de Ciberseguridad. • Se realiza la comunicación al enlace del área afectada para que se activen los planes de contingencia necesarios para complementar las acciones técnicas y mantener en lo posible la operación del servicio. • Se lleva la primera evaluación al PMU que ya se encuentra activo y en conjunto deciden activar el protocolo de respuesta corporativo con el fin de sumar recursos de nivel corporativo que se encarguen de las consecuencias que pueden volverse críticas.	El equipo de participantes se encuentra en este momento más ubicados en los roles y en la toma de decisiones. Un tema que se debe revisar es la decisión de activación del Protocolo de Respuesta de Nivel Corporativo, el cual de acuerdo con el Procedimiento Gestión de Incidentes y reconociendo que es un incidente de Ciberseguridad, es para este caso el líder del equipo de respuesta con el líder del área afectada quienes determinan cuando activar dicho protocolo. Para el caso de ejercicio de simulación fue en el PMU donde se llevó la información y se toma dicha decisión. Otro tema que no se puede perder de vista son las restricciones de movilidad por los efectos del COVID 19 en la empresa y lo que implica en los desplazamientos a las

incidente o crisis. De acuerdo con el nivel de gradualidad de los efectos, se deberán activar en la organización. ○ Activación de los pasos de la gestión del evento, incidente y crisis; PASÓ 1 - Comunicar Evento, PASÓ 2 - Activar cadena de llamadas, PASÓ 3 - Evaluar situación, PASÓ 4 - Atención del evento.		• El equipo de nivel táctico se reúne para realizar la evaluación de la situación y determinar en relación con los efectos potenciales cual puede ser la intensidad y gradualidad del incidente en curso. • Se revisan los planes que se deben activar en apoyo a la atención del incidente. • Se generan los primeros boletines de comunicación tanto al interior como al exterior de la organización.	instalaciones siguiendo los protocolos vigentes. Ya en este punto las actividades que se ejecutan a continuación corresponden a las acciones esperadas tanto en el procedimiento Gestión de Incidentes como del Protocolo de Respuesta Corporativo.	
9:30 - 10:00 am	Se inicia con el tercer evento	Presentar el evento 3	3 minutos	Fredy Gómez - Héctor Valencia V.
Un grupo hacktivistas muestra en sus redes sociales que está atacando una Subestación de Energía y no es posible realizar el monitoreo, ni el control sobre varios equipos de la subestación.				
ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo		**ACCIONES REALIZADAS en atención del evento**	**OBVSERVACIONES**	

Procedimiento Gestión Incidentes ○ Ejecución de la respuesta a la ocurrencia de eventos, incidentes y crisis siguiendo los procedimientos y protocolos definidos para su gestión. ○ Realizar la activación de la respuesta de nivel corporativo y externos requeridos. ○ Gestión de las comunicaciones internas y externas durante y después de la ocurrencia de eventos, incidentes y crisis. **Protocolo de Respuesta Corporativa** ○ Clasificación de los eventos, incidentes y crisis de acuerdo con la intensidad y gradualidad de los efectos que los eventos, incidentes y crisis pueden generar en la empresa y su entorno. ○ Planes, protocolos, guías y recursos necesarios para la atención de un evento,	• El equipo de respuesta a incidentes de ciberseguridad está verificando que la anormalidad sea causada por un ciberataque, determinar los indicadores de compromiso, los ciber activos que están comprometidos. • Se inician las actividades de detección y evaluación. • Se continua con el monitoreo a través de redes sociales y páginas utilizadas por el atacante. • Se están desplazando al sitio cuadrillas de mantenimiento para verificar las restricciones de las operaciones remotas y continuar de manera temporal con la operación en mando local. • Se activan las cadenas de llamadas a Proveedores y Contratistas.	El PMU ya con el Protocolo de Respuesta Corporativa activo, el equipo táctico de Nivel 2 y el equipo de respuesta a incidentes, se considera que ya no es relevante y se debería desmontar hasta nueva orden para evitar duplicidad de acciones y decisiones que pueden entrar en contravía con el incidente en curso. Las actividades que se ejecutan a continuación corresponden a las acciones esperadas tanto en el procedimiento Gestión de Incidentes como del Protocolo de Respuesta Corporativo Se observa mayor dinamismo y compenetración del equipo de participantes, se enfocan en las actividades de evaluación y de tipo correctivo, ante la dificultad del Transformador.

incidente o crisis. De acuerdo con el nivel de gradualidad de los efectos, se deberán activar en la organización. ○ Activación de los pasos de la gestión del evento, incidente y crisis; PASÓ 1 - Comunicar evento, PASÓ 2 - Activar cadena de llamadas, PASÓ 3 - Evaluar situación, PASÓ 4 - Atención del evento.		• Se reporta la novedad al PMU y se comunica igualmente al Equipo de nivel táctico de la situación. • Se recibe reporte de las cuadrillas en sitio de la imposibilidad de operar y controlar el transformador de la Subestación. • Se realiza comunicación de la situación de la Subestación al líder del equipo de respuesta a incidentes, al jefe de emergencias de la instalación afectada y al líder del equipo táctico de Respuesta Corporativa con el fin de evaluar los pasos a seguir.	Se observa tres acciones en este punto del ejercicio, los que atienden el incidente de ciberseguridad, los que están atendiendo la operación y los que están atendiendo los efectos y consecuencias en el servicio.	
10:00 am - 10:30 am	Se inicia con el cuarto evento	Presentar el evento 3	3 minutos	Fredy Gómez - Héctor Valencia V.
Inicio de las actividades de contención, erradicación y recuperación.				
ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo		**ACCIONES REALIZADAS en atención del evento**	**OBVSERVACIONES**	

Procedimiento Gestión Incidentes ○ Ejecución de la Respuesta a la ocurrencia de eventos, incidentes y crisis siguiendo los procedimientos y protocolos definidos para su gestión. ○ Realizar la activación de la respuesta de nivel corporativo y externos requeridos. ○ Gestión de las comunicaciones internas y externas durante y después de la ocurrencia de eventos, incidentes y crisis. **Protocolo de Respuesta Corporativa** ○ Clasificación de los eventos, incidentes y crisis de acuerdo con la intensidad y gradualidad de los efectos que los eventos, incidentes y crisis pueden generar en la empresa y su entorno. ○ Planes, protocolos, guías y recursos necesarios para la atención de un evento,	• Se inicia con las actividades de contención, erradicación y recuperación de la subestación. • Se reporta por parte de las cuadrillas en sitio que se desconoce si pueden existir otras instalaciones comprometidas. • El centro de Control no reporta novedades de otras anomalías en el sistema. • Se toma la decisión de activar al Equipo de Crisis Gerencial. • Por prevención se toma la decisión entre los equipos en sitio, el equipo táctico y el equipo de crisis, de interrumpir la conectividad entre el centro de control y la subestación para evitar acciones de comando y control por parte del atacante. • El equipo de nivel táctico y el equipo de crisis, en coordinación con el Jefe de	Las actividades que se ejecutan a continuación corresponden a las acciones esperadas tanto en el procedimiento Gestión de Incidentes como del Protocolo de Respuesta Corporativo. Es importante mencionar la articulación y comunicación del equipo participante para llegar a los acuerdos en la toma de decisiones.

incidente o crisis. De acuerdo con el nivel de gradualidad de los efectos, se deberán activar en la organización. ○ Activación de los pasos de la gestión del evento, incidente y crisis; PASÓ 1 - Comunicar evento, PASÓ 2 - Activar cadena de llamadas, PASÓ 3 - Evaluar situación, PASÓ 4 - Atención del evento.		Emergencias deciden interrumpir el servicio en la subestación para tener aislamiento y comenzar con las acciones de recuperación. • Debido a la interrupción del Servicio desde la Subestación los Sectores la luz, la estrella y la cascada quedan temporalmente sin energía. • Se elaboran nuevos comunicados del avance de la situación por parte de la organización tanto interno como externo. • Se entra en coordinación con el personal del ejército a través del convenio para la defensa de infraestructura critica.		
10:30 am - 11:00 am	Se inicia con el quinto evento	Presentar el evento 3	3 minutos	Fredy Gómez - Héctor Valencia V.
Restablecimiento del Servicio de Energía en las regiones afectadas del país.				

ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo	ACCIONES REALIZADAS en atención del evento	OBVSERVACIONES
Procedimiento Gestión Incidentes ○ Ejecución de las actividades de recuperación y restablecimiento de las condiciones y requerimientos mínimos del servicio, entre otros. ○ Gestión de las comunicaciones internas y externas durante y después de la ocurrencia de eventos, incidentes y crisis. **Protocolo de Respuesta Corporativa** ○ Seguimiento y evaluación de la respuesta. ○ Identificar las lecciones aprendidas en el desarrollo de actividades y capacidades en la gestión de eventos, incidentes y crisis.	• Se encuentran en coordinación y gestión del incidente, el personal de operación, el equipo de respuesta a incidentes, el equipo táctico, el equipo de crisis. • Se están manejando las acciones de recuperación del activo en conjunto con el Csirt del Sector y el Coordinador nacional de energía del país para la conexión de los activos al Sistema (Xm). • Se está dando reporte del incidente a los organismos competentes. • Se continua en la coordinación de acciones con el Comando Conjunto Cibernético. • Se elaboran últimos reportes desde la organización para los diferentes Grupos de Interés.	Las actividades que se ejecutan a continuación corresponden a las acciones esperadas tanto en el procedimiento Gestión de Incidentes como del Protocolo de Respuesta Corporativo. Es importante mencionar la inclusión de nuevos actores desde las decisiones que el equipo de participantes menciona en atención y evolución del incidente de ciberseguridad.

		• Se restablece el servicio de energía.		
11:00 am - 12:00 am	Se inicia con el Cierre del Ejercicio	Presentar Evaluación del Ejercicio y Cierre	5 minutos	Fredy Gómez - Héctor Valencia V.
Cierre del Incidente				
ACCIONES ESPERADAS Procedimiento Gestión Incidentes y del Protocolo de Respuesta Corporativo		**ACCIONES REALIZADAS en atención del evento**	**OBVSERVACIONES**	
Procedimiento Gestión Incidentes ○ Gestión de las comunicaciones internas y externas durante y después de la ocurrencia de eventos, incidentes y crisis. ○ Identificación de las lecciones aprendidas en el desarrollo de actividades y capacidades en la gestión de eventos, incidentes y crisis. ○ Implementación de las mejoras basadas en las lecciones aprendidas y revisar estrategias existentes a todo nivel. ○ Identificar las necesidades de fortalecimiento necesarios para la gestión de incidentes en términos de las estrategias y		• Seguimiento y Evaluación del tratamiento de los reportes y escalamientos. • Seguimiento y Evaluación de la respuesta. • Identificación de temas pendientes en la recuperación y regreso a la normalidad. • Reunión de evaluación de la atención del Incidente con los diferentes grupos de trabajo involucrados. • Identificación de asuntos por corregir, mejorar y potenciar.	Gran parte de las acciones esperadas se mencionan por el equipo de participantes del ejercicio de simulación, quedaron pendientes el cierre de comunicaciones tanto internas como externas, la atención y validación de la eficacia de las recomendaciones y mejoras que salen de la evaluación, la identificación de las necesidades de fortalecimiento a todo nivel luego del análisis del incidente ocurrido, socialización de los resultados de las lecciones aprendidas, la conservación de las evidencias (informes del evento) para tener un soporte ante las solicitudes	

capacidades que respondan a la realidad de los riesgos de ciberseguridad, de su tratamiento y del manejo de sus consecuencias. o Socialización de los resultados de las lecciones aprendidas identificadas y documentadas al personal responsable de la gestión de incidentes y a la alta dirección en la organización. o Realización de auditorías, ejercicios y pruebas que demuestran la eficacia o no de las medidas de mejoramiento con el fin de aumentar los niveles de resiliencia organizacional. **Protocolo de Respuesta Corporativa** **PASÓ 5 - Cierre del evento:** Se debe elaborar un informe describiendo los hechos sucedidos por las personas que los presenciaron y solucionaron. Este informe debe contener las lecciones aprendidas y su	• Elaboración del informe de cierre para los interesados con las recomendaciones de los equipos de respuesta para la atención de brechas de seguridad, temas que requieren de un fortalecimiento a nivel general en la organización.	de los entes de control, posibles reclamaciones de compañías aseguradoras y solicitudes de otros interesados y la realización de las auditorias y pruebas del nivel de resiliencia alcanzado posterior al incidente ocurrido en la organización.

socialización, mejoras a los procedimientos del proceso o áreas afectadas: o Recolectar información (pruebas, hechos, costos, entre otros), elaborar y entregar informe a los interesados. o Evaluar y evidenciar las acciones realizadas en la atención del evento y sus consecuencias. o Incorporar lecciones aprendidas. o Continuar con la atención de las necesidades de la población afectada. o Conservar las evidencias (informes del evento) para tener un soporte ante las solicitudes de los entes de control, posibles reclamaciones de compañías aseguradoras y solicitudes de otros interesados. o Regresar a la normalidad bajo estándares de calidad y confiabilidad.		

Fuente: Elaboración Propia

24) Evaluación De La Simulación

Tabla 3-22. Formato de Evaluación de la Simulación

Evaluación de la Simulación				
Tipo y nombre del ejercicio	**Simulación de respuesta ante un ataque cibernético a la infraestructura tecnológica en la Empresa Destello E.S. P.**			
Instituciones involucradas	Operación - Equipo Gestión Incidentes - Equipo Respuesta Corporativo (Comunicaciones, Logística, Legal, Seguros - Equipo Respuesta Crisis (Gerente General, Directivo Transmisión y Distribución)			
Lugar	Reunión Teams - Salón social Urbanización XXX.	**Fecha**	22 de junio de 2021	
Responsable	Fredy Humberto Gómez - Héctor Valencia V – Juan F. Grajales	**Hora**	8:00am a 12:00m	
Evaluación del Ejercicio de Simulación				
El ejercicio de simulación realizado sirvió para validar la aplicación del nuevo procedimiento gestión de incidentes de ciberseguridad y su articulación con la respuesta a nivel corporativo siguiendo el protocolo elaborado para tal fin, ambos en el marco de la investigación, a partir de un equipo de participantes que de acuerdo con unos roles asignados durante la ejecución del ejercicio lo que permitió al equipo evaluador concluir que los objetivos planteados en la simulación se cumplieron.				

Evaluación del Procedimiento Gestión de Incidentes vs Caso de Estudio
De acuerdo con las observaciones consignadas en las fases de ejecución y evaluación del ejercicio de simulación por parte de los participantes y de acuerdo con sus roles de observador y evaluador, se puede concluir que la mayoría de las actividades definidas en el procedimiento de Gestión de Incidentes, se ejecutaron. Esto significa que, desde lo procedimental, técnico y metodológico, el procedimiento funciona y es factible de implementar en cualquier tipo de organización. El aporte de este nuevo procedimiento es que integra la gestión en el antes, durante y después del evento, articulándose con la respuesta corporativa para ser más eficaces en la atención, coordinación de los recursos y mejorando la comunicación con las partes interesadas, así como disminuyendo las consecuencias y protegiendo la imagen y reputación de la organización.
Evaluación del Protocolo de Respuesta Corporativa Vs Caso de Estudio
De acuerdo con las observaciones consignadas en las fases de ejecución y evaluación del ejercicio de simulación por parte de los participantes y de acuerdo con sus roles de observador y evaluador, se puede concluir que la mayoría de las actividades definidas en el procedimiento de respuesta corporativo, se ejecutaron. Esto significa que, desde lo procedimental, técnico y metodológico, el procedimiento funciona y se articula con el procedimiento de Gestión de Incidentes, lo que trae como beneficio para la organización una mejor gestión y optimización de los recursos requeridos para atender, contener, erradicar y cerrar el evento de manera eficiente y con una mejora en la comunicación entre el equipo de respuesta a incidentes y los niveles operativo, táctico y estratégico de la organización.

Fuente: Elaboración Propia

25) Lecciones Aprendidas - Incorporación de Mejoras Y Ajustes

En general y relacionado con mejorar el procedimiento de gestión de incidentes se relacionan las siguientes:

- Hacer énfasis y validar el entendimiento en la explicación e importancia de los roles que participan en el ejercicio y aún más cuando se esté gestionando un incidente que se presente en la vida real para ser más efectivos en su atención.
- Tener claro las funciones de cada rol, su alcance, su responsabilidad, su autoridad y la línea de mando para que la toma de decisiones fluya y no se desperdicien recursos, tiempo, dinero e inclusive se aumenten las consecuencias por la confusión y los malentendidos que se pueden presentar al momento de gestionar el incidente.
- Se debe revisar y hacer claridad de quien es la responsabilidad de activar el Protocolo de Respuesta de Nivel Corporativo, para que la articulación con el procedimiento de Gestión de incidentes tenga la efectividad esperada y la respuesta en la atención sea efectiva.
- Tener presente e incluir en el ejercicio las limitaciones, restricciones y situaciones que faciliten o puedan impedir el desarrollo normal del ejercicio.
- En un próximo ejercicio de simulación incluir como uno de los objetivos a evaluar la activación del protocolo de respuesta corporativo en el momento oportuno y adecuado y de acuerdo con lo definido para que la articulación y la respuesta tengan la eficacia requerida.
- El entrenamiento, la formación, la concienciación y la comunicación se convierten en factores claves para que estos ejercicios arrojen los resultados esperados y eleven el nivel de madurez y la cultura en la gestión de incidentes articulando la respuesta corporativa y mejorando la eficiencia en la disponibilidad y continuidad en la prestación de los servicios para así aumentar la resiliencia organizacional.
- Entrenar al personal de todos los niveles, operativo, táctico, estratégico y el equipo de respuesta a incidentes en temas de comunicación y relacionamiento para que la articulación entre los niveles y diferentes equipos de respuesta fluya y sea eficaz.

- Realizar ejercicios de socialización, comunicación y homologación del lenguaje y usar los términos y las palabras adecuadas, acorde con el público o las partes interesadas a las cuales se les está comunicando la situación del evento o incidente con el fin de que los recursos requeridos, las acciones y las decisiones sean acertadas y se logre atender el evento de manera oportuna.

4. Conclusiones y recomendaciones

4.1 Conclusiones

A continuación, se presentan las conclusiones del trabajo de investigación realizado por cada uno de los objetivos alcanzados tanto del general como de los específicos y en este mismo orden.

Como se puede apreciar en los resultados de este trabajo de investigación se propone el diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa, dando respuesta al problema planteado y en consecuencia el objetivo general se ha cumplido. Dicho procedimiento, el cual fue validado con un Caso de Estudio para probar su funcionamiento se puede replicar a todas las organizaciones que manejen sistemas de control industrial y las tecnologías de la operación e incluso las tecnologías de la información porque su enfoque está basado en el ciclo PHVA para hacer una gestión más efectiva de los incidentes desde al antes, el durante y el después, garantizando así una respuesta corporativa coherente, integrada y oportuna, dándole continuidad a la prestación de los servicios y disminuyendo su impacto frente a las partes interesadas de las organizaciones acorde con su misión y objeto social.

Al lograr integrar en el procedimiento los temas de riesgos, continuidad, crisis y resiliencia articulado con la respuesta corporativa la gestión de los incidentes de seguridad (cumpliendo el objetivo general) pasa de ser reactiva y concentrada en la respuesta a ser una gestión más proactiva, preventiva e incluso predictiva, lo que le trae beneficios a la organización como:

- Identificar los posibles eventos a través de los análisis de riesgos que se puedan convertir en incidentes de seguridad.
- Definir planes de tratamiento para cerrar esas brechas de seguridad detectadas en los análisis de riesgos.
- Definir las estrategias de continuidad para disminuir el número de incidentes y su atención en la respuesta.
- Preparar al personal que conforman los equipos de respuesta para que manejen la crisis, en caso de presentarse y adquirir madurez y mejorar la resiliencia.

- Generar confianza a sus partes interesadas.
- Proteger la imagen y reputación de la empresa.
- Optimizar los costos, disminuir las posibles pérdidas que pueden generar los incidentes y aumentar las ganancias y los ingresos al mantener la continuidad en la prestación de los servicios que la empresa ofrece.

Así mismo, se puede concluir para el primer objetivo específico "Establecer las características y requerimientos mínimos del servicio de TO para tener en cuenta en el procedimiento, en cuanto a disponibilidad", que se logró exitosamente dadas las entrevistas realizadas y la consulta de información con fuentes secundarias relacionadas con la prestación del servicio, los requisitos exigidos por la ley y la normatividad para garantizar su disponibilidad, con foco en los incidentes de seguridad que puedan afectar su operación fueron claves, porque con el conocimientos de los expertos vivido desde la experiencia en la operación del servicio y cruzando la información secundaria, se pudo obtener la ficha de las características y requerimientos mínimos del servicio de TO para tener en cuenta en el procedimiento, en cuanto a disponibilidad.

Como resultado se obtiene que son 8 las características y requerimientos mínimos (como se muestran en las Tabla 3-4, Tabla 3-8, Tabla 3-9 y Tabla 3-12) que se deben tener presentes en la gestión de incidentes de ciberseguridad con el propósito de poder lograr la disponibilidad en la prestación de los servicios que soportan las tecnologías de la operación. Se llega a esta conclusión después de identificar que cada uno de ellos son incluidos en las diferentes leyes y normas que regulan el servicio de transmisión y distribución de energía y cuya relación se cruzó con las respuestas obtenidas a las preguntas realizadas en la entrevista, donde los encuestados con base en su conocimiento y experiencia, también los identifican como requisitos mínimos esenciales evidenciando que no es posible ofrecer una prestación eficiente y continua de los servicios garantizando su disponibilidad sin contar con estos requerimiento mínimos en la operación de TO.

Para el objetivo específico 2 "Identificar las actividades claves de la gestión de riesgos, continuidad del negocio, gestión de crisis y resiliencia, que se pueda articular a la respuesta de gestión de incidentes y a la respuesta corporativa" se alcanza porque al realizar el referenciamiento de la mejores prácticas a nivel mundial y revisar los procedimientos de respuesta a nivel corporativo se

obtiene la matriz de relacionamiento con los elementos claves con la respuesta corporativa y el Protocolo de Respuesta Corporativa de Eventos – Incidentes – Crisis (como se muestra en la Tabla 3-9). El Mapa conceptual con los resultados del análisis comparativo de los diferentes casos seleccionados, donde se destacan los principales elementos de respuesta de nivel corporativo ante la ocurrencia de eventos de tipo tecnológico articulado al PHVA de la gestión de riesgos, continuidad, crisis y resiliencia, siguiendo la estructura de alto nivel fue un insumo clave para la construcción del nuevo diseño del procedimiento de gestión de incidentes, objetivo principal de este trabajo de investigación, donde se integraron estos componentes para hacer una gestión más integral y articulada con la respuesta corporativa para garantizar su efectividad.

Para cumplir con el objetivo específico 3 "Caracterizar los elementos que componen el procedimiento de gestión de incidentes de ciberseguridad, a través de la revisión de estándares nacionales e internacionales", fue necesario revisar los modelos de respuesta a los incidentes de seguridad – ciberseguridad tomando como referentes las mejores prácticas, modelos de referencias, normas y estándares a nivel nacional e internacional, arrojando como resultado la matriz con el análisis comparativo de los diferentes elementos que componen el procedimiento de Gestión de Incidentes de Ciberseguridad (como se muestra en la Tabla 3-12), donde se señala una breve descripción del propósito de cada uno de los 3 referentes seleccionados, sus etapas, sus ventajas, sus desventajas y el aporte que le brinda al diseño del nuevo procedimiento integrado de gestión de incidentes de ciberseguridad y respuesta corporativa, se llega a la conclusión que el marco de ciberseguridad de NIST se enfoca en desarrollar la capacidad de gestión de la seguridad cibernética en las organizaciones cuyos servicios son soportados en las tecnologías de la operación de infraestructuras críticas, fue la línea base para tomar como punto de partida los elementos que hacen parte del nuevo procedimiento de gestión de incidentes diseñado y tomando como complemento desde el enfoque de la gestión basados en el ciclo PHVA, existiendo una equivalencia con lo ofrecido en el estándar NIST SP 800-61 rev 2: Computer Security Incident Handling Guide, Agosto 2012 y la ISO/IEC 27035 – 1 y 2: Tecnología de la información - Técnicas de seguridad - la información de gestión de incidentes de seguridad, junto con los resultados arrojados en los objetivos 1 y 2 desarrollados en este proyecto y que fueron insumo claves para la construcción del nuevo procedimiento de gestión de incidentes de seguridad digital para cualquier tipo de organización (Tabla 3-11, Tabla 3-12, Tabla 3-13, Tabla 3-14, Tabla 3-15, Tabla 3-16 y Tabla 3-17)

El objetivo específico 4 “Validar el procedimiento de Gestión de Incidentes de Ciberseguridad a través de un ejercicio de simulación o juego de roles dentro de un caso de estudio”, se logra gracias a los resultados obtenidos en los tres objetivos anteriores y que fueron el insumo clave para obtener el diseño integrado de gestión de incidentes de ciberseguridad con la respuesta corporativa. Para poder validar el correcto funcionamiento del nuevo procedimiento de gestión de incidentes de seguridad fue necesario construir los instrumentos de validación (como se muestran en la Tabla 3-17) y que fueron utilizados en la realización del ejercicio de validación a través de un Caso de Estudio donde se simuló un ataque cibernético con el propósito de probarlo y como resultados obtener las siguientes conclusiones y recomendaciones para tener en cuenta para su mejora continua:

- En la ejecución de la simulación que fue en frio y en paralelo sin afectar la operación, se pudo evidenciar que en el deber ser, el nuevo procedimiento si funciona y se puede implementar en cualquier tipo de organización cuya operación sea soportada por las tecnologías de la operación y las tecnologías de la información (como se documentó en la tabla de ejecución de la simulación Tabla 3-21).

- Finalmente, las personas que participaron de acuerdo con el rol asignado, opinaron que el aporte del nuevo procedimiento es que se evoluciona de atender los incidentes basado en la respuesta con un enfoque reactivo a la gestión integral de los eventos, incidentes y crisis desde el antes, el durante y el después, involucrando las disciplinas de riesgos, continuidad, crisis y resiliencia, lo que lo hace ser más proactivo para disminuir la frecuencia en la ocurrencia, mejorar la eficacia en la respuesta en caso de que se materialice y capitalizar las lecciones aprendidas al documentarlas, socializarlas y cerrar las brechas de seguridad con las mejoras identificadas para implementar y estar mejor preparados para eventos futuro.

4.2 Recomendaciones

- Tener en cuenta las mencionadas en el capítulo de Lecciones Aprendidas y Recomendaciones del ejercicio de simulación a través del cual se validó el nuevo procedimiento diseñado como resultado de este trabajo de investigación.
- El entrenamiento, la formación, la concienciación y la comunicación se convierten en factores claves para que estos ejercicios arrojen los resultados esperados y eleven el nivel de madurez y la cultura en la gestión de incidentes articulando la respuesta corporativa y mejorando la eficiencia en la disponibilidad y continuidad en la prestación de los servicios para así aumentar la resiliencia organizacional.
- Entrenar al personal de todos los niveles, operativo, táctico, estratégico y el equipo de respuesta a incidentes en temas de comunicación y relacionamiento para que la articulación entre los niveles y diferentes equipos de respuesta fluya y sea eficaz.
- Realizar ejercicios de socialización, comunicación y homologación del lenguaje y usar los términos y las palabras adecuadas, acorde con el público o las partes interesadas a las cuales se les está comunicando la situación del evento o incidente con el fin de que los recursos requeridos, las acciones y las decisiones sean acertadas y se logre atender el evento de manera oportuna.
- A raíz de los resultados obtenidos con el ejercicio de simulación, las lecciones aprendidas y las mejoras identificadas, se hace necesario realizar en el futuro un trabajo de investigación que se enfoque en desarrollar las habilidades blandas y las capacidades del personal involucrado y responsable en la gestión de incidentes, los equipos de respuesta en los diferentes niveles de la organización en relación con los temas de comunicación, relacionamiento, articulación, coordinación, línea de mando, interacción y trabajo en equipo con el fin de complementar y mejorar lo procedimental, lo técnico y la interacción de las personas bajo presupón en el momento de la gestión de los eventos, incidentes y crisis que se presenten, dando la respuesta oportuna y eficaz para elevar el nivel de resiliencia organizacional y mantener la disponibilidad y la continuidad en la prestación de los servicios que la organización ofrece.

A. Anexo 1: Formato Entrevista

B. Anexo 2: Consolidado de las Encuestas Def Req Servicio SD Energía

C. Anexo 3: Consolidado Inf Ftes Sec Req Servicio SD E

D. Anexo 4: Consolidado Elementos Clave Riesgos Cont Cri Res Vs Nist

E. Anexo 5: Matriz Rel Elem Claves con Resp Corp

F. Anexo 6: Protocolo Respuesta Corporativa Eventos Incidentes Crisis

G. Anexo 7: Procedimiento Gestión de Incidentes de Ciberseguridad

H. Anexo 8: Guía para llevar a cabo ejercicios de Simulación y Simulacros

I. Anexo 9: Estudio de Caso para ejercicio de simulación

Bibliografía

[1] ICONTEC - ISO, NORMA TÉCNICA COLOMBIANA NTC-ISO 55000 2015-10-15 GESTIÓN DE ACTIVOS ASPECTOS GENERALES, TERMINOLOGÍA E: PRINCIPIOS, ICONTEC - ISO.

[2] CNO, Acuerdo 1347, Consejo Nacional de Operación del Sector Electrico, 2020.

[3] CONPES, Consejo Nacional de Politica Economica y Social, Documento de Politica Nacional de Confianza y Seguridad Digital 3995, 2020.

[4] CONPES, Consejo Nacional de Politica Economica y Social, Bogota /Colombia: Lineamientos de Politica para Ciberseguridad y Ciberdefensa 3701, 2011.

[5] Autor Corporativo, «Glosario de Terminos ISO 27000 - Punto a Punto,» [En línea]. Available: https://normaiso27001.es/referencias-normativas-iso-27000/#def32.

[6] Autor Corporativo, Metodologia GIR - Glosario de Términos, EPM, 2020.

[7] INCIBE, «Ciber-Resiliencia: Aproximación a un marco de medición,» 2014. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/ciberresiliencia-marco-medicion.

[8] BSI Group, Gestión de Crisis - Orientación y Buenas Practicas, Reino Unido: BSI, 2014.

[9] I. Autor Corporativo, ISO/CD 22301.2, Security and resilience - Business continuity management systems - Requirements, Ginebra / Suiza: ISO/TC 292 Security and resilience, 2018.

[10] J. J. Cano, Ciberseguridad empresarial: reflexiones y retos para ejecutivos del siglo XXI, Bogotá: Lemoine Editores, 2021.

[11] ISO, Norma ISO de Calidad ISO 9001:2015, Ginebra - Suiza: ISO, 2015.

[12] R. Forbes Álvarez, «Estructura de alto nivel de la ISO y su impacto en las normas de sistemas de gestión,» Éxito Empresarial - CEGESTI., vol. 277, 2014.

[13] I. Autor Corporativo, ISO 22316:2017 Security and resilience, Ginebra / Suiza: Organización Internacional de Estandares - ISO, 2017.

[14] ISO, GTC - ISO/IEC 31000:2018 GESTIÓN DEL RIESGO. DIRECTRICES, Bogota / Colombia: ISO, 2018.

[15] W. Romero y B. Guerrero, «Documento CONPES 3701 Lineamientos de políticas para la ciberseguridad y ciberdefensa,» Documento CONPES 3701, Colombia, 2016.

[16] Mindefensa, Guia de Infraestructura Critica en Colombia, Bogota - Colombia: Mindefensa, 2016.

[17] Kaspersky, «El ransomware: qué es, cómo se lo evita, cómo se elimina,» [En línea]. Available: https://latam.kaspersky.com/resource-center/threats/ransomware.

[18] CONPES, Politica Nacional de Seguridad Digital 3854, Bogota /Colombia: CONPES, 2016.

[19] BSI Group, Guia de Resiliencia Organizacional., Londres - Reino Unido: BSI, 2014.

[20] Cigref working group, «IT/OT convergence. A fruitful integration of information systems and operational systems,» Cigref is a network of major French corporations and public administrations, Paris, 2019.

[21] C. Feltus, M. Ouedraogo y D. Khadraoui, «Towards Cyber-Security Protection of Critical Infrastructures by Generating Security Policy for SCADA System,» Paper presented at The 1st International Conference on Information and Communication Technologies for Disaster Management, Algeria, 2014.

[22] Autor Corporativo, «Ciberseguridad en el sector eléctrico Amenazas para sistemas TI y OT,» [En línea]. Available: https://www2.deloitte.com/co/es/pages/risk/articles/ciberseguridad-en-el-sector-electrico.html.

[23] J. J. M. González Díaz, «Ciberriesgo desde la perspectiva del riesgo sistémico,» Revista Sistemas, pp. 74 - 84, 2019.

[24] O. d. C. -. B. -. O. Autor Corporativo, «Reporte de ciberseguridad 2020, Ciberseguridad riesgos, avances y el camino a seguir en América Latina y el Caribe,» 2020. [En línea]. Available: http://www.observatoriociberseguridad.com/.

[25] E. &. L. Autor Corporativo, Sector energético es el segundo mercado más atacado por el cibercrimen, Revista Empresarial & Laboral, Escrita por y para empresarios, 2018.

[26] A. Autor Corporativo, Panorama de Ciberamanezas en Colombia 2020, Fortinet® (NASDAQ: FTNT), 2020.

[27] BBC News Mundo, «EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país,» 2021. [En línea]. Available: https://www.bbc.com/mundo/noticias-internacional-57033536.

[28] J. A. Lecuit, «Hacia la fusión entre la ciberseguridad industrial y los sistemas de información corporativos,» 2019. [En línea]. Available: http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari6-2019-lecuit-hacia-fusion-entre-ciberseguridad-industrial-y-sistemas-informacion-corporativos.

[29] A. Andronache y A. Althonayan, «Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management alignment,» Brunel University London · Brunel Business School PhD Researcher, Londres - Reino Unido, 2019.

[30] H. A. Mestre, «Ciberseguridad en los sistemas de control industrial,» Empresa INCIBE, España, 2018.

[31] S. Bouchon, «The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state-of-the-art.,» European Commission, Directorate-General Joint Research Centre, Institute for the Protection and Security of the Citizen;, UE - Italy, 2006.

[32] B. Carreras, D. Newman, I. Dobson y A. Poole, «Evidence for self-organized criticality in a time series of electric power system blackouts,» Circuits Syst I: Regul Pap, IEEE Trans, 2004.

[33] Autor Corporativo, «¿Qué es la tecnología operativa (TO)?,» [En línea]. Available: https://www.fortinet.com/lat/solutions/industries/scada-industrial-control-systems/what-is-ot-security.

[34] Autor Corporativo, «What is Cybersecurity?,» 2021. [En línea]. Available: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/#:~:text=Cyber%20security%20refers%20to%20the,applications%2C%20devices%2C%20and%20data..

[35] E. J. Santiago y J. Sánchez Allende, «Tecnologi@ y desarrollo, Riesgos de ciberseguridad en las empresas,» Escuela Politécnica Superior. Universidad Alfonso X el Sabio., p. 11, 2017.

[36] N. Machín y M. Gazapo, «UNISCI Journal, #42, La Ciberseguridad como factor crítico en la seguridad de la Unión Europea,» Universidad Complutense de Madrid, p. 48, 2016.

[37] A. Signorino Barbat, «Ciber riesgos: Su dimensión social, funcional y ética,» Revista Ibero-Latinoamericana de Seguros, 2019.

[38] S. López Serrano, El impacto de los Ciberriesgos en la Gerencia de Riesgos Tradicional, Barcelona / España: Universidad de Barcelona, 2017.

[39] J. J. Cano, «Conceptos y retos en la atención de incidentes de seguridad y la evidencia digital,» Revista de Ingenieria - Universidad de los Andes, 2002.

[40] G. Gómez Morales, «¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos?,» 2019. [En línea]. Available: https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/.

[41] P. Remy, Manejo de Crisis, Lima - Perú: Universidad Peruana de Ciencias Aplicadas S. A. C., 2011.

[42] INCIBE, Instituto Nacional de Ciberseguridad de España, «Ciber resiliencia», Madrid / España: Instituto Nacional de Ciberseguridad de España.

[43] EPM, «Distribución energía,» 2021. [En línea]. Available: https://www.epm.com.co/site/clientes_usuarios/clientes-y-usuarios/nuestros-servicios/energia/distribuci%C3%B3n.

[44] Sector Electricidad, «Distribución de energía eléctrica,» 2019. [En línea]. Available: http://www.sectorelectricidad.com/9602/distribucion-de-energia-electrica/.

[45] J. A. García, «Ciberseguridad aplicada a los SCI con énfasis al sector energético,» Universidad Oberta de Catalunya, Barcelona / España, 2017.

[46] F. Navarro, «Las Normas ISO y la Estructura de Alto Nivel,» 2016. [En línea]. Available: https://revistadigital.inesem.es/gestion-integrada/las-normas-iso-la-estructura-alto-nivel/.

[47] BSI Group, «ISO 9001 Revisión 2015,» [En línea]. Available: https://www.bsigroup.com/es-ES/Gestion-de-Calidad-ISO-9001/ISO-9001revision-2015.

[48] ISOTools, «¿En qué consiste el ciclo PHVA de mejora continua?,» 2015. [En línea]. Available: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua/.

[49] H. A. Rodríguez G., «CICLO PHVA,» 2015. [En línea]. Available: https://ntc6001.wordpress.com/2015/07/31/ciclo-phva/.

[50] J. Daza y M. Posada, «Los ciberriesgos vuelan,» Revista Sistemas, 2019.

[51] J. J. Cano, «Superando los silos en la gestión de riesgos corporativos. Breves anotaciones para el riesgo cibernético,» 2021. [En línea]. Available: https://es.linkedin.com/pulse/superando-los-silos-en-la-gesti%C3%B3n-de-riesgos-breves-cano-ph-d-cfe?trk=read_related_article-card_title.

[52] F. Capra, La trama de la vida. Una nueva perspectiva de los sistemas vivos, Barcelona / España: Anagrama, 1998.

[53] D. Autor Corporativo, «Nuevas prácticas de gobierno corporativo en Colombia,» 2021. [En línea]. Available: https://www2.deloitte.com/co/es/pages/risk/articles/Nuevas-Practicas-de-Gobierno-Corporativo-en-Colombia.html.

[54] P. Zongo, The five anchors for cyber resilience. Why some enterprises are hacked into bankruptcy while others easily bounce back, Victoria / Australia: Broadcast Books, 2018.

[55] O. Rebollo, D. Mellado y E. Fernández-Medina, «A systematic review of information security governance frameworks in the cloud computing environment,» J. Ucs, Vol. 18 No. 6, pp. 798-815, 2012.

[56] M. Nicho, «A process model for implementing information systems security governance,» Information & Computer Security, Vol. 26 Issue: 1, pp. 10-38, 2018.

[57] D. S. Preston y E. Karahanna, «Antecedents of IS strategic alignment: A Nomological network,» Information Systems Research, p. 159–179, 2009.

[58] S. Wu, D. Straub y T. Liang, «How information technology governance mechanisms and strategic alignment influence organisational performance: insights from a matched survey of business and IT managers,» MIS Quarterly, pp. 497-518, 2015.

[59] H. Servaes, A. Tamayo y P. Tufano, «The theory and practice of corporate risk Management,» Journal of Applied Corporate Finance 21(4), p. 60–78, 2009.

[60] I. Atoum, A. Otoom y A. Abu Ali, «A holistic cyber security implementation framework,» Information Management and Computer Security, 22(3), p. 251–264, 2014.

[61] I. Atoum, A. Otoom y A. Abu Ali, «Holistic cyber security implementation framework: a case study of Jordan International Journal of Information,» Business and Management, 9 (1), pp. 108-119, 2017.

[62] F. Bergeron, L. Raymond y S. Rivard, «Ideal patterns of strategic alignment and business performance,» Information and Management, 41(8), p. 1003–1020, 2004.

[63] OTAN - CCDCOE Cooperative Cyber Defence Centre of Excellence, Marcos de Referencia de Ciberseguridad Internacional, OTAN, 2010.

[64] J. Webb, A. Ahmad, S. B. Maynard y G. Shanks, «Foundations for an Intelligence-driven Information Security Risk-management System,» JOURNAL OF INFORMATION TECHNOLOGY THEORY AND APPLICATION, 2016.

[65] L. Kauspadiene, A. Cenys, N. Goranin y S. Tjoa, «High-Level Self-Sustaining Information Security Management Framework,» Modern Computing, Vol 5, pp. 107 - 123, 2017.

[66] A. Calder y S. Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002, Londres - Reino Unido: Editorial Kogan Page, 2012.

[67] D. L.Nazareth y J. Choi, «A system dynamics model for information security management,» Information & Management, Vol 52, pp. 123 - 134, 2015.

[68] L. Li, W. He, L. Xu, I. Ash, M. Anwar y X. Yuan, «Effects of Evidence-Based Malware Cybersecurity Training on Employees,» 2019. [En línea]. Available: https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/11/.

[69] A. Andronache y A. Althonayan, «Shifting from Information Security towards a Cybersecurity Paradigm,» 2018.

[70] H. Hidekazu, T. Yuma, A. Tomomi, H. Yoshihiro y K. Ichiro, Concienciación, capacitación y entrenamiento en Gestión de Incidentes de Ciberseguridad, 2018.

[71] C. J. Alberts y A. J. Dorofee, «OCTAVE Method Implementation Guide Version 2.0.,» 2001. [En línea]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html.

[72] Joint Task Force Transformation Initiative, «Guide for Conducting Risk Assessments - SP 800-30 Rev. 1,» 2012. [En línea]. Available: NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments.

[73] «Mehari - Metodo de Evaluación y Gestión de Riesgos en el dominio de la Seguridad de Información,» 2010. [En línea]. Available: http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf.

[74] A. Corporativo, «MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» 2014. [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.

[75] ISO, Norma Tecnica Colombiana NTC-ISO/IEC 27005:2018, ISO Organización Internacional de Estandares, 2018.

[76] J. M. Kaplan, T. Bailey, D. O'Halloran, A. Marcus y C. Rezek, «Beyond Cybersecurity: Protecting Your Digital Business,,» New jersey/USA, Wiley; 1er edición, 2015, p. 163.

[77] M. Á. Caballero y D. Cilleros Serrano, Ciberseguridad y Transformación Digital, Madrid/ España: ANAYA Multimedia, 2019.

[78] M. Szylkowska, «Amenazas cibernéticas y riesgo de proliferación en el área de logística: un resumen del problema,» Anales de la Real Academia de Doctores de España. Volumen 4, número 1, pp. 5 - 15, 2019.

[79] ISO, GTC - ISO/IEC 27032Tecnologias de la información. Técnicas de seguridad, directrices para ciberseguridad, Bogota / Colombia: ICONTEC, 2020.

[80] A. Althonayan y A. Andronache, «Resiliency under Strategic Foresight: The effects of Cybersecurity Management and Enterprise Risk Management Alignment,» 2019. [En línea]. Available: https://www.researchgate.net/publication/332094387.

[81] I. O. I. d. Estandares, «ISO 27103 guia implementación marco ciberseguridad,» ISO Organización Internacional de Estandares, 2018.

[82] Autor Corporativo, «Que es la Ciberseguridad?,» 2021. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.