Desarrollo de un escenario de crisis cibernética para evaluar la preparación organizacional ante incidentes de seguridad

Luisa Fernanda Ossa Ruiz

Asesor

Daniel Felipe Palomo Luna

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2026

Resumen

Este proyecto describe el Desarrollo de un Escenario de Crisis Cibernética para Evaluar la Preparación Organizacional ante Incidentes de Seguridad. Este proyecto busca responder a la creciente necesidad de evaluar y fortalecer las capacidades organizacionales frente a amenazas cibernéticas, que representan un riesgo significativo para la continuidad operativa y la reputación de las entidades.

El marco teórico se fundamenta en estándares internacionales como NIST e ISO 27001, que establecen lineamientos para la gestión de incidentes y la resiliencia organizacional. El proyecto tiene como objetivo general evaluar la preparación integral de las entidades mediante un ejercicio práctico, y como objetivos específicos, incluye diseñar un escenario de crisis con roles definidos, establecer un minutograma detallado que guíe las actividades del ejercicio, ejecutar la simulación y registrar las respuestas organizacionales, y tabular los resultados para identificar fortalezas y áreas de mejora.

La metodología combina simulación de incidentes en un entorno controlado con un enfoque mixto que integra análisis cualitativo y cuantitativo. Los resultados esperados incluyen un diagnóstico detallado del nivel de preparación organizacional, recomendaciones para fortalecer los protocolos de respuesta y la promoción de una cultura organizacional orientada a la gestión proactiva de incidentes de ciberseguridad.

Palabras clave: Crisis, Ciberseguridad, TableTop, Incidente.

Abstract

This project proposes the development of a cyber crisis scenario to assess the level of preparedness of organizations at the tactical, technical, and executive levels in the face of a cybersecurity incident. This project seeks to respond to the growing need to evaluate and strengthen organizational capabilities in the face of cyber threats, which represent a significant risk to the operational continuity and reputation of entities.

The theoretical framework is based on international standards such as NIST and ISO 27001, which provide guidelines for incident management and organizational resilience. The general objective of the project is to assess the comprehensive preparedness of entities through a practical exercise. The specific objectives include designing a crisis scenario with defined roles, establishing a detailed timeline to guide the exercise activities, executing the simulation and recording organizational responses, and tabulating the results to identify strengths and areas for improvement.

The methodology combines incident simulation in a controlled environment with a mixed approach that integrates qualitative and quantitative analysis. The expected results include a detailed diagnosis of organizational preparedness, recommendations to strengthen response protocols, and the promotion of an organizational culture focused on proactive cybersecurity incident management.

Keywords: Risk, Tabletop, Cybersecurity, Incident.

Tabla De Contenido

Lista de Tablas

Lista de Figuras

Introducción

En la era digital, las organizaciones enfrentan un entorno cada vez más complejo y dinámico en materia de ciberseguridad. La creciente sofisticación de los ciberataques, como el *Ransomware*, el phishing y las intrusiones avanzadas persistentes (APT), ha generado un impacto significativo en la continuidad operativa, la reputación y la seguridad de la información. Según el National Institute of Standards and Technology (NIST, 2018) y la International Organization for Standardization (ISO, 2022), la gestión de incidentes es una prioridad estratégica para garantizar la resiliencia organizacional. Sin embargo, muchas entidades aún presentan brechas significativas en su capacidad de respuesta ante crisis cibernéticas, lo que resalta la necesidad de implementar estrategias de evaluación y mejora continua en este ámbito.

El impacto económico de los ciberataques sigue en aumento. De acuerdo con IBM Security (2023), el costo promedio de una brecha de datos ha alcanzado los 4.45 millones de dólares a nivel mundial. Asimismo, el Informe de Amenazas 2023 de Verizon señala que el 74% de las brechas de seguridad involucran errores humanos, lo que evidencia la importancia de fortalecer las estrategias de preparación y respuesta ante incidentes (Verizon, 2023). Estos datos subrayan la necesidad de que las organizaciones desarrollen planes efectivos de gestión de crisis cibernéticas, integrando simulaciones y ejercicios estructurados que permitan evaluar su nivel de preparación.

Este proyecto tiene como propósito el diseño y desarrollo de un escenario de crisis cibernética que permita medir el nivel de preparación organizacional en los niveles táctico, técnico y ejecutivo. A través de un enfoque estructurado basado en estándares internacionales como NIST e ISO 27001, se busca evaluar la efectividad de los protocolos de respuesta,

identificar fortalezas y debilidades en los procesos de gestión de incidentes y fortalecer la resiliencia cibernética de las entidades participantes.

Para lograr estos objetivos, se propone una metodología que integra simulaciones controladas, análisis de respuesta en tiempo real y técnicas de evaluación cualitativa y cuantitativa. A partir de los resultados obtenidos, se formularán recomendaciones prácticas que contribuyan a la optimización de las estrategias de respuesta a incidentes, promoviendo una cultura organizacional orientada a la prevención y gestión proactiva de riesgos cibernéticos. Con ello, este estudio pretende aportar no solo al fortalecimiento de la ciberseguridad en las organizaciones, sino también a la generación de conocimiento práctico aplicable en diversos sectores.

Planteamiento del Problema

En el panorama digital contemporáneo, la ciberseguridad ha dejado de ser un asunto puramente técnico para convertirse en un pilar crítico de la resiliencia institucional. A nivel global, la sofisticación de las amenazas cibernéticas, como el *Ransomware* y la filtración de datos, ha crecido de manera exponencial. Según el informe *Cost of a Data Breach Report 2023* de **IBM Security**, el costo promedio de una exfiltración de datos alcanzó los 4.45 millones de dólares, lo que representa un aumento significativo que pone en riesgo la estabilidad financiera de cualquier organización. Por su parte, **Verizon (2023)** señala que el 74% de las brechas de seguridad incluyen un componente humano, ya sea por error, mal uso de privilegios o ingeniería social, lo que demuestra que la tecnología por sí sola es insuficiente si el personal no está preparado.

En el contexto colombiano, la presión regulatoria y la frecuencia de los ataques han obligado a las empresas a adoptar marcos de control más estrictos. La Superintendencia de Industria y Comercio (SIC) y otros entes de control han incrementado la vigilancia sobre la protección de datos personales, imponiendo sanciones millonarias a entidades que demuestran negligencia en la gestión de incidentes. Sin embargo, a pesar de contar con herramientas de defensa perimetral (firewalls, antivirus), muchas organizaciones presentan un vacío crítico: la falta de una cultura de respuesta coordinada ante crisis. Existe una desconexión evidente entre los equipos técnicos y los niveles directivos, legales y de comunicación en el momento de enfrentar un incidente en tiempo real.

Sin una evaluación previa de la preparación organizacional, las empresas se enfrentan a una parálisis en la toma de decisiones, pérdida de confianza por parte de los clientes, multas por incumplimiento de la Ley 1581 de 2012 y, en casos extremos, el cierre definitivo de operaciones

por daño reputacional irreparable. El problema radica en que las organizaciones no saben si están preparadas hasta que el ataque ocurre, lo cual es un riesgo que la gestión de seguridad moderna no puede permitir.

Ante esta realidad, surge la necesidad de desarrollar herramientas prácticas que permitan medir la capacidad de respuesta no solo técnica, sino estratégica y operativa, involucrando a todos los actores clave de la entidad. Por lo tanto, el presente proyecto busca dar respuesta al siguiente interrogante:

¿De qué manera se puede medir el nivel de preparación de las organizaciones en los niveles táctico, técnico y ejecutivo ante un incidente de ciberseguridad?

Justificación

El desarrollo de un escenario de crisis cibernética resulta altamente relevante debido a la creciente frecuencia e impacto de los incidentes de ciberseguridad en organizaciones de todos los sectores. La ciberseguridad no solo es un desafío técnico, sino una necesidad estratégica que incide directamente en la continuidad operativa, la protección de datos sensibles y la confianza de clientes y socios (National Institute of Standards and Technology [NIST], 2018; International Organization for Standardization [ISO], 2022).

Casos recientes han evidenciado las graves consecuencias de una respuesta ineficaz ante crisis cibernéticas. En 2023, un ataque de *Ransomware* afectó a MGM Resorts, paralizando sus operaciones durante varios días y generando pérdidas estimadas en 100 millones de dólares (MGM, 2023). De igual manera, el ataque a Colonial Pipeline en 2021, que comprometió el suministro de combustible en Estados Unidos, puso en evidencia la vulnerabilidad de infraestructuras críticas y la necesidad de una gestión proactiva de riesgos (CISA, 2021). Estos ejemplos refuerzan la importancia de contar con mecanismos de evaluación y mejora continua que permitan medir y optimizar la capacidad de respuesta organizacional.

Este proyecto responde a esta necesidad al evaluar y fortalecer las capacidades de respuesta en los niveles táctico, técnico y ejecutivo, promoviendo una gestión integral de riesgos cibernéticos.

Desde el punto de vista académico, este proyecto contribuye al avance del conocimiento práctico en ciberseguridad, integrando estándares internacionales como NIST e ISO 27001 en un entorno aplicado. Además, fomenta la implementación de metodologías innovadoras para evaluar la preparación organizacional, fortaleciendo la conexión entre la teoría y la práctica.

En el ámbito social, este proyecto tiene un impacto significativo al mejorar la resiliencia de las organizaciones frente a amenazas cibernéticas, protegiendo no solo sus activos digitales, sino también a sus colaboradores, clientes y comunidades ante posibles fugas de información, fraudes e interrupciones críticas. La mejora en la gestión de crisis cibernéticas reduce la exposición de las empresas a ataques de alto impacto, promoviendo así una sociedad más segura en el ámbito digital.

A nivel personal y profesional, este estudio representa una oportunidad para profundizar en competencias técnicas y metodológicas avanzadas, permitiendo desarrollar estrategias efectivas de gestión de crisis y respuesta a incidentes. Asimismo, contribuye de manera tangible a la mejora de la seguridad cibernética en las organizaciones, consolidando un perfil profesional especializado en gestión de riesgos y seguridad informática.

Objetivos

Objetivos General

Medir el nivel preparación de las organizaciones para responder a un incidente de ciberseguridad en los diferentes niveles, táctico, técnico y ejecutivo de las diferentes áreas de la entidad.

Objetivos Específicos

Diseñar un escenario de crisis cibernética simulado, mediante la identificación y definición de los actores a través de una narrativa estructurada, con el fin de representar una situación realista que permita analizar la capacidad de respuesta organizacional ante incidentes de ciberseguridad.

Trazar un minutograma estructurado del ejercicio de crisis, identificando y secuenciando los inyectores y eventos clave, para observar las reacciones, toma de decisiones y coordinación entre los diferentes niveles de la organización.

Ejecutar el ejercicio de crisis cibernética, aplicando el minutograma y documentando las respuestas y acciones tomadas por los equipos participantes, para evaluar la eficacia y sincronización de los protocolos existentes ante ciberincidentes.

Evaluar el desempeño de la organización frente al escenario simulado, mediante el análisis cualitativo y cuantitativo de la información recopilada durante el ejercicio, con el propósito de identificar fortalezas, debilidades y oportunidades de mejora en la gestión de crisis.

Marco Referencial

El presente estudio se fundamenta en la necesidad de fortalecer la capacidad de respuesta de las organizaciones ante crisis cibernéticas mediante el uso de simulaciones estructuradas. La relevancia de este enfoque se sustenta en investigaciones previas que han demostrado cómo los ejercicios de crisis pueden mejorar la resiliencia organizacional y la coordinación entre equipos técnicos y directivos en situaciones de alta presión.

Las simulaciones de crisis cibernética han sido reconocidas como una herramienta efectiva para evaluar la preparación de las organizaciones y optimizar sus protocolos de respuesta. Según el Informe de Ciberseguridad de IBM (2023), las empresas que realizan ejercicios regulares de simulación de crisis reducen el tiempo de respuesta a incidentes en un 30% en comparación con aquellas que no cuentan con este tipo de prácticas (IBM Security, 2023).

Un ejemplo destacado es el caso del ataque de *Ransomware* a Norsk Hydro en 2019, donde la empresa logró contener y mitigar el impacto del ataque debido a la implementación previa de ejercicios de simulación, lo que permitió una respuesta estructurada y efectiva (Norsk Hydro, 2019). De manera similar, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha promovido simulaciones a gran escala, como Cyber Europe, donde se evalúa la capacidad de respuesta de entidades gubernamentales y privadas ante escenarios de crisis multinivel (ENISA, 2022).

Estos casos evidencian que las simulaciones no solo permiten identificar debilidades en los protocolos existentes, sino que también facilitan la implementación de estrategias proactivas para mejorar la resiliencia ante incidentes reales.

El uso de simulaciones en la preparación ante crisis cibernéticas ha sido ampliamente validado en el ámbito académico y profesional. De acuerdo con Information and Computer Security (2022), los ejercicios de simulación mejoran significativamente la capacidad de respuesta organizacional, especialmente en entornos con trabajo remoto y tecnologías emergentes. En particular, el enfoque de "Scenario-Based Incident Response Training" ha permitido desarrollar metodologías de aprendizaje experiencial que optimizan la toma de decisiones en situaciones de crisis (Alhassan & Adjei, 2024).

Estudios recientes destacan que las organizaciones que realizan ejercicios de crisis cibernética logran identificar brechas críticas en sus protocolos y mejoran la coordinación entre equipos técnicos y ejecutivos. Además, la implementación de este tipo de simulaciones ha demostrado reducir los tiempos de respuesta y mitigar el impacto financiero de los ciberataques (Springer, 2023).

Las simulaciones han sido implementadas en distintos sectores con resultados positivos:

Sector académico: El ataque de *Ransomware* a la Universidad Autónoma de Barcelona (Iglesias, 2024) evidenció cómo la falta de protocolos estructurados generó retrasos en la recuperación. Este caso refuerza la necesidad de ejercicios de crisis en instituciones educativas.

Infraestructura crítica: En el caso de la infraestructura portuaria colombiana (Lores Acosta, 2024), se identificaron vulnerabilidades en sistemas de gestión logística y control de accesos. La implementación de simulaciones especializadas permitió mejorar la coordinación entre equipos de TI y seguridad operativa.

Sector financiero: Según el Informe de Riesgos Globales 2023 del Foro Económico Mundial (WEF, 2023), los bancos han aumentado la adopción de ejercicios de crisis para mitigar ataques dirigidos a sistemas de pagos y transferencias internacionales. Investigaciones recientes

indican que las simulaciones han optimizado la resiliencia del sector financiero ante amenazas avanzadas (Springer, 2023).

Estos casos resaltan la aplicabilidad y efectividad de las simulaciones de crisis en distintos entornos empresariales, validando su importancia dentro del presente estudio.

Marco Conceptual

La preparación ante crisis cibernéticas es un componente clave de la ciberseguridad moderna, dada la creciente frecuencia y complejidad de los ciberataques. Sin embargo, muchas organizaciones carecen de estrategias efectivas para enfrentar estos incidentes en los niveles táctico, técnico y ejecutivo. Este proyecto se enmarca en la gestión de incidentes cibernéticos, que abarca el conjunto de procesos y herramientas necesarios para identificar, contener, mitigar y recuperar sistemas afectados por un ciberataque (NIST, 2018).

Conceptos fundamentales como resiliencia cibernética (ENISA, 2016) y simulaciones de crisis (Winger et al., 2024) sustentan el desarrollo de escenarios que permitan medir la capacidad de respuesta de las organizaciones. La resiliencia implica no solo la capacidad de resistir un ataque, sino también de recuperar operaciones críticas de forma rápida y efectiva. Las simulaciones, por su parte, permiten modelar incidentes reales en un entorno controlado para identificar brechas y mejorar los protocolos de respuesta.

Además, la integración entre niveles organizacionales (Lores Acosta, 2024) es crucial, ya que la alta gerencia y los equipos técnicos deben coordinarse para tomar decisiones rápidas y acertadas. Esto incluye la evaluación de factores como la capacitación del personal (Álvarez y Tarrió, 2024) y el uso de seguros cibernéticos como medida complementaria (Signorino Barbat, 2022).

Marco Teórico

El marco teórico de este estudio se basa en estándares internacionales, marcos normativos y casos de estudio, los cuales proporcionan una base sólida para la comprensión y aplicación de estrategias de gestión de crisis cibernéticas. Estos elementos permiten analizar las debilidades actuales en la preparación organizacional y plantear soluciones efectivas para mitigar los riesgos cibernéticos.

Los siguientes estándares han sido adoptados globalmente como referencia para la gestión de la ciberseguridad y la preparación ante incidentes:

NIST Framework for Improving Critical Infrastructure Cybersecurity (2018): Este marco enfatiza la identificación, protección, detección, respuesta y recuperación como fases fundamentales para gestionar riesgos cibernéticos. Proporciona una base sólida para estructurar simulaciones de crisis. Es ampliamente utilizado en organizaciones gubernamentales y privadas para fortalecer la ciberresiliencia y su enfoque en la gestión de riesgos cibernéticos permite diseñar simulaciones de crisis alineadas con las mejores prácticas del sector (NIST, 2018).

ISO/IEC 27001:2022: Ofrece lineamientos para la implementación de sistemas de gestión de seguridad de la información, fundamentales para diseñar protocolos claros en las organizaciones.

ENISA Cyber Crisis Cooperation Framework (2016): Proporciona guías específicas para la cooperación y respuesta en escenarios de crisis cibernética. Este marco inspira la colaboración entre diferentes niveles de la organización.

COBIT 5 (ISACA, 2012): Este marco ayuda a alinear la gobernanza de TI con los objetivos estratégicos de la organización, subrayando la importancia de involucrar a la alta gerencia en la planificación de ciberseguridad.

Casos Reales y Estudios Aplicados

Universidad Autónoma de Barcelona (Iglesias, 2024): Este caso de *Ransomware* ilustra cómo la falta de preparación puede prolongar el tiempo de recuperación y aumentar el impacto operativo. El análisis de lecciones aprendidas informa el diseño de escenarios de crisis más realistas y efectivos.

Infraestructura portuaria colombiana (Lores Acosta, 2024): La digitalización del sector portuario ha incrementado la exposición a ciberataques, esto llevo a la necesidad de diseñar simulaciones adaptadas al sector para mejorar la seguridad operativa. La implementación de pruebas de crisis fortaleció la coordinación entre los equipos técnicos y ejecutivos.

Caso Norsk Hydro (2019): Un ataque de *Ransomware* afectó sus operaciones globales y gracias a la aplicación de estándares como NIST e ISO 27001, la empresa logró contener y mitigar el impacto., esto demostró que contar con protocolos de respuesta bien definidos reduce significativamente el tiempo de recuperación.

Capacitación y Cultura Organizacional

La capacitación del personal es un factor clave en la preparación para crisis cibernéticas. Según Álvarez y Tarrió (2024), mantener al personal técnico actualizado sobre nuevas amenazas y vulnerabilidades es esencial para mejorar la respuesta organizacional.

Además, la alta gerencia también debe recibir formación específica para tomar decisiones bajo presión en escenarios de crisis (Winger et al., 2024). La falta de capacitación en este nivel puede generar respuestas descoordinadas y aumentar el impacto de un ataque cibernético.

Impacto Global y Geopolítico

Los ciberataques pueden trascender el ámbito organizacional, afectando sectores estratégicos e incluso la estabilidad de los países. Según Zafra Díaz (2023), los incidentes de

ciberseguridad pueden desencadenar crisis económicas y conflictos geopolíticos, evidenciando la importancia de considerar no solo las respuestas técnicas, sino también sus implicaciones sociales y económicas.

Un ejemplo de ello fue el ataque a Colonial Pipeline (2021), que generó una interrupción en el suministro de combustible en Estados Unidos, afectando la economía y la seguridad nacional (CISA, 2021). Este tipo de incidentes subraya la necesidad de contar con estrategias de prevención y mitigación a gran escala.

Marco Legal En Colombia

En Colombia, las entidades están sujetas a regulaciones específicas en materia de ciberseguridad y protección de datos personales, emitidas por organismos como la Superintendencia Financiera de Colombia (SFC) y la Superintendencia de Industria y Comercio (SIC). A continuación, se detallan algunas de las principales circulares y directrices relevantes en este ámbito:

Superintendencia Financiera de Colombia (SFC)

Circular Externa 007 de 2018: Esta circular establece medidas mínimas para la administración del riesgo de ciberseguridad en las entidades vigiladas. Entre sus aspectos más destacados se incluyen:

Las entidades deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente los riesgos de ciberseguridad.

Se requiere que las entidades informen a la SFC sobre incidentes de ciberseguridad que afecten significativamente la confidencialidad, integridad o disponibilidad de la información, proporcionando una descripción del incidente, su impacto y las medidas adoptadas para gestionarlo.

Circular Externa 008 de 2018: Orienta sobre los requerimientos mínimos de seguridad y calidad para la realización de operaciones a través de pasarelas de pago, buscando proteger la información de los consumidores financieros en transacciones electrónicas.

Circular Externa 004 de 2024: Define los estándares tecnológicos, de seguridad y demás necesarios que deben adoptar las entidades vigiladas para el desarrollo de finanzas abiertas en condiciones de interoperabilidad. También establece obligaciones para el tratamiento de datos de

los consumidores financieros, garantizando seguridad, transparencia y eficiencia, en cumplimiento de las Leyes 1266 de 2008 y 1581 de 2012.

Superintendencia de Industria y Comercio (SIC)

Circular Externa 002 de 2024: Emitida el 21 de agosto de 2024, esta circular proporciona lineamientos sobre el tratamiento de datos personales en sistemas de inteligencia artificial. Establece principios como idoneidad, necesidad, razonabilidad y proporcionalidad que deben guiar el tratamiento de datos personales en la IA. Además, resalta la importancia de realizar evaluaciones de impacto en la privacidad antes de desarrollar sistemas de IA que puedan implicar altos riesgos para los titulares de los datos.

Circular Externa 003 de 2024: Refuerza la responsabilidad de los administradores de empresas en la protección de datos personales, destacando la importancia de cumplir con las obligaciones legales para evitar sanciones y fortalecer la confianza de clientes y empleados en la organización.

En Colombia, las entidades que no gestionan adecuadamente los ciberataques y vulneran la protección de datos personales pueden ser sancionadas por la Superintendencia de Industria y Comercio (SIC). Las sanciones pueden incluir multas de hasta 2.000 salarios mínimos legales mensuales vigentes (SMLMV), suspensión de actividades relacionadas con el tratamiento de datos y, en casos graves, el cierre definitivo de operaciones.

Multas en Colombia

Central de Información Financiera (CIFIN): En 2018, la SIC impuso una multa de $702.242.400 a CIFIN por incluir información no financiera en los historiales de 288.753 colombianos, lo que evidenció fallas en las medidas de seguridad de la información.

Scotiabank Colpatria: La entidad bancaria fue sancionada con $356.070.000 por no implementar medidas adecuadas para respetar los derechos de los titulares de datos, reflejando deficiencias en la gestión de la información personal.

Empresas Varias: Hasta enero de 2019, la SIC había impuesto multas por más de $19.000 millones por violaciones a la Ley de Protección de Datos Personales, afectando a más de 600 empresas y personas naturales. Las conductas más sancionadas incluyeron fallas en la seguridad de la información y la falta de autorización para el tratamiento de datos personales.

El marco legal expuesto anteriormente no solo pone sobre la mesa los lineamientos para la protección de la información en Colombia, sino que establece la base de responsabilidad para la alta gerencia. El escenario de crisis propuesto en este proyecto se fundamenta directamente en el cumplimiento de la **Circular 007 de 2018** y la **Ley 1581**, ya que un ejercicio de simulación de crisis cibernética permite a la organización validar si sus protocolos de respuesta son suficientes para cumplir con el deber que tienen las organizaciones de reportar incidentes ante la SIC y la SFC.

En conclusión, la normativa colombiana exige un debido proceso que solo puede comprobarse mediante el entrenamiento y la evaluación constante. Por lo tanto, el desarrollo de este escenario de crisis actúa como un mecanismo de control preventivo para evitar las consecuencias sancionatorias descritas en los casos de estudio (como las multas a CIFIN o Scotiabank), transformando la teoría legal en una capacidad operativa real para la entidad.

Marco Metodológico

La metodología propuesta para el desarrollo del proyecto sigue un enfoque estructurado y sistemático, integrando técnicas cualitativas y cuantitativas para garantizar el diseño, implementación y evaluación efectiva de un escenario de crisis cibernética. Se emplearán herramientas de análisis de datos, software de simulación y técnicas de observación estructurada para recopilar y evaluar las respuestas de los participantes.

Tipo de Investigación

La presente investigación es de carácter aplicado y descriptivo, con un enfoque mixto (cualitativo y cuantitativo).

Es aplicada ya que busca resolver un problema práctico dentro de las organizaciones.

Es descriptiva ya que detalla las fases, roles y respuestas observadas durante el ejercicio.

El enfoque es mixto ya que integra el análisis cualitativo (observación del comportamiento y toma de decisiones de los participantes) con el análisis cuantitativo (tabulación de resultados y métricas de desempeño según la escala definida).

Población y Muestra

Dada la naturaleza del proyecto, se define una población estándar que normalmente se encuentra en la estructura organización de las empresas colombianas que representa la estructura de mando de una

Población: Personal integrante de los comités de crisis, áreas de tecnología y departamentos legales/comunicaciones de una entidad.

Muestra: Se ha seleccionado una muestra por conveniencia compuesta por seis (6) roles estratégicos:

- CISO (Chief Information Security Officer)

- Director de TI
- Asesor Legal
- Director de Comunicaciones
- Analista de Respuesta a Incidentes
- Representante de Operaciones

Instrumentos de Recolección de Información

Para la formalización del levantamiento de datos, se han diseñado y seleccionado los siguientes instrumentos:

Minutograma del escenario: instrumento guía que establece la cronología de los inyectores y las respuestas esperadas.

Bitácora de observación: formato estructurado donde el evaluador registra las acciones tomadas, los tiempos de reacción y los cuellos de botella identificados durante la simulación.

Cuestionario de percepción: encuesta aplicada al finalizar el ejercicio para que los participantes autoevalúen su nivel de confianza y la claridad de los protocolos de la organización.

Matriz de tabulación: herramienta para consolidar los resultados y generar las gráficas de nivel de madurez/preparación.

Fases de Desarrollo

Planeación del Proyecto

Se realizará una fase inicial de planeación para definir los objetivos específicos del escenario de crisis, las características del entorno de simulación y los actores involucrados. En esta etapa se llevarán a cabo las siguientes actividades:

Revisión documental: Análisis de estándares internacionales (NIST, ISO 27001 y ENISA) junto con casos de estudio reales para establecer lineamientos del diseño.

Definición de roles y responsabilidades: Identificación de los niveles organizacionales a incluir (táctico, técnico y ejecutivo) y de los inyectores que intervendrán en la simulación.

Herramientas: Uso de software de simulación y plataformas de colaboración para modelar los escenarios como plataformas open-source como SANS Cyber Range, escenarios de mesa o escenarios de simulación de mensajería por medio de correo electrónico.

Diseño del Escenario de Crisis

Se desarrollará un modelo teórico-práctico que contemple las siguientes etapas:

Creación del escenario: Desarrollo de un guion que simule un incidente cibernético específico, con un impacto progresivo en el tiempo del ejercicio.

Definición de los inyectores: Incorporación de eventos desencadenantes que generen respuestas en tiempo real de los participantes, permitiendo evaluar la capacidad de detección, análisis y mitigación.

Minutograma: Elaboración de un cronograma detallado para coordinar las acciones durante la simulación.

Herramientas: MITRE ATT&CK: Para estructurar tácticas y técnicas del ataque.

Pruebas Experimentales y Ensayos

Se llevarán a cabo pruebas controladas del escenario diseñado para evaluar su funcionalidad y realismo. Estas pruebas incluirán:

Pruebas piloto: Simulaciones internas con un grupo reducido para identificar posibles ajustes en el diseño.

Validación técnica: Evaluación de los inyectores y herramientas empleadas, asegurando su correcto funcionamiento.

Feedback de expertos: Consulta con profesionales en ciberseguridad para garantizar que el escenario refleje situaciones reales.

Herramientas: VMware o VirtualBox para emular infraestructuras TI sin afectar los sistemas reales.

Implementación del Escenario de Crisis

La ejecución del escenario será realizada en un entorno controlado, involucrando a todos los niveles organizacionales definidos. Las actividades incluirán:

Recolección de datos: Uso de herramientas de monitoreo para registrar las respuestas de los participantes en tiempo real, incluyendo tiempos de reacción, decisiones tomadas y resultados obtenidos.

Observación estructurada: Registro cualitativo de comportamientos, interacciones y toma de decisiones durante la simulación.

Herramientas: Microsoft Teams o Zoom para coordinar equipos en caso de una crisis real.

Análisis de Resultados

Los datos recolectados se procesarán mediante técnicas estadísticas y análisis cualitativo. Las actividades específicas incluirán:

Tabulación de datos: Organización de métricas clave, como tiempo de respuesta y efectividad en la contención del incidente.

Análisis descriptivo: Identificación de patrones y tendencias en las respuestas organizacionales.

Análisis comparativo: Comparación entre los resultados obtenidos en los diferentes niveles (táctico, técnico y ejecutivo) para identificar brechas y fortalezas.

Validación y Entrega Final

Finalmente, se realizará una validación integral del prototipo en una simulación completa, incluyendo:

Informe final: Presentación de los resultados y conclusiones, junto con recomendaciones para su aplicación en otros contextos.

Métodos de recolección de datos: Encuestas post-simulación, entrevistas con participantes y observación directa.

Herramientas estadísticas: Uso de software como SPSS o Excel para análisis descriptivos y gráficos.

Variables Clave del Proyecto

En el marco del desarrollo del escenario de crisis cibernética propuesto, se identifican las siguientes variables clave que permiten medir de manera efectiva la preparación organizacional ante un incidente de seguridad informática. Estas variables han sido definidas operativamente y se justifica su inclusión a partir de los objetivos del proyecto y de las mejores prácticas en simulación de crisis

Tiempo de Escalamiento

Definición operativa: Tiempo (en minutos) que tarda el equipo en comunicar el incidente al nivel técnico y ejecutivo tras su detección.

Justificación: Evalúa la efectividad del protocolo de escalamiento interno. Un tiempo alto puede retrasar las acciones correctivas y empeorar el impacto del incidente.

Tiempo de Contención

Definición operativa: Tiempo (en minutos) entre la detección del incidente y la aplicación efectiva de medidas técnicas para contener el ataque.

Justificación: Refleja la capacidad técnica de la organización para responder a un ataque en curso y limitar su propagación.

Impacto Residual

Definición operativa: Medida cualitativa o cuantitativa del daño persistente después de aplicar medidas de contención (por ejemplo: pérdida de datos, indisponibilidad de servicios, filtración de credenciales).

Justificación: Permite evaluar la efectividad real de las contramedidas aplicadas y el nivel de preparación ante recuperación post-incidente.

Tiempo de Respuesta Estratégica

Definición operativa: Tiempo (en minutos) que tarda la alta dirección en tomar decisiones estratégicas claves (como activar planes de contingencia, comunicar al público, involucrar autoridades).

Justificación: Mide la velocidad con que se responde desde la dirección a una situación de crisis, lo cual impacta directamente en la gestión integral del incidente.

Efectividad de la Comunicación de Crisis

Definición operativa: Evaluación cualitativa de la claridad, oportunidad y coherencia en los mensajes internos y externos emitidos durante la simulación.

Justificación: La comunicación efectiva es esencial para reducir el pánico, preservar la reputación organizacional y coordinar esfuerzos en todos los niveles.

Coordinación Interdepartamental

Definición operativa: Grado de colaboración y sincronización entre los equipos tácticos, técnicos y ejecutivos, medido mediante observaciones estructuradas y encuestas post-simulación.

Justificación: La coordinación efectiva es uno de los principales factores de éxito en la gestión de incidentes de ciberseguridad.

Resultados Esperados

El análisis de los resultados obtenidos en la simulación de crisis cibernética permitirá evaluar el nivel de preparación organizacional y la efectividad de los protocolos de respuesta en los niveles táctico, técnico y ejecutivo. Para ello, se emplearán métricas específicas que permitan cuantificar el desempeño de los participantes y extraer conclusiones sobre la capacidad de detección, mitigación y recuperación ante incidentes cibernéticos.

Métricas de Evaluación

Se utilizarán indicadores clave de rendimiento (KPIs) para analizar los resultados de la simulación:

Métricas a Nivel Táctico (Equipos Operativos y de Respuesta Inmediata)

Tiempo de detección del incidente (Detection Time - DT): Intervalo entre la ocurrencia del ataque y su identificación.

Precisión en la identificación de amenazas (Threat Classification Accuracy - TCA): % de inyectores correctamente clasificados como incidentes.

Tiempo de escalamiento del incidente (Escalation Time - ET): Tiempo que tarda el equipo táctico en reportar el evento al nivel técnico.

Métricas a Nivel Técnico (Equipos de TI y Ciberseguridad)

Tiempo de contención del ataque (Containment Time - CT): Tiempo desde la identificación hasta la neutralización de la amenaza.

Eficiencia en la implementación de contramedidas (Mitigation Effectiveness - ME): % de medidas aplicadas correctamente para bloquear el ataque.

Impacto residual (Residual Impact - RI): Medición del daño persistente tras la contención, como pérdida de datos o tiempo de inactividad.

Métricas a Nivel Ejecutivo (Toma de Decisiones y Comunicación de Crisis)

Tiempo de respuesta estratégica (Strategic Response Time - SRT): Tiempo en que la alta dirección toma decisiones clave.

Efectividad en la comunicación de crisis (Crisis Communication Effectiveness - CCE): Evaluación del manejo de la información ante stakeholders.

Coordinación interdepartamental (Interdepartmental Coordination - IC): Medición del nivel de colaboración entre áreas en la crisis.

Procesamiento y Análisis de Datos

Los datos obtenidos en la simulación serán tabulados y analizados mediante técnicas cuantitativas y cualitativas.

Análisis cuantitativo: Comparación de tiempos de respuesta, precisión y eficiencia entre los distintos niveles organizacionales.

Análisis cualitativo: Evaluación de la toma de decisiones y la gestión de crisis mediante encuestas post-simulación. Revisión de logs y grabaciones para identificar errores estratégicos y oportunidades de mejora.

Interpretación de Resultados y Aplicación

El análisis de resultados permitirá: Identificar fortalezas y debilidades en la respuesta organizacional, determinar ajustes en los protocolos de ciberseguridad y evaluar la replicabilidad del ejercicio en otras industrias y sectores.

Desarrollo del Proyecto

A continuación, se describen los aspectos clave que se tendrán en cuenta en la ejecución del ejercicio de simulación de crisis cibernética. Este proceso permitirá evaluar la capacidad de respuesta de la organización, identificar áreas de mejora y fortalecer la resiliencia ante incidentes de seguridad.

Preparación y Configuración del Ejercicio

Antes de la ejecución del ejercicio, se realizaron las siguientes actividades:

Determinar los escenarios específicos a simular y las áreas de la organización que participarán.

Asignación de roles, cada actor clave tendrá responsabilidades definidas en función del plan de respuesta a incidentes.

Implementación de entornos controlados para replicar la infraestructura real sin afectar los sistemas de producción.

Escenario

El ejercicio partió desde una afectación inicial a plataformas de terceros criticos para la entidad, y de allí se fueron derivando diferentes situaciones y afectaciones a plataformas propias de las organizaciones hasta llegar a una afectación a usuario final. Dentro del desarrollo del ejercicio se simularon incidentes como:

Ransomware: Se simuló porque es tipo de ataque muy común en la actualidad, y podría provocar interrupciones en los servicios de la entidad, así como grandes pérdidas económicas y reputacionales.

Defacement: Se simula la afectación de los sitios principales de la organización cambiando el contenido para difundir propaganda o información falsa, para afectar la reputación de la institución.

Exfiltración de datos: Se simula la exfiltración de datos sensibles de los clientes de la organización cómo, direcciones de domicilio, números de tarjetas de crédito, datos de contacto, datos biométricos.

Caída de plataformas digitales: En el caso de esta simulación se emula la caída de plataformas digitales para provocar interrupciones en los servicios críticos.

Durante la fase de estructuración se definieron para el “Storyline” un total 18 eventos donde se generarían los sucesos para un total de 100 inyecciones generadas durante el ejercicio de simulación.

Tabla 1

Listado de Eventos

#	Storyline
1	Afectación en la infraestructura que permite los pagos a través de Datáfonos.
2	Publicaciones en redes sociales y prensa.
3	Incidencia de *Ransomware* en los terminales de empleados de diferentes sucursales.
4	Grupo APT sin identificar exige el pago de un rescate.
5	Solicitud del ente de control pidiendo el estado actual del incidente.
6	Ataque de Defacement a páginas web de la organización.
7	Incidencia en pagos electrónicos realizados a través del botón de pago.
8	Incidencia en redes sociales. Publicación de contenido no autorizado por parte de un empleado.
9	Incidencia en redes sociales: Grupo hacktivista se atribuye falsamente el ataque.
10	Caída de servicios web.
11	Grupo APT sube precio de rescate y amenaza con publicar información confidencial.
12	Identificación de la fuente del incidente por parte del área de ciber.
13	Incidencia en redes sociales: Quejas masivas de clientes al no poder operar los servicios.
14	Solicitud del ente de control solicitando un informe resumen de la situación y acciones tomadas para la contención del ataque.
15	Publicación en Paste-bin con datos de clientes.
16	Campaña de phishing.
17	Descubrimiento de la causa raíz.
18	Fin del juego. Solicitud diligenciamiento encuesta.

Nota. Listado de los eventos lanzados en la simulación.

Roles a Delegar en la Simulación

CISO (Chief Information Security Officer): Responsable de la estrategia de ciberseguridad y la respuesta inmediata ante la amenaza.

CIO (Chief Information Officer): Coordina la recuperación de sistemas y restauración de servicios afectados.

Director de Operaciones: Garantiza la continuidad del negocio mientras se gestiona la crisis.

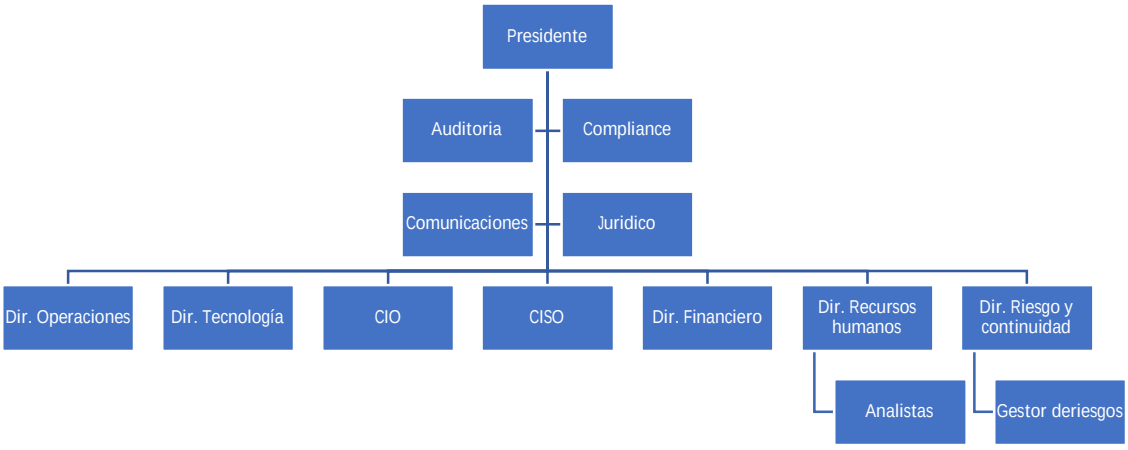
Director de Riesgos: Evalúa el impacto financiero y operativo del incidente.

Director de Comunicaciones: Responsable de la gestión de la comunicación interna y externa.

Director Jurídico: Garantiza el cumplimiento legal y regulatorio en la gestión del incidente.

Figura 1

Organigrama de Representación de Roles



Nota. Mapa de los roles a utilizar en la simulación de crisis.

Entornos Controlados

La simulación se llevó a cabo mediante una plataforma de correo electrónico. Cada rol contaba con acceso a una cuenta de correo donde llegaron los eMail que planteaban los diversos escenarios a resolver.

Los participantes debían discutir cada una de las situaciones planteadas y documentar en la plataforma de correo dichas decisiones.

El desarrollo del ejercicio se llevó a cabo en dos frentes, uno técnico y otro estratégico. Los equipos técnicos se encargaron de resolver las incidencias planteadas en la simulación, y a su vez, brindaban apoyo a los cargos ejecutivos.

Minutograma

Se construyó un minutograma detallado que establece la secuencia temporal de los eventos simulados y los inyectores a ser desplegados durante la ejecución del ejercicio. Este minutograma permite evaluar el tiempo de respuesta, el flujo de comunicación y la toma de decisiones bajo presión, y ha sido validado parcialmente durante la prueba piloto, mostrando buena adaptabilidad y realismo.

Los departamentos de TI y Ciberseguridad son los que acumularon un mayor número de incidencias. El guion diseñado para el escenario del ejercicio tiene un fondo técnico y estos son los departamentos que en caso real reciben las alertas de los servicios de monitoreo. A partir de ellos se canaliza el resto de la historia de los demás departamentos del juego.

Tabla 2

Minutograma

Tiempo	Evento (Storyline)	Inyector	Nivel impactado
00:05	1. Afectación en datáfonos	Correo de incidente desde soporte	Táctico
00:10	2. Publicaciones en redes y prensa	Captura de pantalla (fake tweet)	Ejecutivo
00:15	3. Ransomware en terminales	Alerta técnica / captura pantalla	Técnico
00:20	4. Exigencia de rescate por grupo APT	Correo tipo Ransomware	Ejecutivo
00:25	5. Solicitud de ente de control	Simulación de llamada / correo	Ejecutivo
00:30	6. Defacement sitio web	Imagen fake de página alterada	Técnico
00:35	7. Incidencia botón de pago	Notificación de fallas de usuarios	Táctico
00:40	8. Publicación no autorizada empleado	Captura simulada (red social)	Ejecutivo
00:45	9. Hacktivistas se atribuyen ataque	Post falso en redes	Ejecutivo
00:50	10. Caída de servicios web	Log técnico y quejas	Técnico
00:55	11. APT sube rescate y amenaza filtración	Segundo mensaje tipo *Ransomware*	Ejecutivo
01:00	12. Ciber identifica fuente del ataque	Informe técnico parcial	Técnico
01:10	13. Quejas masivas de clientes	Simulación de comentarios en redes	Ejecutivo
01:15	14. Solicitud de informe de control	Segunda solicitud formal	Ejecutivo
01:20	15. Publicación en Paste-bin con datos	URL simulada con datos	Técnico/Legal
01:25	16. Campaña de phishing detectada	Correo simulado tipo phishing	Técnico
01:30	17. Descubrimiento causa raíz	Informe final técnico	Técnico
01:40	18. Fin del juego / Encuesta	Link encuesta post-juego	Todos los niveles

Nota. Minuto a minuto de la simulación.

Herramientas de Ejecución

Correo simulado, documentos con pistas visuales, tabla de tabulación para calificación de respuestas.

Criterios de Evaluación

Los participantes deberían demostrar su madurez mediante el conocimiento de un plan de respuesta a incidentes, un equipo entrenado y preparado capaz de ejecutar una estrategia de manejo de crisis, y procesos claros para la coordinación de las respuestas en comunicados. Cada rol fue evaluado dentro del marco de una “escala ordinal convencional”, donde una calificación en los rangos de 5 y 4.5 es excelente, entre 4.4 y 3.5 es bueno, entre 3.4 y 2.5 es aceptable, entre 2.4 y 1. es malo y menor que 1, es pésimo.

La evaluación esta alineada a los siguientes puntos:

- Madurez: Evalúa el grado de conocimiento y experiencia en la gestión de ciber crisis.
- Estrategia: Evalúa la habilidad y destreza en el manejo de la situación.
- Sinergia: Evalúa la capacidad y empatía para comunicarse con sus pares y demás áreas involucradas

Evaluación de Desempeño

A continuación, se describen las acciones tomadas por el equipo en el desarrollo del ejercicio, así mismo, se destacan los aciertos y falencias de las decisiones tomadas por cada uno de los roles.

En general, hay varios aspectos por mejorar en el desempeño del grupo de trabajo que hizo parte de la simulación, debido a que obtuvo una puntuación aceptable de 3,4 en el promedio

de los criterios evaluados. Esto indica que el grupo tiene un nivel medio de preparación y capacidad de respuesta ante una crisis cibernética.

En el ámbito de la madurez, el grupo obtuvo una puntuación buena de 3.5 sobre 5, sin embargo, debe que enfocarse en trabajar las siguientes áreas:

Implementar un programa de concientización sobre aspectos como la Ingeniería Social para todos los empleados. Esto contribuirá a que los empleados comprendan que los riesgos de las ciber amenazas provienen de pequeños detalles.

Realizar evaluaciones de seguridad periódicas para identificar y mitigar las vulnerabilidades dirigidas a los procesos y a las personas. Esto ayudará a proteger los sistemas y datos del grupo.

Ajustar los planes de respuesta ante crisis cibernéticas teniendo en cuenta que debe ser claro, conciso y accesible para todos los empleados.

En el ámbito de la estrategia, el grupo obtuvo una puntuación de 3.1 sobre 5. Esto indica que la estrategia del grupo es aceptable pero poco eficaz. El grupo debería centrarse en mejorar los siguientes aspectos:

La claridad y la coherencia de la estrategia. La estrategia debe ser clara y concisa, y debe ser coherente con los objetivos y recursos del grupo.

La estrategia debe ser flexible para adaptarse a diferentes escenarios de crisis.

Ajustar la coordinación entre las diferentes áreas clave al interior y fuera de la organización.

En el ámbito de la sinergia, el grupo obtuvo una puntuación de 3.6 sobre 5. Esto indica que el grupo tiene un nivel de coordinación bueno, pero podría mejorar en las siguientes áreas:

Definir claramente los roles y responsabilidades de cada área. ¿Quién tiene la autoridad para tomar decisiones en cada área?

Establecer un proceso de comunicación y coordinación entre las diferentes áreas. ¿Cómo se comunicarán las diferentes áreas entre sí?

Realizar ejercicios de respuesta a crisis de forma periódica. Esto ayudará al grupo a probar su plan de respuestas y a identificar áreas de mejora.

Las siguientes son las valoraciones realizadas a cada uno de los roles tanto en lo asertivo como en las falencias identificadas en la toma de decisiones.

Tabla 3

Evaluación de Desempeño

Rol	Asertividad en la toma de decisiones	Falencias en la toma de decisiones	Madurez	Estrategia	Sinergia
Director de Operaciones	Recibió el correo de phishing y lo transfirió al CISO. Su comunicación fue homogénea.	Es clave no hacer suposiciones, porque se asumieron unos datos que no eran parte de la simulación, no era necesario añadir nada a los escenarios. Se recomienda ser más propositivo.	3.5	3.5	3.5
CIO	Sus instrucciones de contención del incidente fueron correctas. Las instrucciones de hacer frente a la campaña de phishing fueron acertadas.		4.5	3.8	4.8
CISO		Sus instrucciones se limitaron a ordenar la ejecución de planes teóricos sin aportar detalles específicos acordes con cada inyección. Solicitó takedown de la página de phishing a su director de Comunicaciones. Adicional, etiquetó como phishing los correos legítimos del equipo de TI con anexos.	3.8	3.0	3.5

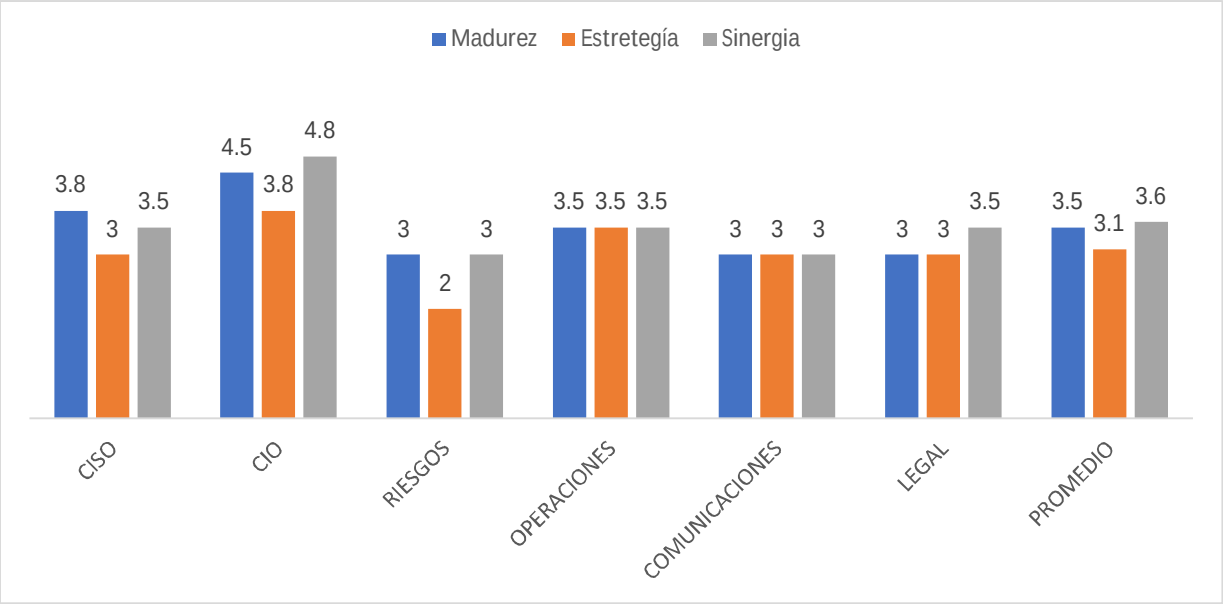
Rol	Asertividad en la toma de decisiones	Falencias en la toma de decisiones	Madurez	Estrategia	Sinergia
Comunicaciones		Se sugiere estar alineados con los protocolos o estándares propios de su entidad, Por el nerviosismo de la situación, el equipo replicaba las notificaciones de su propio departamento de Comunicaciones negando su valoración.	3.0	3.0	3.0
Riesgos	Propuso poner en marcha el protocolo de comunicación con inversionistas.	Se recomienda talleres de escucha activa en situaciones de estres debido a que el equipo tomó la vocería de no autorizar el rescate sin tener en cuenta los demás participantes. Solicitó instrucciones a la mesa para conocer lo que hacía en el resto de los equipos.	3.0	2.0	3.0
Legal	Asumió la vocería del comité de crisis	Se recomienda talleres de manejo de crisis y profundizar en conocimientos de los procedimientos de ciber crisis, porque: Se tomaron decisiones carácter técnico que le correspondían de frente al *Ransomware*.	3.0	3.0	3.5

Rol	Asertividad en la toma de decisiones	Falencias en la toma de decisiones	Madurez	Estrategia	Sinergia
		Ordenó a los equipos de TI que avanzaran en las investigaciones. Aprobó los comunicados del director de Comunicaciones. Se sugiere en ninguna circunstancia negociar con delincuentes, dado que estaba proponiendo la opción de pagar el rescate.			

Nota. Tabulación de la evaluación de desempeño de los participantes de la simulación.

Figura 2

Representación Gráfica de la Evaluación de Desempeño



Nota. Grafica de la evaluación de desempeño de los participantes de la simulación.

Hallazgos Importantes

Durante la evaluación de las respuestas relacionadas con el criterio de comunicación, se observó que en algunos casos no se respetaron los lineamientos establecidos en el plan de comunicaciones institucional. Específicamente, se identificaron situaciones en las que personas no autorizadas emitieron comunicados o realizaron publicaciones en redes sociales, sin estar designadas formalmente para esa función. Se recomienda a las organizaciones garantizar que solo los voceros previamente definidos en su plan de comunicaciones sean quienes se encarguen de informar al público externo, evitando así mensajes contradictorios o no oficiales.

El ejercicio incluyó un escenario frecuente: la divulgación no autorizada de información por parte de empleados. Esta situación, que puede comprometer tanto la imagen institucional como la seguridad de la información, fue presentada en dos momentos durante la simulación. Sin embargo, los participantes no adoptaron medidas específicas frente a este riesgo. Hubiese sido oportuno emitir una directriz interna recordando al personal la importancia de manejar con cautela la información compartida externamente, con el fin de evitar una percepción distorsionada de la crisis.

Adicionalmente, se diseñó un incidente donde un actor malicioso aprovechaba el caos generado por la crisis para lanzar una campaña de phishing, con el objetivo de obtener credenciales válidas de acceso a los sistemas de la entidad. A lo largo del ejercicio, se evidenció que dos usuarios fueron víctimas de esta campaña. No obstante, los participantes asumieron rápidamente que se trataba de un ataque dirigido, sin considerar la posibilidad de un ataque masivo. No fue sino hasta la intervención del equipo SOC simulado, que confirmó que se trataba de una campaña masiva, que se tomaron acciones pertinentes.

Tras esta notificación, surgió una reacción inesperada: los participantes comenzaron a considerar cualquier mensaje o enlace, incluso aquellos provenientes de cuentas legítimas creadas para el ejercicio, como potencialmente maliciosos. Esto generó solicitudes de bloqueo generalizado, lo que pone de manifiesto la necesidad de mejorar los protocolos de verificación y manejo de incidentes en situaciones de alta presión.

Resumen de Fortalezas

Es fundamental entender el ejercicio más allá de una simple medición cuantitativa del desempeño del equipo. El propósito principal no es únicamente evaluar un grupo de trabajo en su contexto inmediato, sino analizar transversalmente el cumplimiento de funciones clave, destacando elementos como la madurez organizacional, la estrategia adoptada y la sinergia entre los distintos equipos técnicos, incluyendo las áreas de tecnología, gestión de riesgos y ciberseguridad institucional.

Durante la simulación se identificaron diversas fortalezas y competencias destacadas, entre las que se pueden resaltar:

- Un alto nivel de motivación y compromiso por parte de todos los participantes, enfocados en alcanzar los objetivos propuestos durante el desarrollo del ejercicio.
- Una gestión técnica y operativa efectiva, demostrando habilidad y rapidez en la resolución de incidentes simulados.
- Una notable capacidad de adaptación y respuesta frente a las situaciones inesperadas planteadas por el ejercicio.
- A pesar de que la simulación estaba diseñada para inducir escenarios de alta presión propios de una crisis real, el equipo mostró un adecuado manejo emocional y técnico, lo que permitió mantener el control de la situación.

- Aunque se presentaron algunas acciones que no estuvieron plenamente alineadas con las directrices institucionales, en términos generales, el desempeño del grupo evidenció un nivel de compromiso satisfactorio y una apropiada comprensión de los roles asignados.

Resumen de Oportunidades de Mejora

Aunque el desempeño técnico general de los equipos durante el desarrollo del ejercicio fue positivo, es importante señalar que se identificaron algunas deficiencias en la gestión del flujo de la crisis por parte de ciertos roles organizacionales. Estas situaciones evidencian oportunidades claras de mejora, entre las que destacan:

Es imperativo fortalecer los niveles de conciencia en torno a la ciberseguridad y la gestión de crisis más allá de los equipos técnicos. Todas las áreas de la organización deben estar alineadas con los protocolos de respuesta y preparados para actuar ante situaciones críticas.

Resulta fundamental implementar programas de capacitación continua, así como desarrollar talleres de simulación periódicos, que abarquen a toda la organización y no se limiten a las áreas tecnológicas.

Debe promoverse una cultura de atención al detalle. Durante el ejercicio, algunos participantes fueron vulnerables a amenazas básicas como el phishing, lo que indica la necesidad de reforzar las competencias básicas en seguridad digital.

Asimismo, se observó que la activación del comité de crisis se realizó de forma anticipada, incluso antes de que los servicios principales de la entidad se vieran comprometidos. Esto sugiere la necesidad de revisar y afinar los criterios de activación, para asegurar una respuesta escalonada y oportuna ante incidentes que inicialmente afectan a terceros o a canales externos.

Con frecuencia, las estrategias y planes de ciberseguridad tienden a quedar restringidos a los equipos técnicos u operativos, lo que limita su efectividad institucional. Es fundamental comprender que la ciberseguridad debe ser abordada de manera transversal, integrando a todas las áreas de la organización. Solo así es posible construir una cultura de seguridad sólida, en la que cada actor, desde la alta dirección hasta el personal operativo, asuma un rol activo en la prevención, detección y respuesta ante incidentes.

Conclusiones

El desarrollo de este ejercicio de simulación de crisis cibernética permitió evaluar de manera integral la capacidad de respuesta de una organización ante incidentes de seguridad digital, desde una perspectiva táctica, técnica y ejecutiva. A través del diseño de un escenario estructurado y realista, la implementación de un minutograma dinámico, y la participación activa de los distintos roles, fue posible observar comportamientos, analizar decisiones y cuantificar métricas clave de desempeño.

Los resultados obtenidos demuestran que, aunque existen oportunidades de mejora en la coordinación interdepartamental y en la alineación con los planes de comunicación, el equipo mostró un nivel aceptable de preparación y un alto grado de compromiso frente a la crisis. Las acciones adoptadas, tanto técnicas como estratégicas, evidencian fortalezas en la respuesta operativa y en la capacidad de adaptación bajo presión.

Este ejercicio no solo contribuye a fortalecer la resiliencia organizacional, sino que también proporciona un modelo replicable para futuras simulaciones. Además, reafirma la importancia de integrar la ciberseguridad como una responsabilidad transversal a toda la organización, más allá de los equipos técnicos, y plantea la necesidad de mantener programas de capacitación continúa orientados a todos los niveles jerárquicos.

Glosario

Amenaza Cibernética

Evento o acción potencial que puede comprometer la seguridad de los sistemas de información, incluyendo malware, ataques de denegación de servicio (DDoS) y técnicas de ingeniería social (NIST, 2018).

Análisis de Riesgo

Proceso de evaluación de amenazas y vulnerabilidades para determinar la probabilidad de que un incidente ocurra y su impacto en la organización (ISO/IEC 27005:2018).

Cibercrisis

Situación en la que una organización enfrenta un incidente de seguridad informática que puede afectar su operación, reputación o confidencialidad de la información (ENISA, 2019).

Ciberseguridad

Conjunto de medidas y estrategias diseñadas para proteger la información digital contra accesos no autorizados, alteraciones o destrucción (ISO/IEC 27001:2022).

Escenario de Crisis

Simulación controlada de un incidente cibernético que permite evaluar la preparación y respuesta organizacional ante amenazas de seguridad (FEMA, 2019).

Gestión de Incidentes

Proceso estructurado para identificar, contener, mitigar y recuperar operaciones afectadas por un evento de seguridad informática (NIST SP 800-61r2, 2012).

Inyector

Elemento o evento simulado dentro de un escenario de crisis que desencadena una respuesta organizacional, permitiendo evaluar la toma de decisiones bajo presión (Mehan, 2020).

ISO 27001

Norma internacional que establece requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos (ISO, 2022).

Minutograma

Documento que detalla la secuencia de inyectores durante una simulación de crisis cibernética, especificando tiempos, actores e inyectores involucrados (Kolb, 2015).

NIST

Instituto Nacional de Estándares y Tecnología de Estados Unidos, responsable del desarrollo de marcos de referencia para la ciberseguridad, como el Cybersecurity Framework y la gestión de incidentes (NIST, 2018).

Phishing

Técnica de ataque basada en la ingeniería social que busca engañar a los usuarios para que revelen información confidencial, como credenciales o datos bancarios (MITRE ATT&CK, 2023).

Resiliencia Cibernética

Capacidad de una organización para anticiparse, resistir y recuperarse de incidentes cibernéticos sin que estos afecten gravemente su operación (World Economic Forum, 2023).

Simulación de Incidentes

Técnica utilizada para entrenar a los equipos de respuesta ante ciberataques, replicando escenarios realistas en un entorno controlado (Wheeler, 2022).

Tabletop Exercise

Método de simulación de crisis en el que los participantes analizan un escenario hipotético para evaluar estrategias de respuesta y toma de decisiones sin ejecutar acciones reales en infraestructura (Gaba, 2004).

Vulnerabilidad

Debilidad en un sistema informático o en las políticas de seguridad que puede ser explotada por amenazas para comprometer la confidencialidad, integridad o disponibilidad de los datos (ISO/IEC 27002:2022).

Referencias

Alhassan, A., & Adjei, J. (2024). *Scenario-Based Incident Response Training: Improving Decision-Making in Cybersecurity Crisis Management.* arXiv. https://arxiv.org/pdf/2404.10988

Alvarez, F., & Martinez, J. (2022). *Building Cybersecurity Awareness: Case Studies and Best Practices.* Cybersecurity Journal, 14(3), 45-62.

CISA. (2021). *Ransomware Attack on Colonial Pipeline: Lessons Learned and Best Practices.* Cybersecurity & Infrastructure Security Agency.

Diálogos Punitivos. (2023). *Protección de datos personales en Colombia: Riesgos y sanciones.* Recuperado de https://dialogospunitivos.com/proteccion-de-datos-personales-en-colombia-riesgos-y-sanciones

Dwight, J. (2023). Collaborate, Design, and Generate Cybercrime Script Tabletop Exercises for Cybersecurity Education. En Proceedings of the 31st International Conference on Computers in Education (ICCE 2023) (pp. 255-264). Matsue, Shimane. ISBN 978-626968902-6.

European Union Agency for Cybersecurity (ENISA). (2019). *Incident Handling and Response.* ENISA Publications. https://www.enisa.europa.eu/publications/incident-handling-and-response

European Union Agency for Cybersecurity (ENISA). (2022). *Cyber Europe 2022: Large-scale cyber crisis exercise.* European Union Agency for Cybersecurity.

Federal Emergency Management Agency (FEMA). (2019). *Incident Response Framework: National Incident Management System (NIMS).* U.S. Department of Homeland Security.

Gaba, D. M. (2004). *The future vision of simulation in healthcare.* Quality and Safety in Health Care, 13(Suppl 1), i2–i10.

IBM Security. (2023). *Cost of a Data Breach Report 2023.* IBM.

Iglesias, R. (2024). *Impacto del Ransomware en instituciones educativas: Caso Universidad Autónoma de Barcelona.*

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 - Information technology — Security techniques — Information security management systems — Requirements.* ISO.

iTech SAS. (2018). *Multa a Scotiabank Colpatria por deficiencias en la gestión de datos personales.* Recuperado de https://www.itechsas.com/blog/tag/multas

iTech SAS. (2018). *Sanción a CIFIN por incumplimiento en seguridad de la información.* Recuperado de https://www.itechsas.com/blog/tag/multas

Kolb, D. A. (2015). *Experiential Learning: Experience as the Source of Learning and Development.* Pearson Education.

Kvietinskaitė, G., Bukauskas, L., & Krinickij, V. (2023). Cyber Security Table-Top Exercise Gamification with Dynamic Scenario for Qualification Assessment. 31st International Conference on Computers in Education (ICCE 2023).

Lores Acosta, P. (2024). *Ciberseguridad en infraestructuras críticas: El caso de los puertos en Colombia.*

Mehan, J. E. (2020). *Cyberwarfare Techniques, Tactics and Tools for Security Practitioners.* Elsevier.

MITRE Corporation. (2023). *ATT&CK Framework: A Guide to Adversarial Tactics and Techniques.* MITRE.

National Cybersecurity Alliance. (2022). *Building Resilient Organizations: Cybersecurity Best Practices.* Cybersecurity Reports.

Norsk Hydro. (2019). *Cyber attack: Lessons learned and response strategies.* Norsk Hydro.

Omand, D., Bartlett, J., & Miller, C. (2022). *How Spies Think: Ten Lessons in Intelligence.* Penguin Random House.

Pérez, J. M. (2020). *Impacto del ciberataque en la seguridad internacional.* Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=9061864#

Phaal, R., Farrukh, C. J., & Probert, D. R. (2004). *Technology roadmapping—A planning framework for evolution and revolution.* Technological Forecasting and Social Change, 71(1-2), 5-26.

Signorino Barbat, A. (2022). *Los Seguros Cibernéticos: Alcance frente a los Ciber Riesgos.* EBSCO.

Snyder, H. (2019). *Literature review as a research methodology: An overview and guidelines.* Journal of Business Research, 104, 333-339.

Springer. (2023). *Cybersecurity in Financial Systems: Improving Response to Fraud and Cyber Threats.* https://link.springer.com/article/10.1007/s10207-023-00704-z

Superintendencia de Industria y Comercio (SIC). (2019). *Multas impuestas por violaciones a la Ley de Protección de Datos Personales en Colombia.* Recuperado de https://www.sic.gov.co/sabia-usted

Tandfonline. (2021). *Cybersecurity Exercises: Bridging the Gap Between Theory and Practice in Incident Response.* https://www-tandfonline-com.bibliotecavirtual.unad.edu.co/doi/full/10.1080/19393555.2021.1980159

Telos. (2023). *Cybersecurity in the Age of Hybrid Warfare.* Fundación Telefónica Publications. https://telos.fundaciontelefonica.com

The Economist Intelligence Unit. (2020). *Global Cybersecurity Index 2020: Trends and Insights.* The Economist.

Wheeler, E. M. (2022). *Cybersecurity for Business: Protecting Your Digital Assets.* Wiley.

Wiley Online Library. (2023). Cybersecurity Research: Challenges and Opportunities in 2023. Security and Privacy, 2(126). https://onlinelibrary.wiley.com/doi/10.1002/spy2.126

World Economic Forum. (2023). *The Global Risks Report 2023.* WEF. https://www.weforum.org/reports/the-global-risks-report-2023/

Zafra Díaz, J. M. (2023). *Los ciberataques son parte de la guerra híbrida que persigue causar inestabilidad y desconfianza.* Telos.