UNIVERSIDAD CENTRAL

VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

PROPUESTA DE DISEÑO E IMPLEMENTACIÓN DE UN MODELO DE CIBERSEGURIDAD PARA LA MEJORA EN LA GESTIÓN DE RESPUESTA A INCIDENTES Y AMENAZAS EN BN FONDOS

MODALIDAD DE TESIS PARA OPTAR POR EL GRADO DE LICENCIATURA EN INFORMÁTICA CON ÉNFASIS EN GERENCIA INFORMÁTICA

ELABORADO POR:

JULIO ALONSO BRENES RUEDA

TUTOR:

RODRIGO GUERRERO JIMÉNEZ

SEDE CENTRAL

DICIEMBRE, 2024

Índice General

Índice de Tablas

Índice de Figuras

Dedicatoria y Agradecimiento

Quiero agradecer a mi esposa Seidy, mis hijas Isabella, Mónica, María Fernanda y Stephanie, quienes con su amor y apoyo incondicional me motivaron a seguir adelante a pesar de los contratiempos y atenciones que se deben brindar en el hogar, en el trabajo y demás aspectos que median en nuestra vida diaria; por el tiempo que no logré compartir con ellas por atender el compromiso del estudio con el fin de poder cumplir y finalizar una meta educativa adicional.

Agradezco a Jehová Dios, por darme en cada amanecer un día más de vida, un regalo preciado que nos da Jehová en medio de tiempos difíciles.

Resumen Ejecutivo

El proyecto tuvo como objetivo diseñar e implementar un modelo integral de gestión de incidentes y ciberresiliencia adaptado a las necesidades de BN FONDOS. Se buscó fortalecer la capacidad de respuesta ante incidentes de ciberseguridad y garantizar la continuidad del negocio mediante la creación de un sistema documentado de políticas, procedimientos, capacitación y herramientas técnicas.

La metodología utilizada se basó en el marco de trabajo NIST CSF 2.0 y en normativas de ciberseguridad internacionales, personalizando el enfoque a la operativa de BN Fondos. Esto incluyó una serie de fases: análisis de riesgos, evaluación de vulnerabilidades, y la integración de prácticas de gestión de incidentes y recuperación ante desastres.

Dentro de los principales resultados de la investigación están los siguientes:

Creación de manuales y procedimientos: Se desarrollaron manuales específicos de gestión de incidentes y recuperación ante desastres, así como procedimientos detallados que optimizan el tiempo de respuesta a incidentes críticos, garantizando una actuación rápida y organizada.

Propuesta de normativa interna y capacitación: Se diseñaron normativas internas de ciberseguridad para uniformizar la respuesta a incidentes, acompañadas de materiales de capacitación para todo el personal de BN FONDOS. La capacitación incluyó simulaciones prácticas que fortalecieron la preparación de los empleados.

Herramientas de soporte y arquitectura técnica: Se seleccionaron herramientas tecnológicas para el monitoreo y respuesta a incidentes y se diseñó una arquitectura de hardware y software que facilita la integración de las herramientas en los sistemas de BN FONDOS, permitiendo una visibilidad completa del entorno de seguridad.

Modelo de ciberresiliencia: Se implementó un modelo de ciberresiliencia que asegura la continuidad del negocio incluso ante incidentes de gran impacto, estableciendo un plan de continuidad y recuperación estructurado, con métricas de recuperación alineadas a los objetivos del negocio.

En conclusión, el resultado de la investigación permite a BN FONDOS obtener una mayor capacidad de respuesta y ciberresiliencia, asegurando la protección de los activos digitales y una mejor preparación frente a incidentes de ciberseguridad. Las políticas y procedimientos establecidos, junto con la capacitación del personal y la arquitectura de soporte, ofrecen una base sólida para mitigar riesgos futuros. Este modelo no solo responde a las necesidades actuales de BN FONDOS, sino que también permite su escalabilidad ante nuevos desafíos en ciberseguridad.

Capítulo I: Problema

Planteamiento del Problema

En el entorno empresarial actual, tanto en el ámbito público como en el privado, la seguridad de la información ha emergido como un pilar fundamental para garantizar la continuidad y la integridad de las operaciones. La protección de los datos empresariales es crucial, dado que la información constituye uno de los activos más valiosos para cualquier organización. La creciente amenaza de ciberataques, que busca robar o secuestrar estos datos, ha obligado a las empresas a establecer y fortalecer los sistemas de seguridad que mitiguen los riesgos asociados.

A nivel mundial, las empresas de todos los sectores se enfrentan a un número creciente de amenazas cibernéticas. Según estadísticas reportadas por Arroyo Guardeño (2020), en España, solo en el año 2019 se cometieron 218.302 delitos, lo que representó el 10% de todos los delitos cometidos en ese año y supuso un incremento del 35.81% respecto al año 2018. Dentro de estas cifras, el fraude informático destacó con 192.375 casos, seguido por amenazas y coacciones, falsificaciones informáticas, accesos e interceptaciones ilícitas, y delitos contra el honor, entre otros. Este crecimiento exponencial en los delitos cibernéticos es indicativo de una tendencia global en la que los ciberataques se vuelven cada vez más sofisticados y frecuentes, exigiendo a las organizaciones la adopción de medidas más rigurosas de ciberseguridad.

En América Latina, el panorama no es diferente, Aguilar (2021) destaca que, desde el 2012, los ciberataques en la región han crecido a tasas anuales superiores al 61%. Países como Ecuador, Guatemala, Bolivia, Perú y Brasil, se encuentran entre los más afectados por el malware y desde 2015, el fraude bancario ha emergido como una amenaza significativa, con un

92% de las entidades financieras reportando algún tipo de ciberataque, y con una tasa de éxito del 37%. Estos datos subrayan la urgencia de que las organizaciones latinoamericanas fortalezcan sus defensas cibernéticas para proteger sus activos más críticos.

Un ejemplo paradigmático de las consecuencias devastadoras que pueden tener los ciberataques es el caso de Costa Rica en el año 2022. Según Cano (2022), la ola de ciberataques que ha afectado al país se enmarca en un contexto más amplio de inestabilidades geopolíticas global. Este caso evidenció cómo el ransomware, un tipo de código malicioso que secuestra datos para exigir un rescate y puede paralizar completamente las operaciones de las instituciones públicas. Este riesgo no solo puso en riesgo la información sensible de las entidades afectadas, sino que también comprometió la reputación y la credibilidad del país en el ámbito internacional.

La ciberdelincuencia en Costa Rica y sus efectos no pueden ser subestimados. La capacidad de un ciberataque para paralizar por completo a una organización y exponer su imagen públicamente crea un riesgo de reputación que puede tener repercusiones severas en su permanencia en el mercado. La necesidad de contar con un modelo robusto de gestión de incidentes de ciberseguridad es, por lo tanto, no solo una medida de protección, sino una cuestión de supervivencia empresarial.

En este contexto global y regional, surge la necesidad imperiosa de que las organizaciones, especialmente las que manejan información crítica y sensible, desarrollen estrategias de ciberseguridad más efectivas. Este es el caso de la Sociedad Administradora de Fondos de Inversión, BN FONDOS del Banco Nacional de Costa Rica, dado lo expresado previamente, en BN FONDOS existe una necesidad que se debe solventar y se enfoca en el área de atención de incidentes de ciberseguridad. Dentro de BN FONDOS en el contexto citado se identifica claramente la necesidad de implementar un modelo para la gestión de respuesta a

incidentes y amenazas ante ataques de ciberseguridad, con el fin de garantizar la oportuna, la resolución eficiente y la continuidad del negocio con la menor afectación posible. Esta medida es esencial para salvaguardar no solo la reputación de BN FONDOS, sino también los servicios que presta a sus clientes y al ciudadano costarricense en general.

Cano (2022) subraya que, en el caso de un ciberataque, es crucial entender la diferencia entre un evento de seguridad de la información, que puede o no afectar al negocio o a la información. Por lo tanto, es de gran relevancia diseñar e implementar modelos de atención que permitan a las organizaciones responder de manera rápida y eficiente a estos incidentes para minimizar su impacto. Esto requiere la asignación de recursos humanos, materiales, organizados adecuados que permitan gestionar las amenazas de manera efectiva y oportuna.

BN FONDOS, al igual que muchas otras organizaciones, enfrenta una serie de desafíos en la gestión de la ciberseguridad. Algunos factores identificados como variables problemáticas ante ciberataques incluyen:

- Escasos presupuestos para las áreas de tecnología: La falta de recursos financieros adecuados para invertir en tecnologías de ciberseguridad avanzada limita la capacidad de las organizaciones para protegerse eficazmente contra las amenazas emergentes.
- Escasos controles en la seguridad de la información: La ausencia de planes de contingencia bien definidos pone en riesgo la capacidad de las organizaciones para recuperarse rápidamente de un incidente de seguridad.
- Carencia de planes de prevención y concienciación de ciberseguridad: La falta de programas de conciencia y capacitación en ciberseguridad entre los empleados

incrementa el riesgo de que estos caigan víctimas de ataques como el phishing, facilitando así el acceso no autorizado a los sistemas de la organización.

La evolución tecnológica y el incremento de las amenazas cibernéticas exige que las organizaciones adapten continuamente sus estrategias de seguridad de la información. En el caso de BN FONDOS, es imperativo que se diseñen, preparen e implementen medidas de seguridad informática, planes de gestión de respuesta a incidentes y estrategias de ciber resiliencia que permitan una pronta recuperación de los servicios en caso de una intrusión.

Esto no solo protegerá la información y la reputación de la entidad, sino que también garantizará la continuidad del negocio, manteniendo la confianza de los clientes y público en general.

¿Problema de investigación?

¿Cómo puede la implementación de un modelo integral de gestión de incidentes y ciber resiliencia en BN FONDOS del Banco Nacional de Costa Rica mitigar efectivamente el riesgo de ciberataques, garantizar la continuidad del negocio y proteger la reputación de la entidad en un entorno de amenazas cibernéticas en constante evolución?

Objetivos

De acuerdo con el problema de investigación planteado se ha determinado el objetivo general y objetivos específicos, a continuación, se mencionan.

Objetivo General

Diseñar un modelo integral de gestión de incidentes y ciber resiliencia para BN FONDOS del Banco Nacional de Costa Rica para mitigar efectivamente el riesgo de ciberataques,

garantizar la continuidad del negocio y proteger la reputación de la entidad mediante la implementación de estrategias de prevención, respuesta y recuperación ante la presencia de amenazas cibernéticas.

Objetivos Específicos

1. Analizar las principales amenazas cibernéticas que afectan a BN FONDOS del Banco Nacional de Costa Rica para identificar los riesgos críticos que deben ser abordados en el modelo de gestión de incidentes y ciber resiliencia mediante la recopilación de datos históricos de ciberataques.
2. Evaluar los resultados históricos de pruebas de penetración efectuadas en la infraestructura tecnológica de BN FONDOS para determinar posibles brechas de vulnerabilidades existentes que podrían comprometer la continuidad del negocio mediante auditorías de seguridad informática y pruebas de penetración.
3. Desarrollar estrategias específicas de prevención, respuesta y recuperación para mitigar el impacto de posibles ataques en BN FONDOS mediante la integración de mejores prácticas de ciberseguridad y la alineación con estándares internacionales.
4. Proponer un sistema de monitoreo y detección temprana de amenazas para fortalecer la capacidad de BN FONDOS para responder de manera oportuna y efectiva incidentes de seguridad mediante el uso de tecnologías avanzadas de inteligencia artificial y análisis predictivo.
5. Diseñar un plan de capacitación para el personal de BN FONDOS en ciberseguridad y gestión de incidentes para garantizar una respuesta coordinada y eficiente ante

ciberataques mediante un programa de formación continua y simulaciones de ciberataques.

Justificación

El propósito de la presente investigación es determinar la viabilidad de implementar un modelo integral de gestión de incidentes y ciber resiliencia para BN FONDOS con el cual se pueda mitigar efectivamente el riesgo de ciberataques, garantizar la continuidad del negocio y proteger la reputación de la entidad mediante la implementación de estrategias de prevención, respuesta y recuperación ante la presencia de amenazas cibernéticas.

Arroyo Guardeño (2020) menciona que la protección de una infraestructura tecnológica requiere identificar amenazas y para ello debe establecer e implementar mecanismos de protección y medidas preventivas, como lo son procesos y políticas de seguridad en la que se definen los recursos a proteger, tales como los centros de datos, equipos tecnológicos, bases de datos, entre otros. Para lo cual se debe evaluar la importancia de cada uno de ellos, la probabilidad que se vea afectado por un ciberataque y el impacto que puede tener en el negocio de la institución.

En consecuencia, se determina que los incidentes de seguridad requieren una atención rápida y eficiente para minimizar los impactos en la organización; Moreno García (2022) detalla que el objetivo primordial de una dirección de la organización es establecer una buena gestión de incidentes de seguridad. Amplía mencionado que el equipo de respuesta antes incidentes es el conjunto de analistas especializados que darán respuesta a cualquier notificación sobre un incidente. Estos equipos definidos previamente por la alta gerencia deben estar disponibles para

detectar, analizar cualquier amenaza, clasificar su impacto, atención y resolución inmediata para mitigar los daños y restablecer la normalidad de los servicios en el menor tiempo posible.

La presente investigación se realiza con el fin de determinar un modelo de gestión de incidentes en BN FONDOS el cual permita optimizar la plataforma tecnológica y los servicios que brinda el negocio a los clientes en general.

Según el Ministerio de Ciencia (2023), la Estrategia de Ciberseguridad 2023-2027 establecida por el Gobierno de Costa Rica, esta estrategia proporciona una visión cohesiva y convincente construida por todas las partes interesadas, ya sea públicos o privados, la cual aborda las necesidades y los desafíos que promueven la igualdad de oportunidades y la participación en las iniciativas de ciberseguridad.

La estrategia en mención se enfoca en mitigar las múltiples amenazas y así proteger los intereses de las empresas en Costa Rica. Por esta razón, para BN FONDOS es vital poder contar con un modelo de atención de incidentes y resiliencia para proteger de manera efectiva las infraestructuras críticas de la organización.

La problemática de ciberataques, como bien es conocido se ha incrementado en los últimos años, según Espinoza Reyes (2024) posterior a los eventos de ciberataques, los cuales fueron reconocidos internacionalmente en el año 2022, Costa Rica pasó a formar parte como un país de interés para los ataques cibernéticos, ya que los análisis post ataques mostraron severas carencias y deficiencias en la seguridad de las instituciones gubernamentales. Uno de los hallazgos más importantes fue la detección de falta de procesos eficientes y de monitoreo continuo en materia de ciberseguridad, los cuales hubiesen mitigado el impacto negativo a nivel económico, social, comercial y político.

Dadas las justificantes previamente mencionadas y el alto grado de riesgos identificados dentro y fuera del territorio nacional se deben evaluar normativas y marcos de trabajo que contribuyan a solucionar el problema de estudio.

Todos los factores indicados previamente vuelven relevantes la investigación para BN FONDOS misma que es de gran beneficio para garantizar ante el cliente o usuario final que el servicio brindado y sus datos confidenciales están protegidos y mantienen su integridad.

Antecedentes

Hoy en día las empresas o instituciones no están preparadas para los ciberataques y pueden ser víctimas por esta modalidad de los delincuentes tecnológicos, los impactos o efectos post ciberataques pueden afectar la operativa diaria junto con la pérdida de información confidencial de las mismas; lo cual ha llevado a una revolución tecnológica y administrativa para la protección de los datos.

Con el fin de evaluar el estado del arte de investigaciones previas tanto nacionales como internacionales que aporten valor al proceso de investigación, a continuación, se citan y analizan los siguientes antecedentes.

Antecedentes Internacionales

Un primer trabajo corresponde a Guardeño (2020), lleva por título “Ciberseguridad”. Se trata de un análisis e investigación de como la tecnología día a día crece y aun mismo tiempo se hace vulnerable a las personas y empresas del mundo. Por ellos se enfocan en las amenazas y los ataques a las plataformas tecnológicas y los sistemas de seguridad que se deben implementar.

La investigación enuncia lo siguiente:

En términos globales es posible tener una idea del impacto de las incidencias de ciberseguridad a través de una estimación del coste económico que las fallas de seguridad, los ciberataques y los ciberdelitos han ocasionado a empresas y ciudadanos. Según el Observatorio Español de Delitos Informáticos, en el 2019 el ciberdelito implicó pérdida del orden de millones de euros a las víctimas. El informe de Accenture (2019) señala que, en los próximos cinco años, las empresas del sector privado corren el riesgo de perder alrededor de 5,2 billones de dólares debido a los ciberataques, lo cual es casi el tamaño de las economías de Francia, Italia y España. (Arroyo Guardeño, 2020, p. 18)

Este extracto se relaciona con la investigación en curso, ya que muestra claramente como los ciberataques tienen un gran impacto económico en las empresas a nivel mundial, también refleja que los departamentos de tecnología presentan fallas de seguridad informática; adicionalmente proyectan que a futuro las pérdidas económicas pueden llegar a incrementar en un plazo de 5 años.

Un segundo trabajo corresponde a Ametller (2021), lleva por título “Ciberseguridad, Un nuevo reto para el Estado y los Gobiernos Locales”. Esta investigación trata de como las personas hoy en día se encuentran con una inseguridad en varios ámbitos; su enfoque se basa en la urgencia que los gobiernos o estados deben adoptar medidas efectivas ante los riesgos de robos cibernéticos.

El análisis efectuado indica que:

La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio del 2016, estableció las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS), esto es, las obligaciones de seguridad de los operadores de servicios esenciales que dependan para su provisión de redes y

sistemas de información; y de los proveedores de servicios digitales. La Directiva NIS fue incorporada a nuestro ordenamiento jurídico interno por el mencionado Real Decreto-ley 12/2018, de 7 de setiembre (RDLSRSI). (Canals Ametller, 2021, p. 82)

Este extracto se relaciona con la investigación en curso, ya que muestra como el Parlamento Europeo establece políticas o medidas a nivel internacional para fortalecer las medidas de seguridad ante ciberataques; por lo tanto, es importante esta referencia para tener claridad de las acciones que países desarrollados están tomando acciones para mitigar los efectos de los ciberataques los cuales se deberían tomar como modelo para nuestro país.

Un tercer trabajo corresponde a Moreno García (2022), lleva por título "Gestión de Incidentes de ciberseguridad". El objetivo de la investigación es definir las directrices necesarias a establecer en una organización la gestión y atención de incidentes de ciberseguridad, cual es el ciclo de vida de una gestión de un incidente y dar a conocer las normativas internacionales que se deben tomar en consideración como lo es la NIST.

La investigación enuncia lo siguiente:

NIST es el acrónimo de Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology), organismo dependiente del Departamento de Comercio de Estados Unidos.

Como resultado de la creciente cantidad de ciberataques a sistemas de infraestructuras críticas y al impacto que dichos ataques pudieran tener en el contexto de la seguridad nacional de Estados Unidos, el 1 febrero de 2013 el Presidente Barack Obama redactó la Orden Ejecutiva (EO) de Mejora de Ciberseguridad de Infraestructuras Críticas (Execute Oder 13636 – Improving Critical Infraestructure Cybersecurity) en donde delegaba en el NIST el desarrollo de un marco

de trabajo para la reducción de riesgos asociados con este tipo de entornos, con el soporte del Gobierno, la industria y los usuarios. (Moreno, 2022, p. 17)

Este extracto aporta a la investigación en curso recomendaciones que podrán ser valoradas y tomadas en consideración para el objetivo de la investigación, ya que la norma NIST (Instituto Nacional de Estándares y Tecnología) hace referencia y orientación para identificar las normas y directrices de seguridad para ser establecida y aplicada en infraestructuras críticas.

Un cuarto trabajo corresponde a Moreno García (2022), lleva por título "Gestión de Incidentes de ciberseguridad". El objetivo de la investigación también pretende clasificar los diferentes tipos de incidentes que se pueden presentar lo cual contribuya a las empresas a establecer planes de trabajo de atención, análisis, contención y erradicación.

La investigación menciona:

Puesto que no todos los incidentes poseen las mismas particularidades ni tienen las mismas implicaciones, cada organización debe establecer una taxonomía de los incidentes a gestionar, lo que ayudará posteriormente a su análisis, contención y erradicación.

Crear una taxonomía no es una tarea sencilla. Puede haber diferentes formas de clasificar los incidentes y no siempre es fácil o posible determinar cuál es la mejor. Muchas organizaciones a menudo terminan desarrollando su propia taxonomía inspiradas en las proporcionadas por organismos de referencia de incidentes con un marco legal. (Moreno, 2022, p. 23)

Este extracto se relaciona con la investigación en curso, ya que es esencial para comprender y determinar cómo se realiza la clasificación de incidentes y su respectivo ciclo de vida.

Antecedentes Nacionales

Un primer trabajo corresponde a Cano (2022), lleva por título “El ransomware: una estrategia de desestabilización geopolítica. El caso de Costa Rica”. El objetivo de este análisis es representar los crecientes eventos de ciberataques a sistemas críticos y las tensiones e inestabilidades geopolíticas que pueden afectar un país. Hace énfasis en la materialización de ataques tipo ransomware en las instituciones públicas de Costa Rica.

La investigación menciona:

Los eventos recientes relacionados con el ataque cibernético efectuado a las instituciones del gobierno de Costa Rica muestran una nueva faceta de las tensiones geopolíticas ahora desde la perspectiva cibernética. El ransomware (o secuestro y extorsión con datos – de ahora en adelante RSW) se configura como un arma y una estrategia donde convergen los intereses de grupos criminales internacionales que buscan obtener ganancias por cuenta de estos eventos, con el deterioro de las instituciones y las vulnerabilidades cognitivas de las naciones, que sólo requieren de un motivo para activarse, y así, crear la inestabilidad que desencadene acciones adversas que afecten la dinámica de las naciones y socaven la institucional de los gobiernos.

Por tanto, este documento desarrolla un breve análisis de los eventos que han ocurrido en Costa Rica, considerando las noticias y documentos públicos disponibles a la fecha, para desde allí establecer una base conceptual y práctica del uso del RSW como una estrategia y arma de desestabilización geopolítica, que motivada desde los elementos claves como deterioro o falta de atención sobre infraestructuras críticas (de información y cibernéticas), las vulnerabilidades cognitivas de las sociedades y las tensiones políticas, sociales y económicas de un país, es capaz de concretar operaciones cibernéticas que cambien el rumbo de la dinámica de un Estado y por tanto, la lectura de los conflictos modernos (Cano, 2022).

Este extracto se relaciona con la investigación en curso, ya que es base para determinar por qué las instituciones públicas en Costa Rica pueden estar expuestas al robo o secuestro de datos críticos, y a su vez, tomar las acciones correctivas y preventivas para no tener un impacto significativo y económico en las empresas.

Un segundo trabajo corresponde al Informe del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (2023-2027), lleva por título "Estrategia Nacional de Ciberseguridad de Costa Rica". El objetivo de este documento es establecer una nueva Estrategia Nacional de Ciberseguridad 2023-2027 la cual brinde una visión estratégica bajo un modelo institucional que refuerce la gobernanza de ciberseguridad.

El documento menciona:

El ransomware, el phishing, las estafas en línea y la intrusión informática (es decir, la piratería) son las tendencias de ciberdelincuencia que perciben los países con mayor frecuencia como amenazas "altas" o "muy altas" a nivel mundial (INTERPOL, 2022), conllevando a la indisponibilidad de servicios ofrecidos virtualmente, el robo de información, o incluso la afectación a servicios esenciales generando consecuencias negativas en el bienestar económico de la ciudadanía o en el eficaz funcionamiento de las organizaciones privadas o públicas.

Costa Rica cuenta con un marco jurídico y reglamentario para proteger a la sociedad contra la ciberdelincuencia y promover un entorno cibernético seguro, de conformidad con los principios de inclusión y de entorno de confianza.

El país ha suscrito convenios y tratados internacionales asumiendo varios compromisos internacionales que tienen relación con la ciberseguridad, por ejemplo instrumentos: para proteger y garantizar los derechos humanos, en especial los derechos humanos básicos que deben disfrutar los niños, las niñas y adolescentes, para eliminar la discriminación contra la mujer, para

prevenir, sancionar y erradicar toda forma de violencia contra la mujer, para impulsar el desarrollo sostenible, para desarrollar legislación nacional integral sobre ciberdelitos, para combatir la impunidad de quienes han cometido crímenes de extrema gravedad, para prevenir y combatir más eficazmente la delincuencia organizada transnacional, entre otros (Ministerio de Ciencia, 2023, pp. 6-7).

Este extracto se relaciona con la investigación en curso, ya que BN FONDOS por ser una entidad pública debe someterse a las normas establecidas por el Gobierno de Costa Rica, lo cual va a contribuir con establecer las mejores prácticas contra ciberataques.

Un tercer trabajo corresponde a Espinoza (2024), lleva por título “Fortaleciendo la ciberseguridad en Costa Rica: Monitoreo, pilar en la detección de amenazas”. La tesis presentada hace ver que Costa Rica se ha convertido en un país víctima de ciberataques, lo cual muestra la carencia o debilidad en aspectos de ciberseguridad principalmente en el sector público, recalca la necesidad de mejorar los sistemas de monitoreo para la detección de amenazas cibernéticas.

El documento menciona:

Luego de los eventos de ciberataques, reconocidos internacionalmente en el año 2022, Costa Rica se posicionó como un objetivo de interés para adversarios cibernéticos, que dejaron en evidencia severas carencias dentro de la postura de seguridad en instituciones gubernamentales. Uno de los hallazgos más importantes es la falta de un proceso eficiente de monitoreo continuo de ciberseguridad en un contexto nacional, sectorial e institucional, que hubiese podido mitigar el impacto negativo a nivel económico, social, comercial y político. En materia de seguridad cibernética, la visibilidad se comprende como la capacidad de conocer e interpretar lo que sucede en el entorno tecnológico de las organizaciones y detectar cuando algún evento o acción sobrepasa los umbrales de comportamiento regular (Espinoza Reyes, 2024, p.4).

Este extracto se relaciona con la investigación en curso, ya que es clave para analizar y prever esquemas de atención y resolución de eventos de ciberseguridad, lo cual contribuya en BN Fondos a implementar mejoras prácticas de monitoreo y planes de contingencia ante este tipo de eventos.

Proyecciones

Alcances

La presente investigación se enfoca en el desarrollo de un modelo integral de gestión de incidentes y ciberresiliencia, con el objetivo de mitigar el riesgo de ciberataques y garantizar la continuidad del negocio en BN FONDOS.

El primer alcance implica la identificación y modelado de atención a incidentes cibernéticos, lo que incluye la identificación de amenazas que puedan afectar los servicios de la organización. Para ello, se recopilará y analizará información histórica de pruebas de intrusión, estableciendo un modelo de atención basado en estos datos, lo que permitirá mejorar la capacidad de respuesta y reducir el impacto de futuros incidentes. Este modelo se espera que esté listo para su implementación en un plazo de seis meses, específicamente durante el primer semestre de 2025.

El segundo alcance abarca la evaluación de la infraestructura tecnológica y los sistemas actuales de BN FONDOS, con el propósito de identificar vulnerabilidades. Se documentarán las vulnerabilidades existentes y se desarrollará un plan de mejoras que asegure la confidencialidad, integridad y disponibilidad de la información. Este plan deberá completarse en un periodo de seis meses, también en el primer semestre de 2025.

El tercer alcance se centra en el diseño de un plan de respuesta a incidentes que asegure una pronta recuperación de los servicios. Esto implica analizar y adaptar las mejores prácticas en seguridad para su implementación en BN FONDOS. El diseño debe estar listo para pruebas y validación en un plazo de seis meses del año 2025.

El cuarto alcance propone la implementación de un sistema de monitoreo en tiempo real para detectar eventos y ciberataques. Se evaluarán herramientas tecnológicas que permitan la detección proactiva de incidentes, y el sistema debe estar operativo dentro de un periodo de seis meses.

Finalmente, el quinto alcance contempla la creación de planes de capacitación y evaluaciones periódicas para el personal de BN FONDOS. Esto incluye el desarrollo de evaluaciones de conocimiento y simulaciones de respuesta a ciberataques, asegurando que todo el personal esté capacitado para actuar adecuadamente en caso de un incidente. Las capacitaciones y evaluaciones se realizarán de manera continua, completando un ciclo inicial en un año.

Limitaciones

Dentro del proyecto de investigación se han contemplado las siguientes limitaciones:

En primer lugar, el alcance geográfico y organizacional se limita exclusivamente a los servicios y operaciones de BN FONDOS, excluyendo otras áreas del Banco Nacional de Costa Rica. Esta restricción garantiza que los recursos se concentren en un análisis detallado y específico, asegurando que los resultados sean directamente aplicables a BN FONDOS.

Otra limitación es el acceso a información confidencial, ya que la investigación podría verse restringida por la disponibilidad de datos clasificados de la organización. Cualquier

restricción en el acceso a esta información será documentada y considerada en la interpretación de los datos, trabajando con la información accesible y no confidencial.

Asimismo, el diseño e implementación de la solución no incluirán la compra de nuevos equipos, software o suscripciones necesarias. El proyecto se centrará en utilizar los recursos y herramientas disponibles dentro de BN FONDOS, asegurando que se mantenga dentro del presupuesto.

Por último, no se incluirán en el diseño soluciones que requieran hardware adicional o licenciamiento oficial de uso. El enfoque se limitará a soluciones que puedan implementarse con los recursos tecnológicos existentes en la organización, lo que es fundamental para cumplir con las restricciones de presupuesto del proyecto.

Capitulo II: Marco Teórico

El presente marco teórico proporciona los fundamentos conceptuales y metodológicos que sustentan la investigación sobre la implementación de un modelo de ciberresiliencia y gestión de incidentes en BN FONDOS. Se aborda la importancia de la ciberseguridad en el sector financiero, los enfoques y normativas internacionales, como el NIST CSF, y se exploran conceptos clave como ciberresiliencia, gestión de riesgos y continuidad del negocio.

Este marco establece una base para comprender cómo los componentes teóricos y prácticos de la ciberseguridad pueden integrarse en un entorno bancario, permitiendo a BN FONDOS no solo prevenir y mitigar incidentes, sino también fortalecer su capacidad de respuesta y recuperación en un panorama de amenazas cada vez más complejo y desafiante.

Banco Nacional de Costa Rica

De acuerdo con la página web BNCR (s.f.) El Banco Nacional de Costa Rica se fundó el 9 de octubre de 1914 con el nombre de Banco Internacional de Costa Rica, posteriormente en 1936 pasó a llamarse Banco Nacional de Costa Rica, por lo tanto, en octubre 2024 la entidad bancaria cumple 100 años de proveer al pueblo costarricense un desarrollo y crecimiento en el ámbito financiero. La entidad bancaria pertenece al Estado costarricense, posee 152 oficinas en todo el país, con más de 450 cajeros automáticos y con una afiliación de más 3000 comercios a nivel nacional afiliado a BN Servicios, con una población de 5000 colaboradores.

El objetivo primordial que se detalla en BNCR (s.f.) el Banco Nacional estima ser el Conglomerado Financiero de punta en Costa Rica el cual llegue a fortalecer el desarrollo y bienestar de Costa Rica, basado en el servicio y en proveer una buena experiencia al cliente, con una salud organizacional y robustez financiera sostenible. Como valores claves del Banco

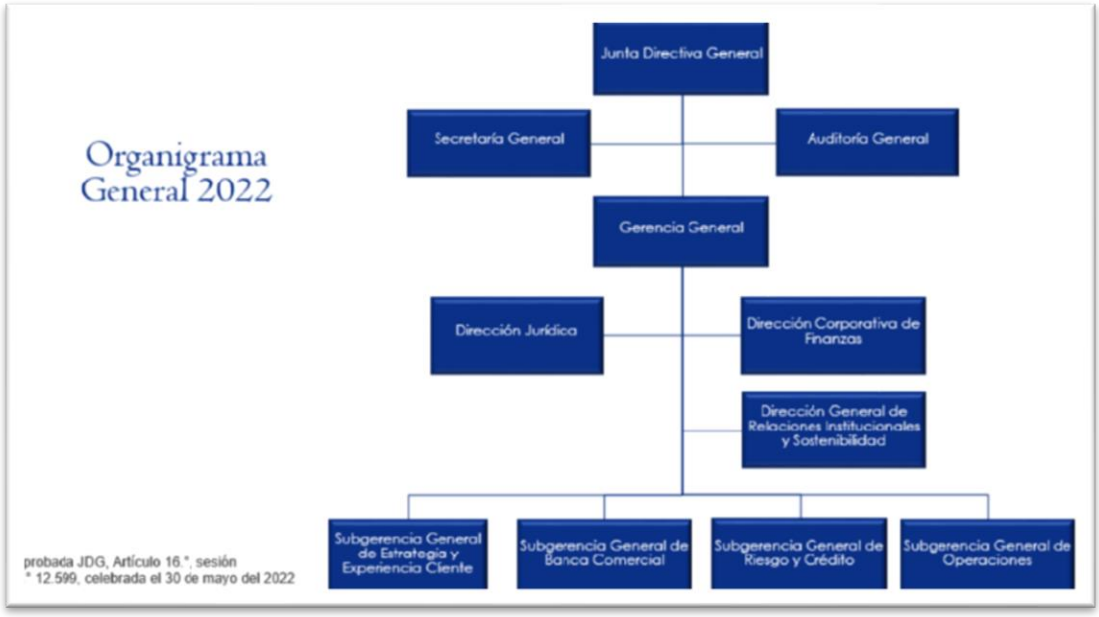
Nacional sobresalen el saber escuchar y resolver de la mejor manera y con empatía las necesidades del ciudadano costarricense, atender con prioridad y disciplina a los clientes, a lo interno se incentiva en trabajar de forma colaborativa y haciendo el trabajo lo mejor posibles para agregar valor al servicio.

En la página BNCR (s.f.) menciona que el Banco Nacional se caracteriza por ser un banco sostenible en la creación de valor socioeconómico y medioambiental a mediano y largo plazo, de esta manera contribuye al crecimiento del bienestar y al progreso del país, logrando una mejor calidad de vida a la mayor cantidad de personas posibles.

El organigrama que se menciona en BNCR (s.f.) lo encabeza la Junta Directiva, esta junta es el máximo órgano rector del Banco Nacional de Costa Rica, las funciones que ejercen son de absoluta independencia y bajo su responsabilidad, siguiendo los lineamientos, normas establecidas por las leyes y reglamentos basados en técnicas bancarias. Esta junta elegida se apoya en dos áreas como lo son la Secretaría General y la Auditoría General, posteriormente se establece la Gerencia General apoyada por la Dirección Jurídica, la Dirección Corporativa de Finanzas y la Dirección General de Relaciones Institucionales y Sostenibilidad, finalmente se definen las Subgerencia General de Estrategia y Experiencia al Cliente, Subgerencia General de Banca Comercial, Subgerencia General de Riesgo y Crédito y la Subgerencia General de Operaciones.

Figura 1

Organigrama BNCR



Nota. Organigrama Banco Nacional de Costa Rica tomado de BNCR (s.f.)

Según BNCR (s.f.) el Conglomerado Financiero del Banco Nacional el cual será mencionado en adelante CFBNCR está formado por la siguientes Sociedades Anónimas:

- BN FONDOS
- BN VALORES
- BN VITAL
- BN CORREDORA DE SEGUROS

El Código de Conducta para el Conglomerado Financiero Banco Nacional en BNCR (s.f.) lo determina como un objetivo claro de definir los principios y conductas que deben guiar la actitud y el comportamiento de los funcionarios del Conglomerado Financiero del Banco

Nacional, el cual, es de acatamiento obligatorio para los integrantes del conglomerado, así como para los proveedores que brindan algún tipo de servicio, aplica también para los miembros de comités de apoyo a las Juntas Directivas y a la administración.

Los valores organizacionales que se mencionan en BNCR (s.f.) se fundamentan en:

- Colaboración
- Escucha
- Innovación
- Negocios sostenibles y responsables

A su vez en BNCR (s.f.) se detallan los servicios de transacciones en forma ágil y segura, los cuales provee por medio de canales digitales que le permitan al cliente final una facilidad en su uso, se destacan:

- Canales digitales y seguridad
- Cuentas y transferencias
- Ahorro e inversión
- Tarjetas de débito y crédito
- Préstamos

Dada la importancia y renombre que tiene el Banco Nacional de Costa Ruca a nivel local e internacional, y relacionando la creciente ola de ciberataques que se dan hoy día en la región, el área de tecnología ha implementado mejoras tecnológicas con herramientas de última generación para proteger las diferentes plataformas que ofrecen los servicios a la institución, agencias bancarias y a las sociedades anónimas; el monitoreo 24 x 7 x 365 es esencial para detectar de manera pronta y eficaz cualquier evento que trate de violentar los sistemas, software, hardware,

etc. que conforman la infraestructura tecnológica. De cara al cliente final y de una manera muy eficaz se han implementado controles de seguridad tales como:

- Firma Digital
- Software Token o Token Celular
- Hardware Token o Token Llavero
- Registro de Dispositivo
- Códigos de Seguridad
- Límites de Transacciones
- Sistemas Biométricos (huella dactilar o reconocimiento facial)
- Tarjeta Virtual
- Alertas Financieras

El Banco Nacional de Costa Rica promueve una campaña preventiva con 5 consejos para evitar caer en las trampas de los ciberdelincuentes:

- Verificación de fuentes de información
- Desconfianza ante algo inusual
- Educación continua
- Protección de datos personales
- Reportar actividades sospechosas en la red

El Banco Nacional de Costa Rica como el ente primordial del Conglomerado Financiero brinda un marco de gobierno de TI con el objetivo de proporcionar los lineamientos y estrategias a las Gerencias de TI de las Subsidiarias con fin cumplir los objetivos del manejo adecuado de los riesgos en materia de tecnología. Se tiene claro que las tecnologías de la información son un

elemento clave para el cumplimiento de las estrategias en los departamentos de TI dentro de un mundo cada vez más digitalizado, por lo tanto, se deben incrementar las acciones en la identificación, análisis, reducción, monitoreo y control de los riesgos asociados al área de TI.

El Conglomerado Financiero del Banco Nacional determina como procedimientos fundamentales el Plan de Recuperación de Desastres (DRP, Disaster Recovery Plan) y el Plan de Continuidad del Negocio (BCP, Business Continuity Plan), planes para la Administración de Disponibilidad y Capacidad de Gestión de Incidentes, pruebas de intrusión, pruebas de continuidad de servicios tecnológicos, planes de parcheo de sistemas operativos, aplicaciones, entre otros.

A su vez, existe un Centro de Operaciones de Seguridad (SOC) que monitorea 24 x 7 x 365 las diferentes plataformas del Conglomerado Financiero del Banco Nacional notificando alertas en tiempo real a los diferentes departamentos de TI de las Sociedades.

Si bien es cierto el Banco Nacional cubre con su sombrilla todas las sociedades anónimas, cada una de las unidades de negocio incluyendo BN FONDOS no están exentas de tomar sus propias medidas para garantizar la ciberseguridad y ciberresiliencia particulares.

Sociedad Administradora de Fondos de Inversión (BN FONDOS)

En los años ochenta, según BNFONDOS (s.f.) Costa Rica contempló un cambio significativo dentro del ámbito financiero con la fundación de una institución destinada a gestionar y administrar fondos de inversión denominada Sociedad Administradora de Fondos de Inversión, BN FONDOS, Sociedad Anónima del Banco Nacional. La historia de este emprendimiento comenzó el 29 de abril de 1988, cuando se registraron ante la Superintendencia General de Valores las primeras inscripciones en posesión del Banco Nacional de Costa Rica.

Este acto fue autorizado por una sesión clave realizada el 17 de diciembre de 1998 bajo el auspicio del Consejo Nacional de Supervisión.

De acuerdo con la página web BNFONDOS (s.f.) BN FONDOS pertenece 100% al Banco Nacional, es regulada por la Ley Reguladora del Mercado de Valores según el artículo 65, que exige que las Sociedades Administradoras de Fondo de Inversión (SAFI) se establezcan bajo un modelo de Sociedad Anónima.

Igualmente, en BNFONDOS (s.f.) se menciona que el objetivo principal de BN FONDOS es prestar servicios eficaces para el manejo de los fondos de inversión que participaran en las actividades regulatorias autorizadas. Dentro del marco estratégico construido por sus fundadores, BN FONDOS se comprometió a alcanzar varios hitos clave:

- Consolidarse como la entidad más influyente en el país en términos de volumen y rentabilidad (FONDOS, no especificado).
- Impulsar un desarrollo sostenido del mercado financiero mediante la gestión innovadora e inmersa en capitales.
- Posicionarse entre los principales interesados como una sociedad líder en fondos de inversión.
- Desarrollar y expandir su red distribuidora, que incluye tanto agencias como sucursales del Banco Nacional de Costa Rica.
- Gestionar fundos especializados, destacando los Fondos Inmobiliarios e Hipotecarios.

La misión según BNFONDOS (s.f.) trasciende la mera gestión financiera; está imbuida en el ideal de mejorar las condiciones socioeconómicas para un mayor número de personas a través de servicios financieros que promuevan una creación y sostenimiento de riqueza. Este compromiso se refleja en todas sus operaciones, buscando no solo obtener rentabilidad sino

también contribuir significativamente al bienestar económico del país. A medida que BN FONDOS creció y adquirió experiencia a lo largo de los años, se convirtió en una presencia indispensable para la economía costarricense. A través de su dedicación continua y adaptación al entorno financiero cambiante, consolidó un rol crucial dentro del tejido económico nacional e internacional. El legado que deja BN FONDOS no solo reside en los fondos gestionados sino también en el impacto positivo sobre la vida de sus clientes y la sociedad costarricense.

En el corazón del Banco Nacional de Costa Rica se encuentra una historia fascinante sobre la evolución y adaptación tecnológica que ha impulsado a BN FONDOS a convertirse en un pilar innovador dentro del sector financiero nacional. Desde su fundación, no solo como administradora de fondos sino también como agente de cambio e innovación, este emprendimiento se ha posicionado al frente de la transformación digital y el crecimiento estratégico impulsando una serie de pioneras iniciativas que han moldeado su imagen en el mercado. La creación del BN FONDOS por el Banco Nacional de Costa Rica en abril de 1998 marcó una pauta para redefinir las operaciones financieras. Se planteó un modelo que permitiera la inversión con montos iniciales mínimos, haciendo posible que incluso aquellas personas con recursos limitados puedan participar en actividades de ahorro y crecimiento patrimonial.

La implementación del Banca en Línea según BNFONDOS (s.f.) representó un hito significativo para democratizar el acceso a los fondos financieros, facilitando operaciones como la asignación de personas beneficiarias con solo ₡5,000 o $20. Este modelo innovador abrió un mundo de posibilidades para que el sector inversionista costarricense disfrutara de una mayor inclusión y diversificación. La normativa de la Ley 8204 se fundamenta en establecer los requisitos mínimos para evitar y prevenir operaciones ocultas y la movilización de capitales de procedencia dudosa, legitimar capitales o financiar actividades u organizaciones terroristas. En

este caso BN FONDOS es fiscalizado por la Superintendencia General de Entidades Financieras (SUGEF), la Superintendencia de Pensiones (SUPEN), Superintendencia General de Valores (SUGEVAL y la Superintendencia General de Seguros (SUGESE). Dados estos lineamientos BN FONDOS se ve en el compromiso con la gestión integral del riesgo cibernético que se convierte en otro punto central a fines del siglo XXI, dada las amenazas constantes emergentes que podrían desestabilizar operaciones financieras críticas como las de BN FONDOS.

Antes de mencionar los diferentes productos que se muestran en BNFONDOS (s.f.), primero aclaramos que un fondo de inversión es una alternativa financiera que permite a las personas reunir recursos para acceder a posibilidades de inversión; lo cual le permite ahorrar o invertir dinero en dos diferentes modalidades, fondo a la vista, el cual le permitirá al ahorrante tener el dinero cuando lo requiera; y a plazo con inversiones diferentes de 6 meses a 1 año. Las principales características y diferencias se muestran a continuación:

Figura 2

Clasificación de Fondos de Inversión

Fondos a la Vista	Fondos a Plazo
Permite gestionar inversiones y retiros en cualquier momento	Permite realizar inversiones en cualquier momento, pero solo se puede hacer retiros durante la fecha de vencimiento.
Retiro sin cobro de comisión.	En caso de solicitar un retiro anticipado se debe pagar una comisión.
Período de liquidación t+1	Período de liquidación t+5

Nota. Tipos de fondos de inversión de BN FONDOS tomado de BNFONDOS (s.f.)

Teniendo claridad con la clasificación de los fondos de inversión los principales productos y servicios que ofrece BN Fondos del Banco Nacional y se detallan en BNFONDOS (s.f.) están los siguientes:

- Fondos de Mercado de dinero a la vista: se clasifican en cuatro tipos de fondos, a saber, BN DinerFondo, BN FonDepósito, BN SuperFondo y BN SuperFondo dólares Plus.
- Fondos de Crecimiento (largo y mediano plazo): lo conforman el BN RediFondo y el BN CreciFondo.
- Fondos Internacionales: está determinado por el BN Internacional Liquidez, BN Internacional Valor, BN Internacional Suma y BN Internacional Crece.
- Fondos No Financieros: lo conforman BN Fondo de Inversión de Desarrollo de Proyectos de Infraestructura Pública, BN Fondo de Inversión de Desarrollo de Proyectos y BN Vivienda.

La referencia de BNFONDOS (s.f.) menciona que la estructura organizacional de BN FONDOS es independiente a la del Banco Nacional de Costa Rica, su Junta Directiva encabeza la estructura seguido de dos áreas de control como lo son la Auditoría Interna y un Comité de Inversiones. Bajo la Gerencia General se encuentras las áreas de Gestión de Riesgo y Calidad, Gestión de Proyectos, Gestión de Portafolios y Personas y Cultura; las Sub-Gerencias que apoyan la Gerencia General son Gerencia Administrativa-Financiera, Gerencia de Sistemas y Tecnología, Gerencia Comercial, Gerencia de Operaciones y la Gerencia de Fondos Inmobiliarios e Hipotecarios.

Figura 3

Organigrama BN FONDOS

Nota. Organigrama de BN FONDOS tomado de BNFONDOS (s.f.)

BN FONDOS se ha certificado en normas internacionales las cuales le brindan solidez y transparencia en los servicios que brinda, las certificaciones que han impulsado a BN FONDOS a mantenerse como una Sociedad Anónima líder en Costa Rica son:

- Norma ISO 9001:2015 Sistema de Gestión de la Calidad, la cual permite a BN FONDOS estandarizar su operativa de forma integral, lo cual le permite brindar satisfacción al usuario final, mantiene una mejora continua en los procesos internos y brinda un buen tratamiento a los riesgo y oportunidades.
- Norma INTE G:38 Sistema de Gestión para la Igualdad de Género (SIGIG): su principal objetivo es establecer una organización basada en el respeto, tolerancia y

empatía hacia todas las personas desde su diversidad, evitando la discriminación, violencia, acoso laboral y el hostigamiento sexual.

- ISO 27001: Su principal objetivo es establecer los lineamientos para fortalecer la seguridad de la información.

Adicionalmente BN FONDOS ha establecido una Política de Gestión Empresarial con sus tres objetivos primordiales como lo son la integridad, responsabilidad y honestidad, lo cual cumple con el acatamiento de los lineamientos del Conglomerado Banco Nacional de Costa Rica, impulsa la cultura organizacional basada en el respeto, la tolerancia y la empatía a todas la personas, gestiona la capacidad de resiliencia organizacional, mantiene un enfoque al cliente céntrico, humano, cercano y sostenible, establece controles para la confidencialidad, la integridad y la disponibilidad de la información de sus operaciones, del cliente, patrimonio y del personal.

Cabe destacar que BN FONDOS no solo ha evolucionado con su enfoque proactivo hacia la ciberseguridad sino también subraya el compromiso que esta entidad tiene para ajustarse constantemente y responder al panorama de amenazas tecnológicas cambiante. Con un modelo integral enfocado en prevención, respuesta eficaz y recuperación después del incidente cibernético, BN FONDOS se posicionará como líder en proteger la continuidad de sus operaciones financieras del Banco Nacional y de sus clientes.

Tecnología y Sistemas de Información en BN FONDOS

La Gerencia de Sistemas y Tecnología de BN FONDOS establece la gestión de los servicios tecnológicos con el objetivo de proveer y administrar los servicios tecnológicos que el negocio amerita y se puedan alcanzar los objetivos establecidos al gobierno de TI. Que a su vez

determina procesos para la planificación, el control, el diseño de soluciones tecnológicas, asegura la entrega de servicios tecnológicos para brindar la continuidad de los servicios del negocio y monitorea y evalúa estos servicios para garantizar el nivel de servicio ideal tanto al usuario interno como externo de BN FONDOS. A su vez, el área de tecnología se fundamenta en marco integral con una infraestructura tecnológica que permita soportar los diferentes servicios tecnológicos y que garantizan la operativa del negocio de una manera confiable.

Con el fin de mantener una operativa continua y estable, el área de tecnología establece políticas y procedimientos para el monitoreo de la plataforma tecnológica sobre los equipos en el ambiente de producción, el cual se realiza de forma automática y constante, garantizando acciones proactivas y prontas en caso de eventos o alertas del hardware, aplicaciones y servicios.

Igualmente, por herramientas de ciberseguridad de última generación y herramientas de antivirus, servicio que ofrece el Banco Nacional de Costa Rica, la plataforma tecnológica de BN FONDOS se encuentra blindada ante correos sospechosos o ciberataques, estas de manera automática detectan y eliminan los virus informáticos que se puedan presentar en cualquier momento; otras medidas preventivas son las pruebas de intrusión internas, y pruebas de intrusión externas, las cuales por agendas periódicas establecidas pretenden descubrir vulnerabilidades en la red, sus resultados son analizados y se determinar planes de atención ante los hallazgos detectados.

La atención de una mesa de ayuda es primordial para el registro, atención, documentación y seguimiento de solicitudes de servicios, atención de incidentes, gestión de cambios entre otros, lo que garantiza la correcta y adecuada continuidad de los servicios del core de negocio de BN FONDOS.

Ciberseguridad

Hoy en día surge una serie de interrogantes acerca de la palabra ciberseguridad, la cual se determina para asociarla a los ataques que sufren las empresas en general a nivel mundial por medio del internet; las empresas proveedoras que ofrecen productos tecnológicos para combatir los ataques informáticos la determinan de varias formas, por ejemplo el fabricante AWS (2023) la menciona como la práctica para proteger equipos, redes, aplicaciones de software, sistemas críticos con el fin de mantener de una forma integral los datos de los clientes y así cumplir con las normativas de protección de los datos.

Para IBM (2023) la ciberseguridad tiene como objetivo protege los sistemas, aplicaciones, dispositivos, incluye los datos confidenciales y activos de una organización, todos estos elementos y otros son protegidos de virus informáticos y ataques ransomware.

A nivel del marco NIST, IBM (2023) la detalla como las mejores prácticas que pueden llegar a proteger los sistemas más importantes y la información confidencial ante la creciente amenazas y su constante evolución.

Según IBM (2023), la estrategia de la ciberseguridad conlleva la protección de:

- Seguridad de la infraestructura crítica
- Seguridad de la red
- Seguridad de punto final
- Seguridad de aplicaciones
- Seguridad en la nube
- Seguridad de la información
- Seguridad móvil

A nivel mundial las entidades financieras son un punto clave de ciberataques, según FED Finance (2024), la información que se gestiona en el ámbito financiero es esencial para impulsar la economía de un país, por lo tanto, cualquier vulnerabilidad de seguridad puede tener consecuencias graves, pérdida de confianza de los clientes y afectación en su estabilidad financiera. Dado lo anterior los ciberdelincuentes tratan de perpetrar las entidades bancarias aprovechando las transacciones financieras que se realizan en las diferentes plataformas en tiempo real; igualmente las instituciones financieras deben estar atentas al desafío de salvaguardar la integridad y la privacidad de los información de sus clientes; por esta circunstancia es fundamental e importante la ciberseguridad en el sector financiero implementando tecnologías claves para mitigar los riesgos y fortalecer las defensas tecnológicas así lograrán mantener la imagen corporativa.

Los ciberdelincuentes realizan amenazas según la fuente de ataque, en el caso del sector financiero por su abundancia de datos valiosos y sensibles los ataques son muy frecuentes, FED Finance (2024) clasifica principales amenazas en el sector financiero de la siguiente manera:

- Ransomware
- Phishing
- Malware
- Ausencia de actualizaciones de seguridad
- Ataques de denegación de servicios (DDos)

Gestión de Incidentes

De acuerdo con las diferentes normativas internacionales podemos encontrar diferentes definiciones, según Moreno García (2022) la normativa ISO 27001 determina un incidente de

seguridad de la información como un evento o serie de eventos no deseados o inesperados que tienen una alta probabilidad de afectar o comprometer las operaciones y servicios de una empresa. Otra referencia al respeto la obtenemos de Moreno García (2022), INCIBE la detalla como cualquier suceso que llegue a afectar la confidencialidad, la integridad o disponibilidad de los activos de información que contienen una empresa.

Los incidentes deben ser atendidos de una manera secuencial y organizada, por esta razón los organismos internacionales han determinado un ciclo de vida de un incidente determinando cinco (5) fases, Moreno García (2022) explica que de acuerdo con la norma ISO/IEC 27035 Gestión de Incidentes de Seguridad el ciclo de vida de un incidente lo clasifica en:

- Planificación y preparación: esta fase es esencial para la preparación de la organización en la definición de acciones que se deben establecer para atender un incidente de seguridad. Para fortalecer esta fase la organización debe definir el plan de gestión de incidentes, las políticas de seguridad de la información, establecer el equipo de respuesta a incidentes de seguridad, concienciación al personal sobre la gestión de incidentes, realizar simulacros del plan de gestión de incidentes, definir la clasificación de incidentes de seguridad que puedan afectar a la organización.
- Detección y reportes: esta fase es clave para la recopilación de información (interna y externa), identifica el incidente presentado, ya identificado el incidente se registra y notifica el incidente al momento de confirmarse.
- Valoración y decisión: si en la fase anterior ha sido confirmado el incidente de seguridad, en esta fase, se determina la clasificación del incidente se seguridad y

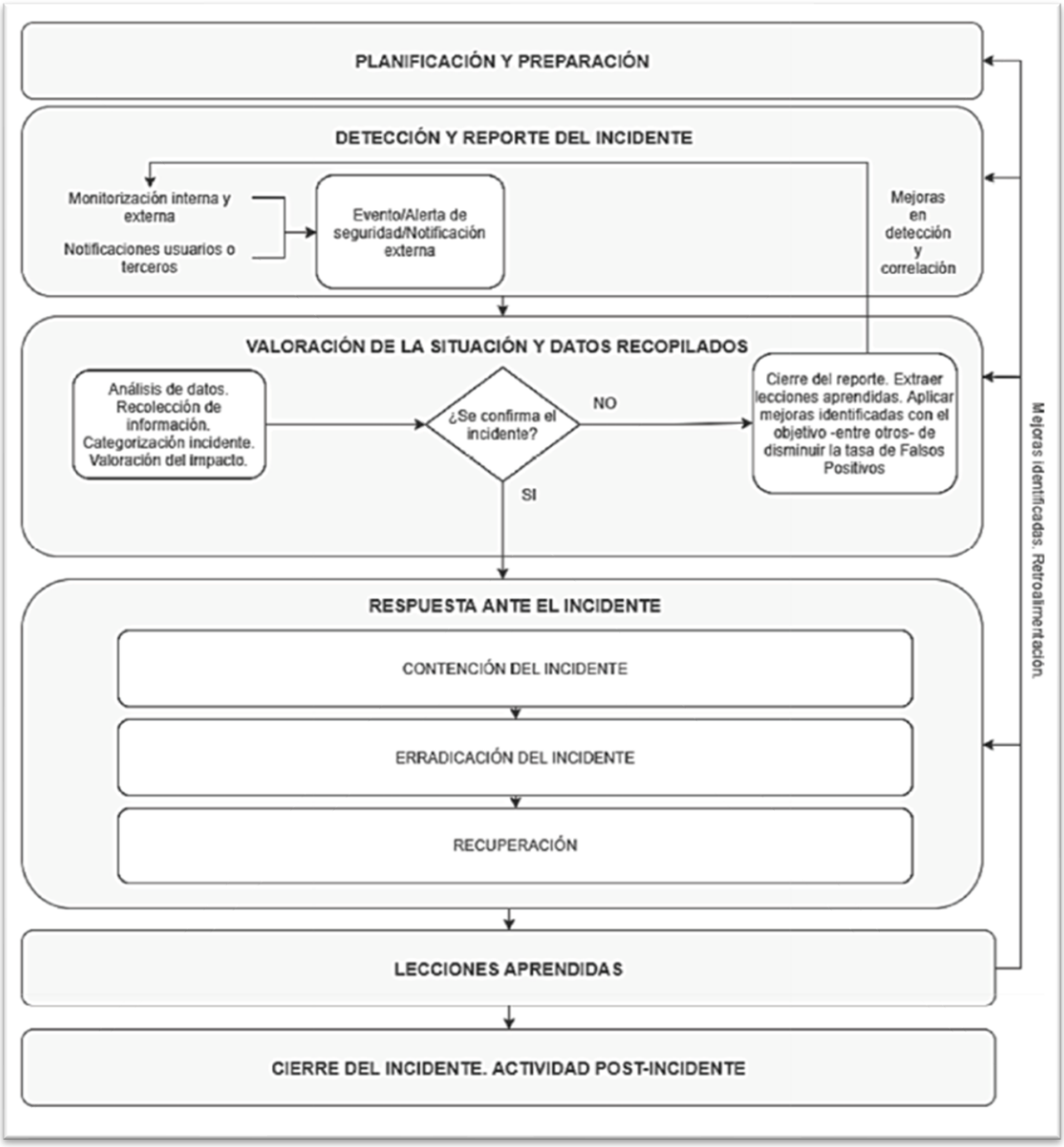
se debe indicar el impacto que está ocasionando o podría ocasionar en la organización.

- Respuesta: en este paso se continúa con el análisis de evidencias del incidente de seguridad para ampliar la información del evento lo que lleva a la toma de decisiones adecuadas, ideales y ágiles con el fin de que el impacto sea lo menos posible, en esta fase se trabaja la contención del incidente, la erradicación del incidente y la recuperación pasado el incidente.
- Lecciones aprendidas: esta etapa es ideal para realizar un análisis post incidente de seguridad para mejorar el ciclo de vida de la gestión de incidentes ya que ayuda a identificar que fases se encuentran con alguna debilidad en su gestión, esto contribuye a identificar las mejoras de los planes, las políticas, procedimientos definidos actualmente; también evalúa la efectividad, agilidad y desempeño del equipo de respuesta de incidentes, finalmente debe identificar las mejoras del monitoreo y recopilación de la información.
- Cierre del incidente: este alcance se desea agregar a las 5 fases ya establecidas, la cual establece que el incidente no se dará por finalizado hasta tener identificadas las lecciones aprendidas y exista un plan de atención.

Un diagrama que ejemplifica las fases anteriores es el siguiente:

Figura 4

Ciclo de Vida de un Incidente



Nota. Ciclo de Vida de un Incidente tomado de Moreno García (2022)

La gestión de incidentes tiene el objetivo de minimizar de una manera pronta y efectiva cualquier evento o amenaza que puede penetrar los medios de seguridad de una empresa, dado esto, se debe tener claridad de cuáles son los diferentes tipos de incidentes que presentan a nivel mundial. Según la Universidad de Costa Rica (2022) menciona los siguientes tipos de incidentes de seguridad:

- Infecciones por código malicioso: este tipo de infección se da por medio del correo electrónico, por páginas web maliciosas, redes sociales.
- Intrusiones o intentos de intrusión: este tipo de afectación se por la explotación de vulnerabilidades, ataques exploits y vulnerabilidades de credenciales, la afectación principal se puede presentar en las cuentas con o sin privilegios.
- Fallos de disponibilidad: se produce por medio de ataques tipo DoS (denegación de servicio) lo que con lleva la afectación de diferentes recursos de la organización como lo son los equipos de redes, la plataforma de infraestructura, equipos de usuario final.
- Compromiso de la información: ataques tipo ransomware que produce el captura, robo o secuestro de los datos de una organización.
- Fraude: esta se penetra por medio de la suplantación de entidad legítima, engañando a las personas de equipos finales para obtener un beneficio económico.

Ciberresiliencia

Una manera de atender y repeler los ciberataques es por medio de la implementación de acciones de ciberresiliencia con el objetivo establecer planes de contingencia para brindar la continuidad del negocio de las empresas, según Carrasco (2015) la ciberresiliencia llega a ser

una cualidad de una organización que le brinde atributos o cualidades para enfrentar una crisis sin que su continuidad del negocio se vea impactada.

IBM (2023) detalla la ciberresiliencia como la capacidad de seguir brindando los servicios de la empresa a pesar de haber experimentado eventos cibernéticos, o bien desastres naturales o ataque económicos; de tal manera la empresa pueda llegar optimizar el valor, el servicio y la credibilidad ante los clientes.

Aspectos claves de la ciberresiliencia según IBM (2023) implica la gobernanza, la gestión de riesgos, la gestión y propiedad de los datos, muy acertadamente la gestión de incidentes.

De acuerdo con las definiciones de ciberseguridad y ciberresiliencia, se puede indicar que se diferencian a dos acciones diferentes: la ciberseguridad habla de la capacidad de prevenir ciberataques y la ciberresiliencia menciona la capacidad de recuperarse en caso de que se produzcan eventos o ciberataques.

Actualmente se entiende que los resultados efectivos de una ciberresiliencia bien implementada y alineada a una buena estrategia de una organización, y según S2 Grupo (2023) produce los siguientes beneficios en la continuidad del negocio:

- Se disminuye la posibilidad de que se presenten ciberataques.
- Se pueden minimizar los impactos de un ciberataque.
- La organización puede experimentar una rápida recuperación de sus servicios.
- La organización se protege ante pérdidas financieras.
- La organización protege su reputación
- Se da un fortalecimiento en el departamento de tecnología.

Según S2 Grupo (2023), una organización preparada estratégicamente con un plan de ciberresiliencia puede llegar a:

- Tener buenas prácticas y políticas de ciberseguridad
- La organización tendrá planes de acción bien establecidas ante situaciones de riesgo.
- La organización tendrá personal capacitado y aún más comprometido en los aspectos de ciberseguridad.
- La organización implementará sistemas de monitoreo en tiempo real para identificar con antelación potenciales riesgos.

Amenazas Cibernéticas

Las diferentes organizaciones deben prepararse para enfrentar a una serie de amenazas cibernéticas, las cuales día a día se actualizan, a continuación, según Arroyo Guardeño (2020) se citan las principales amenazas cibernéticas:

- Malware: se asocia a todo tipo de software malicioso cuyo fin es infectar los equipos del área de tecnología, tales como servidores; del malware se derivan otra serie de amenazas que se emplean para extraer información personal, filtrar contraseñas, robar dinero, etc.
- Phishing: son programas que sustituyen las direcciones de páginas web legítimas con otras similares, pero estas son gestionadas por los ciberdelincuentes, lo cual conlleva a que los usuarios finales introduzcan sus accesos (usuario y contraseña) creyendo que están en la página deseada. A partir de este paso se produce el suplanto de identidad por ejemplo de tipo bancaria.

- Ransomware: esta amenaza constituye el cifrado de datos o información de clientes de una organización, los ciberdelincuentes proceden con el secuestro de los datos, liberándolo solo por medio de pago a cambio de la información secuestrada.
- Spyware: software que recopila y envía información confidencial de una persona, en especial los ciberdelincuentes buscan datos personales que en un momento determinado puedan emplear.
- Adware: tipo de amenaza que se basa en la creación de anuncios publicitarios falsos o engañosos.

Las entidades financieras a nivel mundial son un blanco para los ciberdelincuentes que cada día desarrollan nuevas técnicas para atacar este sector, según Jesús Raya (2023) los tipos más utilizados en ciberataques específicamente en el sector financiero son:

- Phishing o ingeniería social
- Malware
- Ransomware
- Ataques a la infraestructura
- Manipulación del mercado

Los impactos en las entidades que son afectadas por ciberataques son muy delicados en su reputación, imagen y credibilidad por parte de sus clientes, Jesús Raya (2023) detalla los puntos clave de las consecuencias, tales como:

- Pérdidas financieras: este efecto puede producir pérdidas millonarias, retiro de clientes y una recuperación muy sensible.

- Pérdida de confianza: la confianza en vital para tener credibilidad en una entidad, este impacto puede conllevar el retiro de clientes e incluso de socios.
- Riesgo sistemático: este riesgo puede afectar todo el sistema de una organización.
- Pérdida de datos personales: una de las principales amenazas es el robo o secuestro de los datos.
- Reputación dañada: si una organización se ve afectada por amenazas de las antes expuestas es claro que sufrirá la imagen y reputación lo que puede llevarla a la pérdida de clientes y oportunidades de negocio.

Evaluación de Vulnerabilidades

Otro aspecto para tomar en consideración para las prevenciones de ciberataques es tener claridad que vulnerabilidades o debilidades informáticas puedes tener una organización en su plataforma tecnológica, según Limones (2023) una vulnerabilidad informática llega a ser una debilidad un código de sistema o de un dispositivo de la infraestructura tecnológica de una organización que cuando se materialice puede llegar a comprometer o poner en riesgo la información de cliente de la empresa. Normalmente la vulnerabilidad se da por un fallo en el diseño, en la programación, la configuración o error humano que deja el camino abierto a los ciberdelincuentes para llegar a obtener información confidencial.

Una de las recomendaciones de valor agregado para las organizaciones es realizar pruebas de penetración a la plataforma tecnológica, según IBM (2023) detalla que estas pruebas se realizan por especialistas o profesionales en técnicas de hackeo ético, emplean diferentes tipos de herramientas (software) para detectar debilidades ya sea en software o hardware, estos

expertos actúan de manera confidencial y silenciosamente para validar que tan fuerte está preparada una organización ante un ciberataque.

Según IBM (2023), las pruebas previamente calendarizadas simularán un ataque contra los sistemas informáticos de la empresa; algunos tipos de pruebas de penetración son:

- Pentests de aplicaciones: permite buscas debilidades en las aplicaciones, sitios web entre otros.
- Pentests de red: esta fundamenta ya sea en una prueba interna y prueba externa; la primera consiste en simular o imitar comportamientos internos en la empresa, el objetivo es detectar vulnerabilidades dentro de la organización. La prueba externa se enfoca en detectar debilidades ingresando a la empresa por medio del internet, para llegar a descubrir vulnerabilidades en dispositivos como servidores, enrutadores, sitios web, entre otros.
- Pentests de hardware: esta prueba de vulnerabilidad se enfoca en detectar fallas de equipos conectados a la red de datos, tales como equipos de usuario final, incluso dispositivos móviles.
- Pentests de personal: esta prueba es fundamental ya que trata de la búsqueda de debilidades con los empleados, normalmente se simulación ataques tipo phishing con el objetivo de engañar a los empleados y así acceder a información confidencial.

Infraestructura Tecnológica en Seguridad de la Información

La tecnología a nivel mundial se optimiza cada vez más, los fabricantes de soluciones, ya sea en hardware o software, ofrecen tecnologías que mejoran, optimizan y aseguran las

comunicaciones con el fin de brindar una mejor eficiencia y desempeño de los servicios al cliente final. Según IBM (2023) una infraestructura de TI debe ser flexible, confiable y segura, si cumple estos puntos brindara a la organización la oportunidad de cumplir sus objetivos del negocio. Igualmente, una infraestructura de TI debe llegar a:

- Mejorar la experiencia al cliente
- Desarrollar y comercializar las soluciones
- Recopilación y análisis de datos para la toma de decisiones
- Mejora la productividad de los empleados

El punto anterior mencionado será efectivo si el diseño de la infraestructura está compuesto por componentes tecnológicos de última generación; la infraestructura tecnológica según IBM (2023) se define por dos elementos claves como lo son el hardware y el software. El hardware puede estar constituido por:

- Computadoras de mesa
- Computadoras portátiles
- Servidores físicos
- Servidores virtuales
- Switch
- Routers

A su vez el software puede estar estructura por software adquirido o bien desarrollado en la misma empresa, normalmente lo conforman aplicaciones tales como:

- Sistemas de gestión de contenido (CMS)
- Gestión de relaciones con el cliente (CRM)

- Planificación de recursos empresariales (ERP)
- Servidores WEB

Los centros de datos son otro punto fundamental, un centro de datos bien acondicionado dará hospedaje ideal para la plataforma tecnológica, así su red LAN, WAN, SAN, vSAN, etc. funcionarán de la mejor manera.

Estrategias de Prevención en Ciberseguridad

La creciente cantidad de incidentes y ciberataques relacionados con la información y sistemas informáticos que sufren las organizaciones actualmente conlleva la necesidad de implementar controles para la protección de la infraestructura tecnológica y los datos para garantizar al usuario final la credibilidad de sus servicios. A nivel mundial, han surgido normativas o estándares que brindan una serie de alcances con el objetivo de que las empresas sigan las mejores prácticas establecidas para la protección de la información y así garantizarán la confidencialidad, integridad, disponibilidad y autenticidad de los datos quedando protegidos ante cualquier tipo de ciberataque.

La implementación de medidas eficaces de ciberseguridad no es algo sencillo debido a la gran variedad de tecnologías (hardware y software) utilizadas, los ciberdelincuentes se actualizan en sus técnicas para penetrar las redes institucionales para llevar a cabo sus ataques. Por esta razón, surgen estándares y normas ISO relacionadas con la ciberseguridad y seguridad de la información.

- Norma ISO 27000: la norma ISO 27000 es una familia compuesta por varias normas de seguridad de la información que determina una serie de requisitos para implementar un Sistema de Gestión de Seguridad del Información (SGI).

- Norma ISO 27001: normativa internacional que ayuda a las organizaciones a establecer las políticas y objetivos para la gestión de la seguridad de la información.
- Norma ISO 27002: normativa internacional que ayuda a las organizaciones en la implementación de controles de seguridad adecuados según los riesgos a que se puedan enfrentar.
- Estándares NIST: agencia no reguladora que promueve normas, pautas y mejores prácticas que ayudan y benefician a las organizaciones a optimizar las gestiones del riesgo de ciberseguridad.

Estrategias de Respuesta a Incidentes

Las organizaciones deben establecer una metodología para la atención de incidentes dependiendo de los efectos o impactos que puedan presentarse con el objetivo de madurar los procesos y procedimientos definidos a lo interno de la organización, según Tejana (2015) la estrategia de respuesta a incidentes en una organización puede iniciar tomando las siguientes acciones:

- Medidas preventivas: las acciones que se determinan y aplican para prevenir y evitar incidentes de seguridad.
- Medidas de detección: son las acciones que se determinan para monitorear, detectar y alertar posibles incidentes de seguridad.
- Medidas correctivas: posterior a un incidente de las organizaciones están en el deber de analizar que debilidades se presentaron con el incidente de seguridad y

establece mejoras correctivas que sirvan para evitar que no se presente nuevos eventos de seguridad.

Acciones como las anteriores permitirán a la organización tener beneficios en la rápida y eficiente respuesta ante incidentes de seguridad.

El propósito de implementar un plan de respuesta a incidentes beneficiará a las empresas para estar preparadas de antemano para contrarrestar posibles amenazas de ciberataques y poder tener una pronta recuperación de los servicios del negocio. Gómez (2024) determina que para poder establecer un plan de respuesta a incidentes es necesario asignar un equipo de trabajo capaz de trabajar en forma coordinada y organizada para atender oportunamente un incidente de seguridad. Gómez (2024) amplía el concepto de un plan de respuesta a incidentes o IRP (Incident Response Plan) como un documento que define detalladamente los pasos a seguir de una forma eficiente y oportuna de atender el incidente desde su detección hasta su resolución.

El documento definido debe contener los mínimos siguientes alcances:

- Definir que ataques o amenazas son para la organización clasificados como incidentes de seguridad.
- Indicar cual es la persona responsable para la atención en primera línea del incidente de seguridad y como contactar a los demás miembros del equipo.
- Definir en qué condiciones los miembros del equipo deben atender las tareas correspondientes.
- Como los miembros del equipo efectúan las tareas clasificadas y asignadas.

La capacidad de atención a los incidentes de ciberseguridad debe ser atendida por equipos de trabajo debidamente preparados y capacitados para atender de manera oportuna y

eficaz un incidente de ciberseguridad, Moreno García (2022) determina la siguiente clasificación de equipos de trabajo:

- CIRT (Computer Incident Response Team), Equipo de Respuesta a Incidentes Informáticos.
- CIRC (Computer Incident Response Team), Equipo de Respuesta a Incidentes.
- SERT (Security Emergency Response Team), Equipo de Respuesta a Emergencias de Seguridad.
- CERT (Computer Emergency Response Team), Equipo de Respuesta a Emergencias Informáticas o CSIRT (Computer Security Incident Response Team), Equipo de Respuesta a Incidentes de Seguridad Informática.

Específicamente los términos CERT o CSIRT se refieren directamente a la respuesta de incidentes de seguridad; ambos se refieren se concentran en grupos de trabajo centralizados para la atención incidentes de seguridad. Moreno García (2022) amplía la funcionabilidad de estos términos mencionando que el CSIRT complementa el alcance del CERT ya que ofrece de complemento los servicios preventivos y de gestión de seguridad siendo el CSIRT una evolución del CERT.

Las organizaciones deben de establecer los procedimientos a seguir en caso de presentarse un incidente de seguridad lo cual ayude a prevenir y reducir los impactos que puedan darse en la organización, según Moreno García (2022) los procedimientos deben cubrir puntos clave como lo son:

- Declaración de compromiso de la gestión.
- Propósito y objetivos del procedimiento.
- Definir los alcances del procedimiento.

- Definir, según la organización, que se puede considerar como un incidente de seguridad.
- Definir la clasificación de un incidente de seguridad.
- Cómo se evalúa un incidente de seguridad.
- Definir el equipo de respuesta ante incidentes con sus respectivos roles, responsabilidades y niveles de autoridad.

Las organizaciones deben estar preparadas con un esquema de notificación de incidentes, la finalidad de la documentación, notificación inmediata y adecuada evitará y mejorará los procedimientos vigentes lo cual ayudará a evitar y minimizar los impactos de un incidente de seguridad, reducirá la filtración de información falsa o incompleta. Las notificaciones deben ir dirigidas a lo interno de la organización (empleados), a proveedores, clientes, otras organizaciones.

Según Moreno García (2022) la notificación debe contener una serie de datos básicos y mínimos que muestren de la forma más precisa el incidente de seguridad, debe mostrar:

- Debe ofrecer un discurso unificado, por un único canal oficial de comunicación.
- Nunca se debe mentir, debe ser un comunicado transparente.
- El asunto debe tener una breve descripción del incidente de seguridad.
- Descripción detallada del incidente de seguridad.
- Fecha y hora del incidente de seguridad.
- Detallar los recursos y servicios tecnológicos afectados.
- Indicar la causa del incidente de seguridad.
- Estimado del impacto del incidente de seguridad.

Estrategias de Recuperación ante Ciberataques

Ya atendida y erradicada la amenaza presentada, la organización debe concentrarse en volver a la operativa normal de las áreas de negocio, según Moreno García (2022) la organización debe trabajar y apoyar el equipo de continuidad del negocio, basando en el Plan de Recuperación de Desastres y el Plan de Continuidad del Negocio. Este paso debe ser gradual, bien planificado, monitoreando el restablecimiento de las operaciones de la organización. Algunas medidas que se deben tener en consideración para la recuperación son:

- Restauración de datos por medio de respaldos (backups) de los sistemas afectados y desinfectados.
- Validación de que las copias estén libres de amenazas.
- Habilitación de servicios y usuarios.
- Reinstalación de sistemas comprometidos.

La recuperación ante desastres la entendemos como la acción y la capacidad de una organización para responder y recuperarse ante eventos o incidentes de ciberseguridad que afectó directamente las plataformas tecnológicas, así pues, las organizaciones deben tener planes de recuperación, a continuación, se analizarán dos esquemas de planes de recuperación:

- Disaster Recovery Plan (DRP): en plan de recuperación de desastres según Nutanix (2024) es una estrategia de seguridad de primera línea, su objetivo es brindar protección a un centro de datos (TI) ya sea de un desastre natural o artificial. El DRP establecido permitirá que una organización puede reanudar o continuar lo antes posible sus operaciones y servicios.

  Establecer un DRP asegura la oportuna continuidad del negocio lo que permitirá cumplir con las métricas de acuerdo de nivel de servicios (SLA), cumplirá el

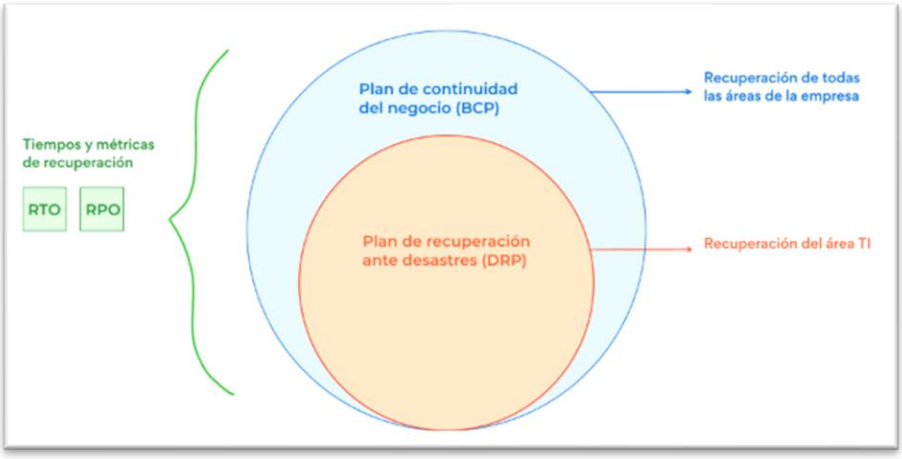
tiempo de recuperación (RTO: tiempo que puede tolerar una empresa ante el paro de sus servicios) y el punto de recuperación (RPO: volumen de datos en riesgo de pérdida que la organización tolere)

- Continuidad del Negocio (BCP): según Araujo (2021) un plan de Continuidad del Negocio es un documento que describe los procedimientos que ha establecido una organización para reanudar la operación normal (de toda la organización) después de una interrupción ante un ciberataque. Los beneficios que provee un BCP es prevenir y minimizar las pérdidas en caso de un desastre, brinda visibilidad de los riesgos identificados que podrían impactar el negocio, puede estimarlas pérdidas por no brindar los servicios normales de la organización.

El DRP es muy similar al BCP, la diferencia radica en que el DRP se enfoca en las actividades de TI, y el BCP se concentra en todas las áreas de la organización.

Figura 5

Recuperación ante Ciberataques



Nota. Esquema de Recuperación ante Ciberataques, RTO y RPO, tomado de Araujo (2021)

- Métricas de recuperación (RTO y RPO): estas son métricas que permitirán determinar el rendimiento de recuperación (RTO) y el segundo se enfocará en establecer que el menor tiempo posible para que la pérdida del negocio sea lo más baja posible.
- Recovery Time Objective (RTO): es el tiempo que una organización necesita para normalizar todos los sistemas después de un incidente de seguridad.
- Recovery Point Objective (RPO): es el tiempo máximo tolerable que una empresa puede permitir desde que se realizó la última copia de seguridad de los datos.

Figura 6

Métricas RTO y RPO

Nota. Diagrama de Métricas RTO y RPO, tomado de Araujo (2021)

Moreno García (2022) detalla el siguiente ejemplo de ciberataque:

- Compromiso por malware: este tipo de ciberataque es uno de los más recurrentes en las organizaciones, según Moreno García (2022) se deben tomar las siguientes acciones:
- Planificación: los departamentos de tecnología deben estar preparados para la detección y atención de este tipo de incidentes con herramientas técnicas como antivirus o antimalware, soluciones que brinden protección ante códigos dañinos; igualmente herramientas con tecnología de punta que puedan censar malware avanzado.
- Detección del incidente y valoración: la organización debe estar preparadas con sistemas de monitoreo y notificaciones en tiempo real, adicionalmente se debe identificar el tipo de malware para aplicar la estrategia de atención y etapas posteriores al incidente.
- Respuesta: Una vez que se tiene claridad del malware que fue censado y se declare como un incidente real, se debe poner en marcha el plan de respuesta para contener y eliminar la infección previniendo que se propague al resto de la organización. Acciones como el bloqueo de las comunicaciones entrantes y salientes, filtrado de correos electrónicos, bloqueo o desconexión de servicios, aislamiento de equipos de red, servidores son acciones que se deben tomar en consideración para aislar el malware detectado. Posteriormente sigue la etapa de la erradicación del malware, pueden emplearse herramientas de antivirus o antimalware. Ya erradicado el malware sigue la etapa de restauración de los sistemas completos de una forma controlada y en orden para volver a la normalidad los servicios de la organización.

- Lecciones aprendidas: un incidente de seguridad no se cierra o se da por atendido hasta haber realizado un análisis que permita identificar las causas de la infección; de igual forma se debe analizar cómo fue la reacción y atención del equipo de atención de incidentes de seguridad.

Monitoreo y Detección Temprana de Amenazas

Dada la importancia y el crecimiento de las amenazas cibernéticas las organizaciones se ven la necesidad de mejora, optimizar y fortalecer las plataformas de monitoreo continuo con el objetivo de detectar con tiempo y minimizar los efectos de una amenaza de este tipo.

Según Vargas (2023) define el monitoreo de seguridad como un proceso continuo con el objetivo de detectar y responder proactivamente una amenaza de ciberseguridad, el monitoreo permite recopilar, analizar y tomar acciones de seguridad y así minimizar el impacto en la organización.

Dentro de las ventajas de monitoreo Vargas (2023) detalla que el monitoreo 24x7 brinda una mayor visibilidad en forma general y a su entorno de seguridad para identificar y responder la amenaza de forma eficaz; se da una reducción del tiempo de respuesta dado que el monitore 24x7 permite una atención pronta y eficaz; el monitore proporciona una mejor eficiencia tanto de los recursos humanos como tecnológicos.

Vargas (2023) amplia mencionando los tipos de monitoreo que una organización puede implementar:

- Monitore de seguridad de la red: este se focaliza en la infraestructura de la red (router, switch, firewall).

- Monitoreo de los sistemas: se centra en los sistemas informáticos (servidores, estaciones de trabajo)

Se puede mencionar que el monitoreo de ciberseguridad es una inversión para la organización dado que estará protegida ante las amenazas cibernéticas ya reducirá el riesgo de sufrir un ataque.

Las organizaciones están expuestas a intentos de intrusión que pueden materializarse en incidentes de seguridad que pongan en riesgo la confidencialidad, integridad y disponibilidad de la información, para fortalecer el área de tecnología las empresas pueden implementar los siguientes sistemas:

- Sistemas de detección de intrusos (IDS): Según Tejada (2015) los IDS son sistemas de monitoreo de tráfico de la red que permiten establecer una protección de complemento a la plataforma tecnológica existente. Existen tipos de IDS tales como IDS basados en red, IDS basados en host (HIDS), IDS de detección por firmas, IDS de detección de anomalías.
- Sistemas de prevención de intrusos (IPS): Tejada (2015) determina este tipo de sistema como un monitoreo de tráfico en tiempo real, se considera con una herramienta que evolucionó del IDS. Los IPS tratan de prevenir amenazas de intrusión con paquetes dañados o incompletos, la red inmediatamente bloquea el paquete para evitar un posible ataque. Los IPS tiene se basan en aplicar filtros nuevos conforme se va detectando el ataque en progreso, minimiza las falsas alarmas, bloque automáticamente en tiempo real los ataques, mejora y optimiza el rendimiento de la red. Existen diferentes tipos de IPS como lo son el IPS de filtrado de paquetes, IPS de bloqueo de IP, IPS con acción de decepción.

Inteligencia Artificial en Ciberseguridad

Otra tecnología que surge para colaborar con los ciberataques es la inteligencia artificial ya que permite automatizar tareas, rutina, detectas amenazas cibernéticas y responde de manera oportuna el análisis de datos y la correlación de eventos. Según Solís (2023) la inteligencia artificial y el machine learning tiene una gran cantidad de aplicaciones, tales como:

- Detección de amenazas: por medio de la inteligencia artificial se pueden procesar y analizar altos volúmenes de información en tiempo real para detectar comportamientos y anomalías que pueden conllevar a incidentes de seguridad.
- Análisis de vulnerabilidades: a través de los análisis de la inteligencia artificial se puede identificar y priorizar las vulnerabilidades más críticas, permitiendo tomar las acciones preventivas antes de que se materialicen.
- Prevención de ataques: dado los análisis de patrones anómalos que efectúa la inteligencia artificial se logra detectar comportamientos atípicos y así se previenen ataques antes de que ocurran.
- Respuesta a incidentes: con la inteligencia artificial se logra la detección en tiempo real de amenazas, respuestas automatizadas basadas en patrones de ataques analizados, análisis de vulnerabilidades y análisis de riesgos.

Como parte del uso de la inteligencia artificial surge el análisis predictivo como un recurso para apoyar los incidentes de ciberseguridad, García (2024) detalla que el análisis predictivo es una herramienta clave en el ámbito de la ciberseguridad. Por medio de datos históricos recopilados, la estadística y el aprendizaje automatizado junto con la inteligencia artificial se puede llegar a prevenir posibles amenazas y ataques cibernéticos antes que se materialicen.

Los análisis predictivos en ciberseguridad se fundamentan en:

- Registro de eventos de seguridad: se registran las actividades existentes en una red.
- Patrones de tráfico de red: revelan anomalías que pueden ser indicativos de actividad sospechosa.

Así como tiene sus ventajas, García (2024) menciona que los análisis predictivos en ciberseguridad tienen sus desafíos, tales como:

- Calidad de los datos: la precisión de los resultados depende de la veracidad de los datos recopilados.
- Complejidad de los algoritmos: requiere recurso humano especializado para su instalación y mantenimiento.
- Interpretación de resultados: es determinante para la buena toma decisiones.

De acuerdo con Solís (2023) los beneficios de la inteligencia artificial en el ámbito de la ciberseguridad aportan muchos beneficios, algunos de ellos son:

- Detección temprana de amenazas: por medio de su tecnología de punta, como lo son los algoritmos sofisticados, la inteligencia artificial puede detectar de manera temprana las posibles amenazas basándose en patrones y comportamientos anómalos.
- Respuesta a rápida a incidentes: reducción del error humano: por su capacidad de aprendizaje la inteligencia artificial genera gran cantidad de registros y datos que agilizan la capacidad de respuesta a incidentes de seguridad, lo que apoya en la detección, mitigación y protección de las amenazas cibernéticas.

- Mejora en la eficiencia y efectividad de los equipos de seguridad: la inteligencia artificial contribuye con las acciones y decisiones de los equipos de seguridad dado su alto nivel de resolución que asume en lugar de ser atendidas por seres humanos, lo que permite que el equipo de seguridad se enfoque en otras tareas estratégicas y críticas, de esta manera se optimizan los recursos humanos y tecnológicos.

Capacitación en Ciberseguridad

La importancia de tener personal capacitado en una organización con conocimientos en ciberseguridad es esencial ya que permite estar actualizado con las nuevas tendencias en tecnología para atender las amenazas cibernéticas, por ello debe existir concientización en que la inversión que se dé no se vea como un gasto sino como una inversión de protección para la organización; se debe tener en consideración que la capacitación debe ser continua, no solo para el área de tecnología sino en forma general para todos los empleados que conforman la organización. Según ETEK (2024) las amenazas están en constante evolución, surgen nuevas vulnerabilidades, las amenazas son más sofisticadas y difíciles de prever. La formación y conocimiento debe ser continuo ya que facilitará la labor de los profesionales en ciberseguridad en el momento que deban atender un incidente de seguridad.

ETEK (2024) amplia mencionando que el cumplimiento normativo es un requisito obligatorio para cumplir con las regulaciones que le correspondan y así no incurran en sanciones legales severas.

Las empresas deben tener programas de capacitación en el área de ciberseguridad y en casos especiales personal certificado en la misma materia de esta forma el personal tendrá conocimientos y habilidades en el campo de la ciberseguridad.

Rosencrance (2024) determina para el año 2024 15 certificaciones ideales para preparar al personal de las áreas de TI:

- CompTIA Security: certificación que sustenta habilidades necesarias para cualquier puesto en el área de ciberseguridad.
- Fundamentos de Ciberseguridad de ISACA: certificación básica que contempla los conocimientos básicos de ciberseguridad.
- Certificado GIAC Security Essentials: certificado con conocimientos básicos para principiantes.
- AWS Certified Security: se basa en el diseño y la implementación de soluciones de seguridad.
- Profesional certificado en Seguridad de la Información: certificación avanzada de ISC2, especial para gerentes de seguridad, profesionales y ejecutivos; su objetivo es llegar a crear, implementar y gestionar un programa de ciberseguridad.
- Auditor Certificado en Sistemas de Información: forma parte del marco ISACA, prepara personas como auditores en ciberseguridad externos e internos para la evaluación de vulnerabilidades de seguridad, diseño y despliegue de controles.
- Profesional certificado en seguridad en la nube (CCSP): se concentra en la seguridad en la nube.

- Hacker Ético Certificado: prepara a la persona con habilidades en la detección de ataques, vectores, pruebas de penetración y prevención.
- Gestor certificado en seguridad de la información: persona tendrá la capacidad de efectuar evaluaciones de riesgo, gobernanza y respuesta a incidentes como gestor de seguridad de la información.
- Profesional certificado en seguridad ofensiva (OSCP): se especializa en las pruebas de penetración.
- Certificado en Riesgos y Control de Sistemas de Información (CRISC): capacita a las personas exclusivamente con habilidades especiales para la gestión ideal de los riesgos de la información.
- Profesional Certificado en Seguridad de Sistemas: la persona desarrollará habilidades para implementar, supervisar y administrar una infraestructura de TI segura.
- Profesional Avanzado en Seguridad de CompTIA: la personal podrá diseñar e implementar soluciones para preparar a la organización ante incidentes de seguridad de la información.
- Asociado Certificado Cisco CybersOps: programa del fabricante CISCO que permitirá tener conocimientos y habilidades en equipos de SOC para detectar y responder eficientemente las amenazas de ciberseguridad.
- Certificado GIAC en Gestiones de Incidentes: garantiza conocimientos, experiencia y habilidades para identificar, responder y resolver incidentes de ciberseguridad.

Una organización preparada en conocimiento y certificaciones en el ámbito de ciberseguridad tendrá una ventaja competitiva porque ofrecerá mayor confianza a los clientes y socios comerciales asegurando que sus datos están protegidos. ETEK (2024) clasifica cinco (5) puntos básicos en la implementación efectiva de la formación continua y la cultura del personal en materia de seguridad organizacional:

- Evaluación de necesidades: la organización debe identificar las habilidades y conocimientos que se requieran.
- Capacitación personalizada: un área específica debe desarrollar los programas de capacitación que se adecuen a la necesidad de la organización.
- Aprendizaje práctico: el conocimiento debe ir acompañado de simulacros de ciberataques para mejorar la capacidad de atención y respuesta del personal ante incidentes de seguridad reales.
- Actualización constante: el programa de capacitación debe estar siendo revisado y actualizado periódicamente por el surgimiento de nuevas amenazas.
- Incentivos y reconocimientos: para el personal el buen aprendizaje acompañado de buenos resultado es motivo de ofrecer por parte de la organización incentivos y reconocimientos.

Normativas y Estándares Internacionales en Ciberseguridad

Según Solutions (2023) la norma ISO 27001 es una estándar internacional que determina una serie de requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad del Información (SGSI), el cual se fundamenta en 3 pilares:

- Confidencialidad de la información: acceso a la información de los usuarios que se encuentran autorizados.
- Integridad de la información: condición completa y exacta de la información.
- Disponibilidad de la información: se garantiza el acceso a la información en el momento que se necesita.

El proceso de la implementación se divide en 4 etapas:

- Etapa de planificación: la organización debe identificar sus requisitos de la seguridad de la información y establecer un plan para la implementación del SGSI.
- Etapa de implementación: en esta etapa se definen las políticas, procedimientos y los controles para proteger la información.
- Etapa de evaluación: la organización evalúa la eficiencia del SGSI implementado e identifica oportunidades de mejora.
- Etapa de mejora continua: se determinan las mejoras en los procesos y controles del SGSI.

Otra norma de suma importancia que forma parte de la familia ISO 27000 es la norma ISO 27035, Schirn (2023) menciona que esta norma muestra los conceptos, principios y los procesos básicos para la gestión de incidentes de seguridad de la información. La norma establece un enfoque estructurado y planificado para:

- Planificar y preparar la gestión de incidentes de seguridad de la información que se conforma por las políticas, la organización el plan, el soporte técnico, la concientización y capacitación entre otros.

- Detectar, notificar y evaluar los incidentes de seguridad de la información y vulnerabilidades involucradas con el incidente.
- Repuesta a los incidentes de seguridad de la información, lo cual incluye la activación de controles para prevenir, reducir y recuperación del impacto.
- Tratar adecuado de las vulnerabilidades de seguridad de la información que se asocian al incidente.
- Lecciones de aprendizaje de los incidentes de seguridad de la información y las vulnerabilidades presentadas para realizar mejoras a la gestión de incidentes de la seguridad de la información.

Otra normativa que apoya a las organizaciones es el Marco de Ciberseguridad del NIST, el cual ayuda a las organizaciones a gestionar de una mejor manera los riesgos de ciberseguridad, según OEA-WAS (2019) este marco fue desarrollado en Estados Unidos con la Orden Ejecutiva número 13636, que se publicó el 2 de febrero del 2013, la cual pretende compartir información sobre amenazas de ciberseguridad y reducir los riesgos para infraestructura crítica, partiendo de este objetivo se denomina el Cybersecurity Framework (CSF).

El Cybersecurity Framework (CSF) se constituye de tres componentes:

- Framework Core: es el conjunto de actividades y resultados en el ámbito de ciberseguridad el cual se organiza en categorías. El Core se basa en tres partes: Funciones, Categorías y Subcategorías, se adicional cinco funciones de alto nivel clasificadas como: Identificar, Proteger, Detectar, Responder y Recuperar.
- Niveles de implementación (Tiers): los niveles detallan el grado de la gestión de riesgos del área de ciberseguridad de una organización, los niveles se clasifican

como Parcial (Nivel 1), Riesgo Informático (Nivel 2), Repetible (Nivel 3) y Adaptativo (Nivel 4).

Figura 7

Niveles de Implementación (TIERS)

Nota. Esquema de Cybersecurity Framework (CSF), tomado de OEA-WAS (2019)

- Perfiles: los perfiles son el método de la definición de los requisitos y objetivos de la organización, estima la tolerancia al riesgo y los recursos a los resultados esperados por el marco NIST. Los perfiles colaboran con la identificación de oportunidades de mejora efectuando la comparación de perfiles actuales con nuevos.

OEA-WAS (2019) detalla cinco (5) funciones del CFS que son como pilares para que un programa de ciberseguridad sea exitoso:

- Identificar: permite la identificación y la administración del riesgo de ciberseguridad tomando en consideración los sistemas, las personas, los activos, los datos y las capacidades de la organización.
- Proteger: se detallan las medidas de seguridad para garantizar la entrega de los servicios de las áreas de TI clasificadas como críticas, lo cual garantiza la limitación del impacto de un incidente de ciberseguridad.
- Detectar: se determinan las actividades para la identificación de un incidente de ciberseguridad lo más oportuno posible.
- Responder: se contemplan las actividades necesarias para tomar las medidas asociadas a un incidente de ciberseguridad.
- Recuperar: en esta etapa se deben establecer las actividades para mantener los planes de resiliencia y para normalizar los servicios que hayan sido afectados por un incidente de ciberseguridad.

Figura 8

Cybersecurity Framework (CSF)

Nota. Fases del Marco NIST, tomado de OEA-WAS (2019)

Otras certificaciones a toma en consideración y de acuerdo UNIR (2020) la certificación CISA (Certified Information Systems Auditor) es reconocida a nivel internacional para realización de auditorías, revisión y controles para la seguridad de la información, forma parte de la principal certificación de ISACA (Information Systems Audit and Control Association) la cual es autoriza por el Departamento de Defensa de los Estados Unidos.

De acuerdo con INCIBE (s.f.) el Instituto Nacional de Ciberseguridad de España (INCIBE) se enfoca en elevar el grado de ciberseguridad y la resiliencia, consolida como una empresa de referencia para el desarrollo de la ciberseguridad.

En Costa Rica de acuerdo con la información que se muestra en MICITT (s.f.), este organismo que impulsa en Costa Rica el cumplimiento de las políticas públicas en materia de ciencia, innovación, tecnología y telecomunicaciones con el fin de mejorar el bienestar social, la igualdad y la prosperidad de la sociedad costarricense,

Normativas para la Atención de Incidentes de Ciberseguridad

Con el objetivo de establecer normativas que sirvan de referencia a la investigación en curso, se procede con el análisis de normativas que contribuyan con la atención de incidentes de ciberseguridad de uso general:

- ISO/IEC 27001, Alonso (2023): norma que determina los pasos a seguir para implementar y gestionar un SGSI.
- ISO/IEC 27032, Alonso (2023): esta norma contribuye con la identificación de líneas generales para optimizar y mejorar el estado de la ciberseguridad en una organización.

- ISO/IEC 27033, Alonso (2023): esta norma logra establecer las pautas de seguridad de la administración, operación y uso de las redes y comunicaciones.
- ISO/IEC 27035, Alonso (2023): por medo de esta norma se definen un conjunto de mejores prácticas que interactúan con la gestión de riesgos y respuesta a incidentes en sistemas de información, basándose en la detección, reporte y evaluación de incidentes de seguridad.
- ISO/IEC 27036, Alonso (2023): norma que apoya la seguridad de la información con la interacción directa con proveedores.
- NIST SP 800-61, NIST (s.f. revisado 4 marzo 2024): recomendaciones y consideraciones de respuesta a incidentes para la gestión de riesgos de ciberseguridad.
- NIST SP 800-84, NIST (s.f.): esta publicación colabora con las organizaciones a diseñar, desarrollar, realizar y evaluar eventos de pruebas, capacitación para mejorar el conocimiento del personal de TI, así una organización pueda maximizar su capacidad para prepararse, responder, gestionar y recuperarse ante desastres.
- NIST SP 800-150, NIST (s.f.): esta publicación ayuda a las organizaciones a establecer objetivos de intercambio de información, identificar fuentes de posibles amenazas.
- COBIT 5, Mendoza (2015): Enfoque en el dominio de la gestión de servicios: este documento de COBIT en su última edición se enfoca específicamente en la seguridad de la información, sus tres (3) módulos son el APO13 Gestión de la seguridad, DSS04 Gestión de la continuidad y el DSS05 Gestión de servicios de seguridad.

De acuerdo con las normativas investigadas se procede a segmentar tres grupos de normas:

- Normas ISO/EIC: normas con serie de regulaciones y estándares internacionales que se pueden aplicar a un amplio sector de empresa y organizaciones, estas normas se centran en la gestión de la seguridad de la información con el fin de fortalecer los sistemas informáticos.
- Normas NIST: el marco de ciberseguridad del NIST ayuda a las empresa y organizaciones a comprender los riesgos de ciberseguridad, lo cual le permitirá administrar y reducir sus riesgos antes ciberataques protegiendo así sus redes y datos; proponer mejorar la seguridad y resiliencia en los sistemas de información.
- Normas COBIT: marco de trabajo para los gobiernos y la gestión de las tecnologías de la información enfocado a cualquier empresa, su objetivo es establecer un marco integral para el control y la gestión de los procesos de TI.

Según Bittencourt (2024) las tres normativas tienes sus características propias en:

- Enfoque y área central: COBIT se centra en la gobernanza y gestión de TI basado en procesos, ISO 27001 se centra en la gestión de la seguridad de la información para implementar un SGSI, y NIST se fundamenta en mejorar la seguridad y la resiliencia de los sistemas de información.
- Fuente y aplicación: COBIT fue desarrollado por ISACA, ISO 27001 desarrollado por la Organización Internacional de Normalización (ISO) y NIST por el gobierno de los Estados Unidos.

- Orientación geográfica: COBIT e ISO 27001 son normas reconocidas a nivel internacional, se puede emplear en cualquier país, NIST es un marco usado en Estados Unidos.
- Alcances y detalles: COBIT proporciona un marco integral para la gobernanza de TI, ISO 27001 se centra en la gestión de la seguridad de la información y NIST ofrece un conjunto completo de estándares para mejorar la seguridad y la resiliencia de los sistemas de información.

Normativas para la Atención de Incidentes de Ciberseguridad de uso Bancario

Con el objetivo de establecer normativas que sirvan de referencia a la investigación en curso, se procede con enumerar normativas que contribuyan con la atención de incidentes de ciberseguridad de uso bancario:

- American Bankers Association (ABA), ABA (2024): organización americana de banqueros que establece capacitaciones, certificaciones, investigaciones en otros, y actualmente apoya con una guía la gestión del riesgo de seguridad cibernética en entornos bancarios.
- BCBS 147, Basel Committee on Banking Supervision, Open_Risk_Manager (2021): constituye un documento para fortalecer las entidades financieras ante situaciones de crisis.
- BCBS 239, Basel Committee on Banking Supervision, KPMG (2024): documento que establece mejores prácticas para la gobernanza de datos, documentación y datos y la gestión de la calidad de los datos; pretende estandarizar regulaciones ara la mejora de la gestión de los datos.

- ISAC (Information Sharing and Analysis Center), ENISA (2005-2024): organización sin fin de lucro, su objetivo es recopilar información sobre amenazas cibernéticas para compartir experiencias, conocimientos, análisis e información sobre amenazas cibernéticas en la industria financiera.
- ISO/IEC 27002, Alonso (2023): Normativa para la implementación de un sistema de gestión de la seguridad de la información en instituciones financieras, se sustenta en 93 controles estructurados en cuatro (4) grandes dominios.
- FFIEC IT Handbook Infraestructure and Operations, FFIEC (2021): guía para la seguridad de la información y la atención de incidentes en entornos bancarios, enfocada en infraestructura y operaciones. Esto procedimientos ayudan a evaluar controles y procesos de gestión de riesgos bancarios.
- NACHA Operating Rules, Nacha (s.f.): Normativa para la seguridad de los datos de transacción en sistemas de pago de EE. UU, su objetivo es reducir las incidencias de intentos de fraudes exitosos.
- NIST 800-171, NIST (2021): Normativa para la protección de datos confidenciales en contratos del gobierno de EE. UU., aplicable también a la industria bancaria, se concentra en la protección de la información no clasificada contralada.

Herramientas Comerciales para la Atención de Incidentes

Con el objetivo de establecer herramientas para la propuesta de la solución a la investigación en curso, se procede con investigar herramientas comerciales para la atención de incidentes:

- Splunk, Splunk (2005-2024): Plataforma SIEM (Security Information and Event Management) que permite monitorear, analizar y responder a incidentes de seguridad en tiempo real, su ventaja: Amplia capacidad de análisis de grandes volúmenes de datos, detección temprana de amenazas y generación de reportes de cumplimiento normativo.
- IBM QRadar, IBM (s.f.): Plataforma SIEM que ofrece monitoreo avanzado y análisis de seguridad, su ventaja es la integración con otras herramientas de seguridad, capacidades de inteligencia artificial y machine learning para detectar patrones de comportamiento anómalo.
- Palo Alto Networks Cortex XSOAR, Paloalto (2024): Plataforma de automatización y orquestación de respuesta ante incidentes (SOAR), su ventaja es que facilita la respuesta automática a incidentes, reducción del tiempo de resolución y gestión eficiente de tickets y flujos de trabajo.
- Microsoft Azure Sentinel: solución SIEM y SOAR nativa de la nube, su ventaja es la alta escalabilidad, análisis basado en inteligencia artificial y fácil integración con soluciones de Microsoft 365, ideal para bancos que utilizan servicios en la nube.
- McAfee MVISION, Trellis-McAfee (s.f.): solución de seguridad integral que incluye SIEM, DLP (Data Loss Prevention) y EDR (Endpoint Detection and Response), su ventaja es la protección avanzada contra amenazas, visibilidad completa en todos los endpoints y fácil integración en infraestructuras corporativas.

- Cisco SecureX, Datacom.Global (s.f.): Plataforma de detección y respuesta que unifica la visibilidad de amenazas en todo el ecosistema de seguridad, su ventaja es la integración nativa con las soluciones de seguridad de Cisco, orquestación y automatización de la respuesta ante incidentes.
- FireEye Helix, Licencias_OnLine (s.f.): plataforma SIEM y SOAR que proporciona detección avanzada de amenazas y capacidades de respuesta, su ventaja es la fuerte capacidad de análisis de amenazas avanzadas, ideal para bancos que enfrentan amenazas persistentes avanzadas (APT), se basa en servicios de protección para ambiente nube.
- Rapid7 InsightIDR, Rapid7 (s.f.): solución SIEM con capacidades de detección de amenazas y respuesta a incidentes, su ventaja es la facilidad de uso, rápida implementación y fuerte enfoque en la detección y respuesta ante amenazas internas, se enfoca en la protección en nube.
- ServiceNow, ServiceNow (2024): herramienta no es tradicionalmente clasificada como un gestor de seguridad, pero sí cuenta con módulos robustos para la gestión de incidentes de ciberseguridad y es ampliamente utilizada en ambientes bancarios y empresariales para gestionar incidentes de seguridad. ServiceNow incluye el módulo Security Operations (SecOps), que ofrece varias funcionalidades clave para la gestión de incidentes de ciberseguridad.
  Algunas de las funcionalidades relevantes de ServiceNow Security Operations (SecOps):
- Gestión de Incidentes de Seguridad: permite registrar, priorizar y rastrear los incidentes de seguridad desde la detección hasta la resolución. Integra

automáticamente las amenazas detectadas con sistemas SIEM y otras fuentes de inteligencia para priorizar los incidentes.

- Orquestación y Automatización (SOAR): automatiza tareas repetitivas y reduce el tiempo de respuesta ante incidentes. Puede integrar con herramientas como Splunk o IBM QRadar para automatizar la contención de amenazas y acelerar la mitigación.
- Gestión de Vulnerabilidades: facilita la identificación y priorización de vulnerabilidades, permitiendo a los equipos de seguridad abordar rápidamente las amenazas que representan mayor riesgo.
- Cumplimiento y Auditoría: ServiceNow permite rastrear el cumplimiento normativo de diversas regulaciones como PCI DSS, ISO 27001 y otros estándares aplicables en ambientes bancarios.
- Integración: ServiceNow se integra fácilmente con otras soluciones de seguridad y herramientas empresariales (SIEM, herramientas de ticketing, etc.), creando un ecosistema unificado para la gestión de incidentes.

Continuidad del Negocio y Gestión de la Reputación

La continuidad del negocio se refiere a la capacidad de una organización de lograr mantener sus servicios clasificados como críticos durante y después de un incidente de seguridad de la información, dado lo anterior la organización debe poseer un plan para atender de manera oportuna la amenaza. S2 Grupo (2023) determina que la continuidad del negocio es vital para garantizar la estabilidad y la capacidad de adaptación a un entorno de amenazas, lo cual le brinda las siguientes ventajas:

- Mantenimiento de operaciones críticas: los servicios se mantienen a pesar de estar en situaciones críticas de interrupción de los servicios tomando en consideración desastres naturales, ciberataques, etc.
- Reducción de pérdidas financieras: relacionadas a la afectación de los servicios de la organización.
- Protección de la reputación y satisfacción al cliente: le permite a la organización mantener la credibilidad de sus clientes y socios al continuar brindando sus servicios a pesar de estar en situaciones críticas.
- Cumplimiento de requisitos regulatorios: no se exponen a sanciones graves por incumplimiento de regulaciones o leyes.
- Garantía de la seguridad de los empleados: les garantiza a los empleados una estabilidad en la que no se ven afectados por la imagen que representan de la organización.

La creación y definición de un Business Impact Analysis (BIA) le permitirá la organización identificar y priorizar los activos críticos para la continuidad de las operaciones del negocio.

Tecnologías Avanzadas en Ciberseguridad

La ciberseguridad se ha convertido en un aspecto muy crítico para las organizaciones, las amenazas cada día tienen avances tecnológicos que hacen que se desarrollen herramientas y soluciones emergentes para el ámbito de la ciberseguridad, algunas son:

- Inteligencia Artificial y Machine Learning
- Blockchain

- Cifrado de Datos
- Seguridad Zero Trust

El Blockchain es una tecnología emergente para combatir las amenazas, IEBS (2024) explica que el Blockchain es una tecnología basada en una cadena de bloques de operaciones descentralizada y pública. Esta tecnología produce una base de datos compartida en forma de bloques de manera simultánea, la cadena de bloques que se va formando determina un registro de transacciones almacenadas. Estos bloques se pueden copiar y replicar en computadoras individuales, todos los bloques son idénticos y están sincronizados entre sí; cuando alguien agrega información o elimina datos, cambia la información de todos.

Con respecto a la interacción del Blockchain y su aplicación con la seguridad de la información, Ciberseguridad (2024) menciona que esta herramienta mejora la protección de los sistemas de seguridad y datos sensibles, sus características y beneficios son:

- Transparencia y trazabilidad: el Blockchain tiene la particularidad de proporcionar un registro inmutable y transparente de todas las transacciones, lo que aumenta la confianza en el sistema y previene manipulaciones y fraudes.
- Descentralización y resistencia a ataques: Blockchain se encarga de distribuir los datos en una red de nodos interconectados, lo que se le hace difícil a un atacante comprender la integridad de los datos, reduciendo de manera significativa la vulnerabilidad de los sistemas.
- Criptografía robusta: Blockchain emplea algoritmos de criptografía avanzada para brindar protección a los datos almacenados en la cadena de bloques mejorando la seguridad de la información.

La relación del Blockchain y la ciberseguridad fortalece la protección de la identidad, se incrementan los niveles de la autenticación y verificación de los datos.

El Big Data es una tecnología novedosa que se fundamente en la identificación de patrones y comportamientos anómalos de una red, esta tecnología puede monitorear gran cantidad de datos en tiempo real que son generados en una organización, Domínguez (2023) determina que el Big Data puede detectar patrones y comportamientos anómalos que pueden llevar a un incidente de ciberseguridad. Algunas aplicaciones en que el Big Data interactúa con la ciberseguridad son:

- Detección de amenazas: por medio del análisis de datos se pueden identificar patrones o comportamientos anómalos en la red empleando datos históricos y en tiempo real permitiendo identificar y prevenir ataques cibernéticos.
- Análisis forense: dada el alto volumen de datos que se pueden gestionar es factible identificar a los responsables de un ataque cibernético.
- Análisis de comportamiento: el big data puede identificar patrones de comportamiento de los usuarios finales indicando si existen movimientos sospechosos.
- Gestión de vulnerabilidades: los datos que maneja big data pueden ser escaneados lo que permite detectar debilidades en la red.

Igual que los servicios on-premise, los servicios que se concentran en la nube deben estar protegidos contra amenazas y ciberataques, por ello se deben establecer políticas, proceso y tecnologías para garantizar la protección de los datos. Kaspersky (s.f.) determina que la seguridad en la nube es el conjunto de tecnologías, protocolos y buenas prácticas que protegen

los datos en un ambiente de nube, esta responsabilidad recae en los proveedores que brindan este tipo de servicio. Los proveedores deben garantizar los siguientes requerimientos:

- Permitir la recuperación de datos en caso de pérdidas de datos.
- Proteger el almacenamiento y las redes contra el robo de datos malicioso.
- Impedir el error o la negligencia humana que causa pérdida de datos.
- Reducir el impacto de cualquier puesta en peligro de los datos

Otro aspecto por tomar en consideración es la transformación digital, Huerta (2023) menciona que son muchos los beneficios que se obtienen de la transformación digital, esta puede ofrecer muchas oportunidades para optimizar la eficiencia operativa, mejorar la experiencia al cliente, pero a su vez lleva muchos desafíos en su implementación en la adopción de nuevas tecnologías y la integración de procesos.

La transformación digital, según Huerta (2023) muestra los siguientes desafíos:

- Desafío 1, resistencia al cambio: el desafío más común es la resistencia de los colaboradores dado que están acostumbrado a trabajar con procesos manuales y tradicionales; por esta razón es necesario el dialogo con los trabajadores y explicarles los beneficios que trae la transformación digital a la organización.
- Desafío 2, falta de habilidades y desconocimiento sobre lo digital: este desafío se da por la falta de oportunidades de mejora en los colaboradores, de manera que, se deben identificar las habilidades y conocimientos que existen en la organización.
- Desafío 3, integración de tecnologías y sistemas existentes: este desafío se presenta al momento de la integración de tecnologías, específicamente al momento de efectuar la compatibilidad, la migración de los datos y la sincronización de los sistemas, para solventar esta situación se debe implementar

un plan de integración que tome en consideración os aspectos técnicos y operativos de la organización.

- Desafío 4, seguridad y privacidad de los datos: para la organización este desafío es muy importante ya que debe velar por la protección de la información confidencial y sensible y así evitar la pérdida de confianza de los clientes y de disputas legales. Por esta razón la organización debe implementar herramientas de seguridad adecuadas, establecer políticas de acceso y control de los datos, y la concientización del personal con prácticas de seguridad digital.

Cultura de Seguridad

La cultura del personal en una organización es esencial porque forma parte de las buenas prácticas y fundamentos para prevenir un incidente de seguridad de la información, por esta razón las organizaciones deben de implementar capacitaciones que den una solidez al personal y así estarán protegidos ante eventos o incidentes de seguridad de la información.

Para Lozano (2024) una cultura de ciberseguridad se refiere al conjunto de valores y comportamientos que existen en una organización que ayudaran a comprender por qué es vital la protección de los datos de la empresa. Amplía mencionando que es vital la participación de todos los empleados dado que cada uno de ellos cumple un rol dentro de la organización y será trascendental su actuar en el momento de una amenaza de ciberseguridad.

Lozano (2024) detalla que la organización debe establecer políticas de ciberseguridad, brindar capacitación continua, realizar pruebas prácticas para identificar vulnerabilidades dentro del personal que pongan en riesgo a la organización en caso de una amenaza cibernética.

Las políticas por establecer deben se sencilla de comprender y aplicar, y en la medida de lo posible alineadas con estándares de seguridad como lo es la ISO 27001.

Para que una metodología en general para la atención de incidentes de seguridad de la información sea exitosa siempre deberá contar con el apoyo e involucramiento de la alta dirección de la organización, Lozano (2024) recalca que el apoyo de la alta dirección es determinante para el éxito de cualquier iniciativa asociada al ámbito de ciberseguridad, esto deben mostrar un alto compromiso asociado a la misma estratega empresarial asegurándola como una prioridad en la toma de decisiones de la empresa.

La alta dirección tiene la responsabilidad de asignar recurso humano y económico para implementar los proyectos que se asocien a las implicaciones de la seguridad de la información de la organización.

Capítulo III: Marco Metodológico

Introducción al Marco Metodológico

El marco metodológico de esta investigación tiene como objetivo principal describir los procedimientos y enfoques que se utilizarán para desarrollar un modelo integral de gestión de incidentes y ciber resiliencia para BN FONDOS del Banco Nacional de Costa Rica. Este modelo tiene como propósito mitigar efectivamente el riesgo de ciberataques, garantizar la continuidad del negocio y proteger la reputación de la entidad ante la creciente amenaza de ciberataques en un entorno digital en constante evolución.

Enfoque de la Investigación

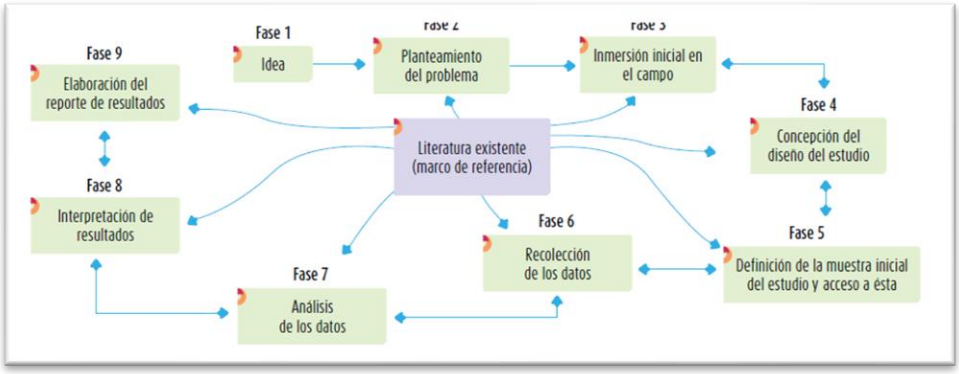
Los diferentes enfoques de investigación pretenden ser procesos muy detallados, son metódicos y a su vez empíricos dado que su objetivo es brindar la mejor y más información posible al caso en estudio; por ellos los enfoques cuantitativos y cualitativos pueden llegar a compartir su estrategia, pero cada una con sus respectivas características.

Como lo indica Sampieri (2014) el enfoque cualitativo se fundamenta en la recolección y análisis de los datos que permitan llegar a formular preguntas e hipótesis durante todo el proceso de la recolección y análisis de datos. La formulación de las preguntas va a permitir aclarar cuales son las preguntas más importantes, afinarlas y finalmente responderlas.

La siguiente figura representa el proceso cualitativo:

Figura 9

Proceso Cualitativo

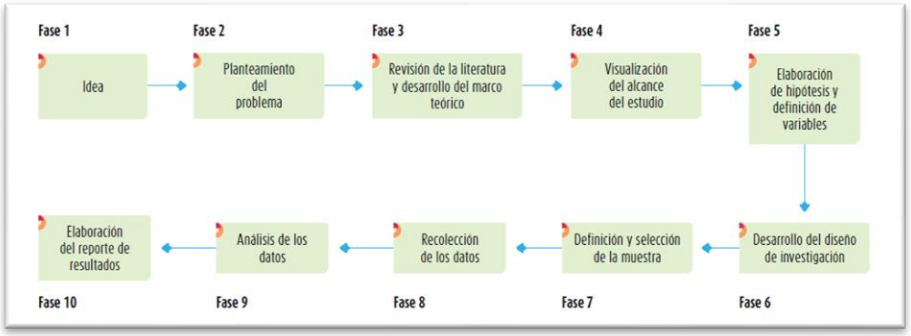


Nota. Esquema del Proceso Cualitativo, tomado de Sampieri (2014)

Por otra parte, Sampieri (2014) con respecto al enfoque cuantitativo indica, que este enfoque representa un conjunto de procesos secuenciales y probatorio. Este enfoque utiliza la recolección de los datos con el objetivo de validar los datos de una manera numérica para determinar el comportamiento del análisis de los datos y probar las teorías.

Figura 10

Proceso Cuantitativo



Nota. Esquema del Proceso Cuantitativo, tomado de Sampieri (2014)

A causa de lo antes dicho, Sampieri (2014) concluye que el enfoque cualitativo se basa en el desarrollo o crecimiento de los datos, se fundamenta en sí mismo; mientras que el enfoque cuantitativo pretende delimitar la información con precisión para establecer patrones de comportamiento según la variable que corresponda.

Enfoque Mixto

El enfoque de investigación mixto se define como la combinación de las rutas cuantitativa y cualitativa. Según Sampieri (2018), esta integración representa un conjunto de procesos sistemáticos, empíricos y críticos, sustentándose en la recolección y análisis de datos provenientes de ambos enfoques, que incluyen información numérica, verbal, textual y visual.

Sampieri (2014) destaca que estos enfoques no deben ser vistos como competidores, sino que ambos aportan un valor significativo. Al combinar sus perspectivas, se logra un acercamiento más completo al caso en estudio. La utilización de un enfoque mixto permite capitalizar las fortalezas de cada metodología, facilitando una comprensión más rica y matizada del fenómeno investigado.

Tras evaluar los tipos de enfoques disponibles, se ha llegado a la conclusión de que el enfoque mixto es el más adecuado para su uso en la presente investigación. Para lograr obtener los resultados buscados por medio del enfoque mixto, se utilizarán instrumentos tales como entrevistas, encuestas, benchmarking y recolección bibliográfica que permitan dar respuesta a la pregunta de investigación planteada.

Justificación del Enfoque

La combinación de métodos cualitativos y cuantitativos permite:

- Profundizar en la comprensión de las percepciones y actitudes del personal hacia la ciberseguridad.
- Cuantificar la extensión y severidad de las vulnerabilidades y amenazas que enfrenta BN FONDOS.
- Desarrollar un modelo que sea tanto técnicamente robusto como operativamente viable, asegurando la participación y el compromiso del personal de la organización.

Componentes del Enfoque Mixto

- Cualitativo: Este componente se enfocará en comprender las experiencias, percepciones y actitudes del personal clave en BN FONDOS. La investigación cualitativa incluirá entrevistas semi-estructuradas.
- Cuantitativo: Este componente se centrará en el análisis de datos numéricos y en la evaluación objetiva de la infraestructura tecnológica y las medidas de seguridad actuales mediante auditorías y pruebas de penetración.

Método de la Investigación

Estudio de Caso

El método principal de esta investigación será el estudio del caso BN FONDOS se analizará en profundidad para entender su contexto particular, identificar sus necesidades específicas en términos de ciberseguridad y diseñar un modelo adaptado a sus características.

Justificación del Método

El estudio de caso es adecuado para esta investigación por las siguientes razones:

- Profundidad del Análisis: Permite un examen exhaustivo y detallado de las variables críticas.
- Contextualización: Considera el entorno específico de BN FONDOS, lo cual es crucial para desarrollar un modelo personalizado de gestión de incidentes y ciber resiliencia.
- Flexibilidad: El estudio de caso permite la adaptación de los métodos de recolección y análisis de datos según las necesidades emergentes durante la investigación.

Fuentes de Información

Otro punto para tomar en consideración son las fuentes de información que darán sustento a la investigación, son la materia prima que nos darán hechos, opiniones y datos relevantes.

Según Sampieri (2014), las fuentes de información o bien la revisión de la literatura nos ayudará a detectar, consultar y obtener fuentes bibliográficas de alta relevancia que contribuya a alcanzar el propósito de la investigación. Las fuentes de información se clasifican en:

- Fuentes primarias: son las que proporcionan datos de primera mano, ejemplos de son libros, tesis, antologías, artículos periodísticos, documentales, videos, foros, páginas web, entre otros.

- Fuentes secundarias: consisten en compilaciones de información, resúmenes o bien listados de referencia, se puede decir que una fuente secundaria se relaciona a información ya procesada.

Fuentes Primarias

- Entrevistas Semi-estructuradas: Se llevarán a cabo entrevistas con expertos en ciberseguridad y personal clave de BN FONDOS, como responsables de tecnología, seguridad informática.
- Encuestas: Se aplicarán encuestas al personal de BN FONDOS para medir su conocimiento y actitud hacia la ciberseguridad, así como para identificar áreas de mejora en la capacitación.

Fuentes Secundarias

- Literatura Académica y Técnica: Se revisarán artículos académicos, libros y publicaciones técnicas sobre ciberseguridad, gestión de incidentes y ciber resiliencia.
- Informes de Pruebas de Penetración: Se analizarán los informes de pruebas de intrusión externas e internas de BN FONDOS efectuadas en los periodos 2022 y 2023 con el objetivo de identificar vulnerabilidades y patrones recurrentes.
- Estudios de Casos Análogos: Se estudiarán casos de otras instituciones financieras que han implementado modelos de gestión de incidentes y ciber resiliencia exitosos.

- Normativas y Estándares Internacionales: Se consultarán normas como ISO 27001, NIST SP 800-61, y otros marcos de referencia reconocidos en ciberseguridad.

Variables o Unidades de Análisis

De acuerdo con Sampieri (2014) una variable es una propiedad, característica o cualidad que pueden cambiar sus valores aun así puede llegar a medirse o bien ser observada. Ejemplos de variables pueden ser personas, objetos, hechos entre otros, estos poseen valores de acuerdo con un valor determinado. Las variables toman relevancia cuando se les llega a relacionar con otra, así llegan a formar parte de una hipótesis o una teoría.

Para la solución del problema detectado en BN FONDOS se determina las siguientes variables:

Tabla 1

Operacionalización de Variables

Objetivos Específicos	Variables	Dimensión	Indicadores	Fuentes de Datos
Analizar las principales amenazas cibernéticas que afectan a BN FONDOS para identificar los riesgos críticos que deben ser abordados en el modelo de gestión de incidentes y ciber resiliencia mediante la recopilación de datos históricos de ciberataques.	Amenazas Cibernéticas	Tipos de Ataque	Número de ataques por tipo, frecuencia de ataques	Datos históricos de ciberataques, informes de seguridad, libros y referencias web
	Riesgos Críticos	Impacto en la confidencialidad, integridad y disponibilidad	Porcentaje de sistemas afectados, tiempo de inactividad, datos comprometidos	Informes de auditorías, análisis de riesgos pasados, evaluaciones de ciberseguridad

Objetivos Específicos	Variables	Dimensión	Indicadores	Fuentes de Datos
	Datos Históricos de Ciberataques	Frecuencia de incidentes, patrones de ataques	Número de ciberataques registrados, patrones de ataques en años recientes	Informes históricos de pruebas de penetración de BN FONDOS
Evaluar la infraestructura tecnológica y los sistemas de seguridad actuales de BN FONDOS para determinar las vulnerabilidades existentes que podrían comprometer la continuidad del negocio mediante el estudio de resultados históricos de auditorías.	Infraestructura Tecnológica	Sistemas críticos y secundarios	Estado de los sistemas tecnológicos, tiempo de operación, actualización de los sistemas	Informes de pruebas de intrusión, revisión de infraestructuras TI en BN FONDOS, entrevistas y encuestas
	Vulnerabilidades Existentes	Brechas de seguridad, nivel de exposición	Número de vulnerabilidades detectadas, criticidad de estas	Resultados de auditorías de seguridad, análisis de vulnerabilidades

Objetivos Específicos	Variables	Dimensión	Indicadores	Fuentes de Datos
	Continuidad del Negocio	Impacto en la operativa, tiempo de recuperación	Tiempo de recuperación ante fallos, nivel de afectación en la operativa	Estudios de riesgos de continuidad
Desarrollar estrategias específicas de prevención, respuesta y recuperación para mitigar el impacto de posibles ataques en BN FONDOS mediante la integración de mejores prácticas de ciberseguridad y alineado con estándares internacionales.	Estrategias de Prevención, Respuesta y Recuperación	Planes y protocolos de seguridad	Existencia de planes de respuesta, medidas preventivas, tiempo de implementación	Informes internos, planes de ciberseguridad actuales, normativas de NIST, ISO 27001, entrevistas y encuestas
	Mejores Prácticas de Ciberseguridad	Normativas internacionales, políticas de seguridad	Nivel de cumplimiento con NIST, ISO 27001	Auditorías, informes de cumplimiento normativo

Objetivos Específicos	Variables	Dimensión	Indicadores	Fuentes de Datos
	Alineación con Estándares Internacionales	NIST, ISO 27001, COBIT	Nivel de cumplimiento de normativas internacionales	Referencias normativas, auditorías de seguridad, reportes de cumplimiento
Proponer un sistema de monitoreo y detección temprana de amenazas para fortalecer la capacidad de BN FONDOS de responder de manera oportuna y efectiva ante incidentes de seguridad mediante el uso de tecnologías avanzadas de inteligencia artificial y análisis predictivo.	Sistema de Monitoreo y Detección	Tecnología de monitoreo, herramientas de análisis	Tiempo de detección de amenazas, frecuencia de incidentes detectados, tecnología utilizada	Reportes de seguridad, herramientas tecnológicas implementadas, auditorías internas

Objetivos Específicos	Variables	Dimensión	Indicadores	Fuentes de Datos
	Tecnologías Avanzadas (IA, análisis predictivo)	Eficiencia en la detección, predicción de amenazas	Tiempo de respuesta ante amenazas, efectividad de predicciones	Informes de implementación de IA, evaluaciones de efectividad del sistema de monitoreo
Diseñar el plan de capacitación para el personal de BN FONDOS en ciberseguridad y gestión de incidentes para garantizar una respuesta coordinada y eficiente ante ciberataques mediante un programa de formación continua y simulaciones de ciberataques.	Plan de Capacitación en Ciberseguridad	Programa de formación, frecuencia de capacitaciones	Número de empleados capacitados, frecuencia de las capacitaciones, evaluaciones de desempeño	Documentos internos, plan de formación, simulaciones de ciberataques

Objetivos Específicos	Variables	Dimensión	Indicadores	Fuentes de Datos
	Simulaciones de Ciberataques	Pruebas de respuesta, capacidad de gestión de incidentes	Número de simulaciones realizadas, tiempo de respuesta ante simulaciones, desempeño del equipo	Informes de simulaciones, auditorías internas

Nota: Elaboración propia, 2024, datos provienen de los objetivos definidos.

Instrumentos

Para proceder con la recolección de datos se debe tomar en consideración los instrumentos idóneos para el estudio, Sampieri (2014) determina que la recolección de datos se fundamenta en un plan detallado que nos permitan agrupar datos con un propósito específico.

Para que exista una certera recolección de datos los instrumentos a emplear deben cumplir con tres requisitos:

- Confiabilidad: se refiere a la acción de aplicar un instrumento de medición a un individuo u objeto y los resultados siempre deberán ser iguales.
- Validez: se refiere a que el instrumento siempre tendrá la capacidad de medir la variable.
- Objetividad: grado del instrumento que puede llegar a cumplir el objetivo ante sesgos o tendencias de las personas que lo administran, califican e interpretan.

En esta investigación se determina la recolección de datos por medio de los siguientes instrumentos:

Entrevistas Semi-estructuradas

- Diseño de la Entrevista: Se elaborará un guion de entrevista con preguntas abiertas que permitan a los entrevistados expresar sus experiencias y conocimientos sobre ciberseguridad en BN FONDOS.
- Selección de Entrevistados: Se seleccionarán individuos clave, incluyendo responsables de TI, seguridad de la información, y altos directivos.
- Proceso de Entrevista: Las entrevistas se realizarán de manera individual, permitiendo un ambiente de confidencialidad para obtener respuestas honestas y detalladas.

Encuestas

- Diseño de la Encuesta: Se diseñarán cuestionarios con preguntas cerradas y escalares para medir el conocimiento y las prácticas de seguridad entre el personal.
- Distribución: Las encuestas se distribuirán electrónicamente a todo el personal de BN FONDOS.
- Análisis Estadístico: Los resultados de las encuestas se analizarán utilizando técnicas estadísticas para identificar tendencias y áreas de mejora.

Pruebas de Penetración

- Resultados de Pruebas de Penetración: Se realizará una revisión de las pruebas de penetración (pruebas de intrusión externas e internas) de los dos últimos años para identificar vulnerabilidades específicas en los sistemas de BN FONDOS.
- Informe de Resultados: Se elaborará un informe detallado de los resultados de las pruebas de penetración, incluyendo recomendaciones de mejora.

Proceso para la Recolección y Análisis de Datos

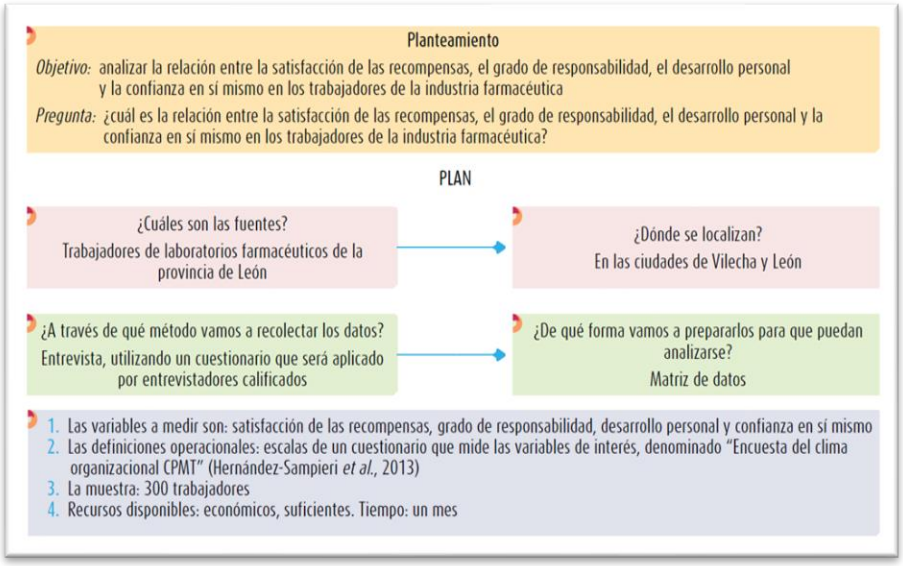
El proceso de la recolección debe estar relacionado con la estrategia definida en la investigación sumado al análisis de datos estos dos elementos permitirán obtener respuestas relevantes a los cuestionamientos planteados, Sampieri (2014) enfatiza que la recolección de datos implica la elaboración de un plan detallado de procedimientos o acciones con un propósito específico, el plan puede desarrollarse tomando en consideración:

- ¿Cuáles son las fuentes de las que se obtendrá la información?
- ¿En dónde se encuentran las fuentes de información?
- ¿Cuál método se empleará para la recolección de datos?
- ¿Cómo se preparará la información para analizarla?
- ¿Cómo analizaremos la información?

El análisis de datos se fundamenta en la forma de trabajar los datos obtenidos para extraer la información que será útil para la investigación y así llegar a tomar decisiones fundamentadas en un resultado.

Figura 11

Plan de Obtención de Datos



Nota. Proceso de Recolección de Datos, tomado de Sampieri (2014)

Diseño del Protocolo de Recolección de Datos

El protocolo de recolección de datos incluirá los procedimientos específicos para llevar a cabo entrevistas, encuestas, auditorías y pruebas de penetración. Este protocolo garantizará la coherencia y validez de los datos recolectados.

Recolección de Datos

- Entrevistas: Se programarán sesiones de entrevistas asegurando la participación voluntaria y el anonimato de los participantes.
- Aplicación de Encuestas: Se enviarán encuestas electrónicas a todo el personal, con un seguimiento para asegurar una alta tasa de respuesta.

- Histórico de Pruebas de Intrusión: se analizará el resultado de las pruebas de penetración efectuadas en los años 2022 y 2023 para validar los grados de afectación que se pueden presentar en BN FONDOS.

Análisis de Datos

- Análisis Cualitativo: Las transcripciones de entrevistas se analizarán utilizando técnicas de codificación y análisis temático para identificar patrones y temas recurrentes.
- Análisis Cuantitativo: Los datos de la encuesta obtenida por medio de la herramienta de Microsoft Form y los resultados de las pruebas de penetración se evaluarán para identificar vulnerabilidades y áreas de mejora.

Integración de Resultados

Los resultados cualitativos y cuantitativos se integrarán para desarrollar un modelo integral de gestión de incidentes y ciber resiliencia. Este modelo considerará tanto las vulnerabilidades técnicas identificadas como las capacidades organizacionales y humanas.

Según Sampieri (2014) explica que posterior a la información obtenida el paso siguiente es ordenas la información según los criterios lógicos asociados al tema de la investigación, el orden puede variar, ya sea cronológicamente, por subtemas, teorías, etc.

Validación del Modelo

El modelo propuesto será revisado y validado con la participación de expertos en ciberseguridad y los responsables de BN FONDOS. Se realizarán ajustes basados en sus comentarios y sugerencias para asegurar la viabilidad y efectividad del modelo.

Consideraciones Éticas

Confidencialidad

Se garantizará la confidencialidad de todos los datos recolectados. Los participantes en entrevistas y encuestas serán informados de que sus respuestas serán tratadas de manera anónima y que los datos se utilizarán exclusivamente para los fines de esta investigación.

Según indica ATLAS.ti (s.f.) menciona que la ética se refiere a las acciones de realizar lo correcto y lo incorrecto por parte de una persona o grupo de personas, por consiguiente, la ética es la norma y directrices que determinan la conducta aceptable en una investigación, garantizando de esta manera la protección, la dignidad y el bienestar de la información tratada. Con respecto a la confidencialidad la determina como el acuerdo que debe existir entre un participante y el investigador sobre cómo tratará, utilizará y difundirá la información obtenida.

Consentimiento Informado

Antes de participar en entrevistas y encuestas, los participantes recibirán una explicación clara del propósito de la investigación y se les solicitará su consentimiento informado.

Con respecto al consentimiento informado, de acuerdo con lo que menciona ATLAS.ti (s.f.) lo define como el proceso de una investigación en que una persona participa voluntariamente en el estudio o investigación en curso tras a ver sido informado detalladamente de los alcances de la investigación. La importancia del consentimiento informado evita el engaño de las personas que participen en la investigación.

Minimización de Riesgos

Se verificarán los resultados históricos obtenidos de las pruebas de penetración efectuadas en los años 2022 y 2023 para validar que vulnerabilidades reflejaron y así brindar recomendaciones para minimizar cualquier riesgo de interrupción de las operaciones de BN FONDOS. Se seguirán procedimientos estrictos para asegurar que las pruebas no comprometan la seguridad o la integridad de los sistemas.

Cronograma de Investigación

Fase 1: Preparación

- Mes 1: Revisión de literatura, planificación detallada del estudio, desarrollo del protocolo de recolección de datos y diseño de instrumentos.

Fase 2: Recolección de Datos

- Mes 2: Realización de entrevistas, encuestas, revisión históricos de penetración.

Fase 3: Análisis y Desarrollo del Modelo

- Mes 2 y 3: Análisis de datos cualitativos y cuantitativos, integración de resultados y desarrollo del modelo de gestión de incidentes y ciber resiliencia.

Fase 4: Validación y Presentación

- Mes 4: Validación del modelo con expertos y ajuste final.
- Mes 5: Redacción y presentación del informe final de la investigación.

Análisis de Benchmarking

Con el objetivo de obtener resultados más exactos a la investigación, se procederá con el análisis del Benchmarking, según Consulting (2023) el objetivo del Benchmarking es lograr comprender y determinar la posición actual de una empresa por medio de reportes de la gestión con relación con las mejores prácticas y así establecer oportunidades de mejora, eficiencia y crecimiento. Según las necesidades y objetivos que se planteen Consulting (2023) menciona las diversas metodologías:

- Benchmarking funcional: se basa en el manejo y la mejora de procesos específicos dentro de una organización, identificando las mejores prácticas, operaciones y funciones posibles.
- Benchmarking operativo: se realiza un análisis para establecer los indicadores generales y específicos de la organización.
- Benchmarking interno: se fundamenta en la parte interna de la organización, su objetivo es identificar y replicar las buenas prácticas de un área en específico.

Los procesos que se deben aplicar en el análisis Benchmarking son:

- Planificación y recopilación de datos: fase inicial en cual se determina la planificación y selección de un método de datos.
- Análisis de datos: análisis que ayudará a establecer tiempos y metas de trabajo.
- Fijación de objetivos: se determinan los objetivos para alcanzar en las distintas áreas de la empresa.

- Establecer un plan de acción: según la información recopilada se establece un plan de cambios en los métodos existentes efectuando al final una evaluación para validar el logro.
- Supervisión del proceso: proceso de mejora continua para validar el éxito del proceso.

Capitulo IV: Análisis de Resultados

Una vez aplicados los instrumentos de recolección de la información, se procedió a realizar el análisis correspondiente para la interpretación de la información obtenida la cual será base fundamental para realizar una propuesta integral de diseño que responda a los requerimientos de BN FONDOS.

Para definir el tamaño de población de la muestra requerida en el siguiente estudio, se aplicó la siguiente fórmula:

Figura 12

Fórmula para calcular la muestra

$$n = \frac{Z^2 pqN}{E^2 x(N-1) + Z^2 xPxq}$$

Nota. Fórmula para calcular la muestra, tomado de INA.

El cálculo de muestra efectuado en BN FONDOS se determinó por medio de los siguientes datos:

Figura 13

Fórmula Población a Encuestar

Encuesta Población BN FONDOS			
Valores para el muestreo		**Resolución**	
Parámetro	**Valor**	Numerador	67,24
N	100	Denominador	1,8703
Z	1,64	**n =**	**36**
p	50,00%		
q	50,00%		
e	11%		

Nota. Elaboración propia, 2024.

El resultado de la formula arroja que de la población total de 100 empleados debe ser aplicada a 36 empleados. Una vez validado este tema, se procedió a aplicar el instrumento obteniendo los resultados que se muestran a continuación.

Análisis de Resultado de la Encuesta

Como parte del proceso de análisis de los datos realizados por medio del cuestionario de la encuesta aplicada se procede a presentar los resultados obtenidos de una muestra de 36 usuarios internos de BN FONDOS los cuales varían según su rol laboral dado que la encuesta fue atendida por personal administrativo, financiero, servicio al cliente, riesgo y calidad, gerentes y personal de tecnología de BN FONDOS.

La información obtenida permite concluir que el personal de BN FONDOS debe conocer y aplicar de una mejor manera los procedimientos establecidos para detectar, prevenir y actuar en caso de una alerta que se pueda materializar en un incidente de ciberseguridad; por lo cual la fuente de información es muy confiable y ejemplifica la necesidad planteada de establecer un

modelo para la mejora en la gestión de respuesta a incidentes y amenazas en ciberseguridad a lo interno en BN FONDOS.

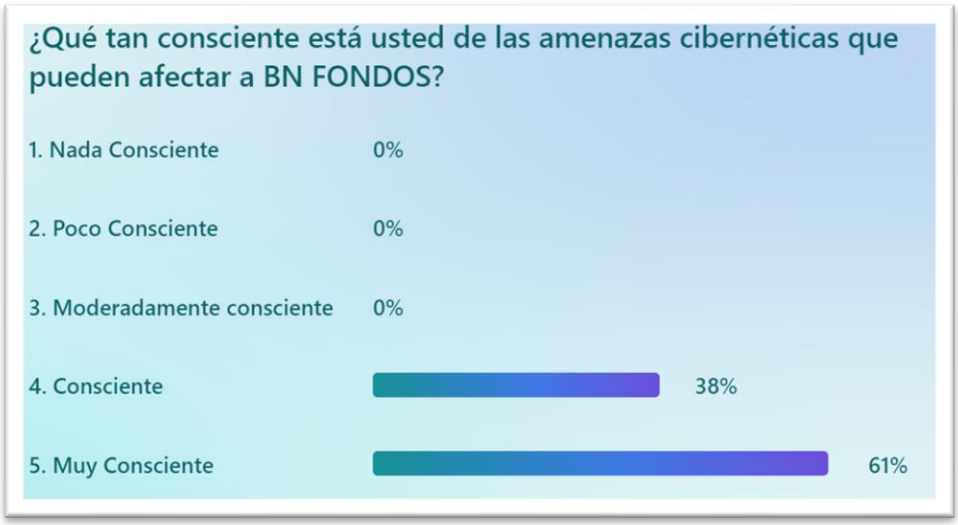
La encuesta se formula con 30 preguntas enfocas en diferentes aristas con el objetivo de identificar las fortalezas y debilidades en el ámbito de la ciberseguridad.

La encuesta plantea preguntas generales en aspectos en ciberseguridad, preguntas que deben ser del conocimiento y dominio del personal en general sin que sea un requerimiento estricto pertenecer al área de tecnología de BN FONDOS.

La pregunta número 1 se enfoca en el conocimiento y la concientización en general que deben tener los colaboradores de BN FONDOS con las amenazas cibernéticas.

Figura 14

Encuesta, Pregunta No 1



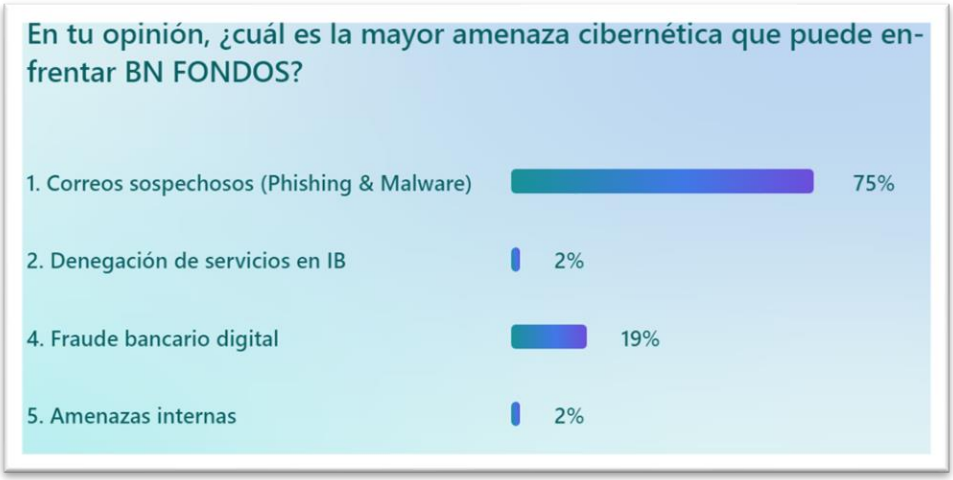
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Se inicia con la opinión de los funcionarios de BN FONDOS sobre la concientización que se debe tener en aspectos de las amenazas cibernéticas, se observa que en términos generales el personal de BN FONDOS si tiene criterio o conocimiento sobre la importancia de las ciberamenazas, las referencias del 38% y 61% muestran que si existe en el personal el criterio de las amenazas cibernéticas.

La segunda pregunta se basa en que los funcionarios, y de acuerdo con su conocimiento y criterio personal, puedan identificar cual sería la mayor amenaza cibernética que puede darse en BN FONDOS.

Figura 15

Encuesta, Pregunta No 2



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

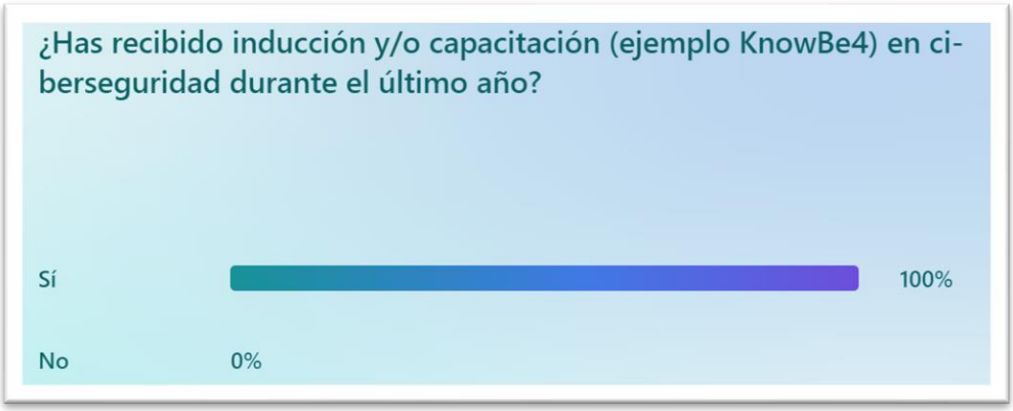
De acuerdo con las respuestas recibidas se logra establecer que la mayor amenaza cibernética, de las 4 opciones presentadas el 75% corresponde a los correos sospechosos (Phishing y Malware) es con el que más se identifican dada la recurrencia que se percibe en el

entorno laboral, como segunda opción resalta el fraude bancario digital con un 19%, un bajo porcentaje del 2% corresponde a la denegación de servicios en IB (Internet Banking) y a las amenazas internas.

El Conglomerado Financiero del Banco Nacional posee un esquema de transferencia del conocimiento en diferentes ámbitos como de leyes, normativas financieras, aspectos generales de tecnología, por lo tanto, la siguiente pregunta pretende evaluar el grado del conocimiento en materia de ciberseguridad.

Figura 16

Encuesta, Pregunta No 3



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

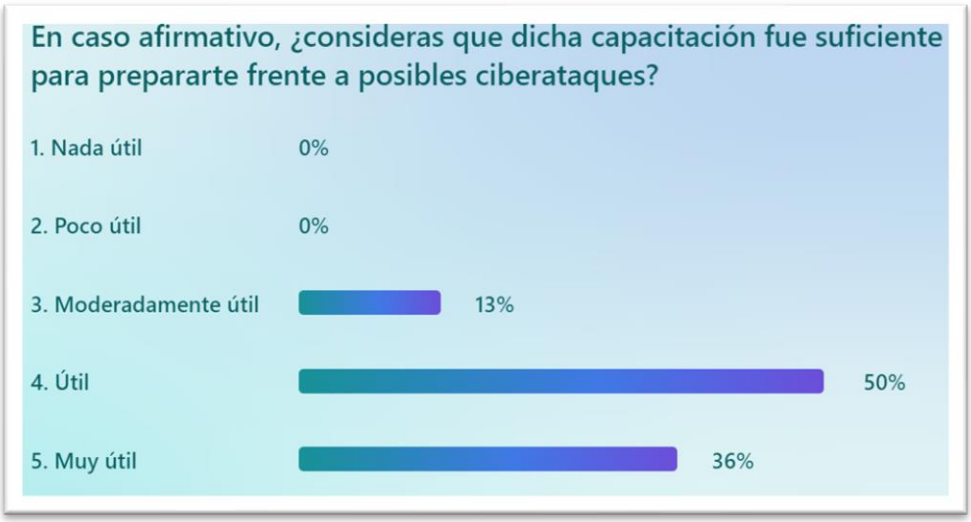
La capacitación es otro elemento clave, el Banco Nacional, promueven campañas de capacitación y concientización en aspectos tecnológicos, el resultado es el esperado al tener el 100% de acuerdo.

Este ambiente abierto a la capacitación valida el criterio sostenido a lo largo del trabajo de investigación sobre la necesidad de incluir en dicho plan una capacitación sobre atención de

incidentes de ciberseguridad con el objetivo de fortalecer el conocimiento y acciones proactivas que puedan desarrollar los funcionarios de BN FONDOS.

Figura 17

Encuesta, Pregunta No 4



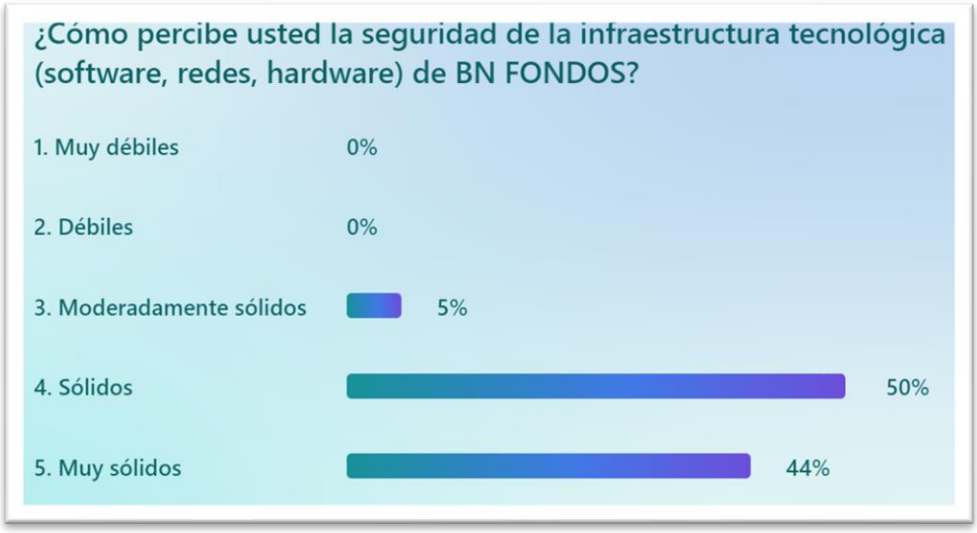
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

El resultado de las capacitaciones recibidas por el personal es variado, teniendo un 50% de útil como el mayor criterio de los funcionarios acerca de la preparación para enfrentar posibles ciberataques, un 36% lo considera muy útil y un 13% moderadamente útil; lo que refleja que se debe trabajar en este aspecto para detectar debilidades en el conocimiento en la ciberseguridad y los ciberataques.

La encuesta se dirigió a personal en general de BN FONDOS (administrativo y técnico), aun así, los funcionarios están en la capacidad de poder responde la pregunta basada en su opinión y criterio de cómo está la seguridad en la infraestructura tecnológica de BN FONDOS.

Figura 18

Encuesta, Pregunta No 5



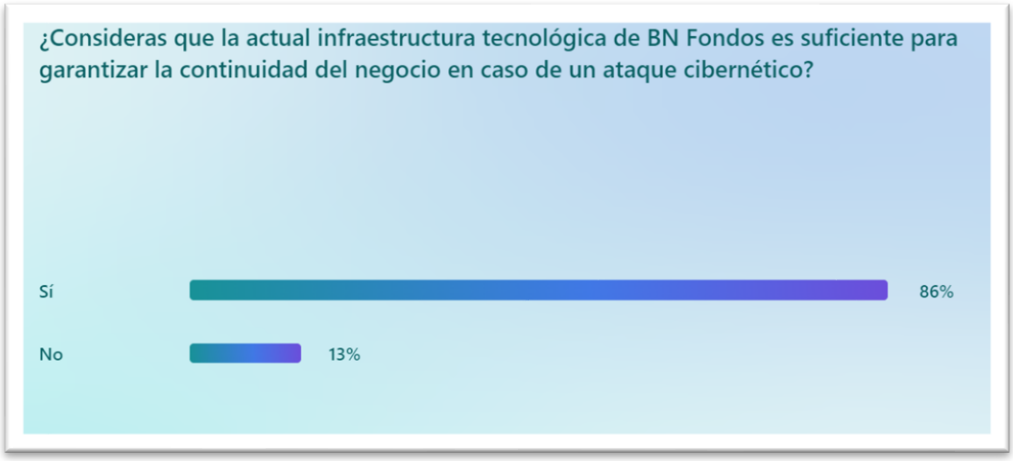
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

La percepción de los funcionarios acerca de la seguridad que pueda tener la infraestructura tecnológica de BN FONDOS es muy variada, un 50% lo considera como sólido, un 44% muy sólidos y un 5% moderadamente sólidos, lo que nos lleva a concluir que el concepto de la protección y seguridad que brinda el área de tecnología en su infraestructura no es unificada para lo cual se debe atender este punto con el personal en general para brindarles un mejor conocimiento.

Según la opinión del encuestado en la pregunta anterior, la siguiente pregunta pretende determinar que el funcionario logre identificar y tener certeza que la Infraestructura Tecnológica de BN FONDOS está preparada para garantizar la continuidad del negocio en caso de un ciberataque.

Figura 19

Encuesta, Pregunta No 6



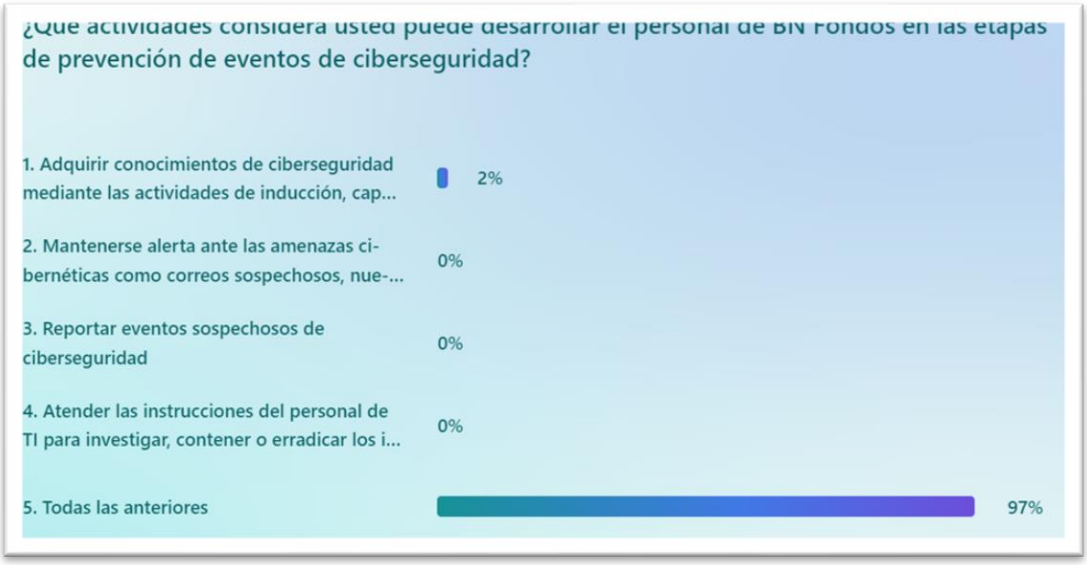
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

El 86% de los funcionarios consideran que, si son suficientes las medidas actuales en BN FONDOS para garantizar la continuidad de los servicios en caso de un ciberataque, contra un 13% que opina negativamente, aun así, es claro que los aspectos en materia de ciberseguridad son un proceso continuo y debe evaluarse periódica estos temas con el personal de BN FONDOS.

La pregunta No 7 formula al funcionario una seria de alternativas o circunstancias que debe identificarlas con certeza para así garantizar que ante un ciberataque BN FONDOS tiene las herramientas necesarias y específicas para actuar sin tener dudas al respecto.

Figura 20

Encuesta, Pregunta No 7



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

La preparación del personal de BN FONDOS en materia de ciberseguridad es clave para la prevención de incidentes, un 98% de los funcionarios indica que todas las actividades mostradas son importantes para tener un buen conocimiento y acción en caso de un ciberataque, por ello se debe atender de manera proactiva por parte de la organización la transferencia del conocimiento de manera regular para que el personal se sienta seguro y capacitado.

El personal de BN FONDOS debe estar preparado para identificar situaciones comprometedoras que puedan llevar a la organización a estar frente a un incidente de ciberseguridad, por tanto, es importante evaluar que los funcionarios de BN FONDOS sepan cómo actuar en caso de un incidente.

Figura 21

Encuesta, Pregunta No 8

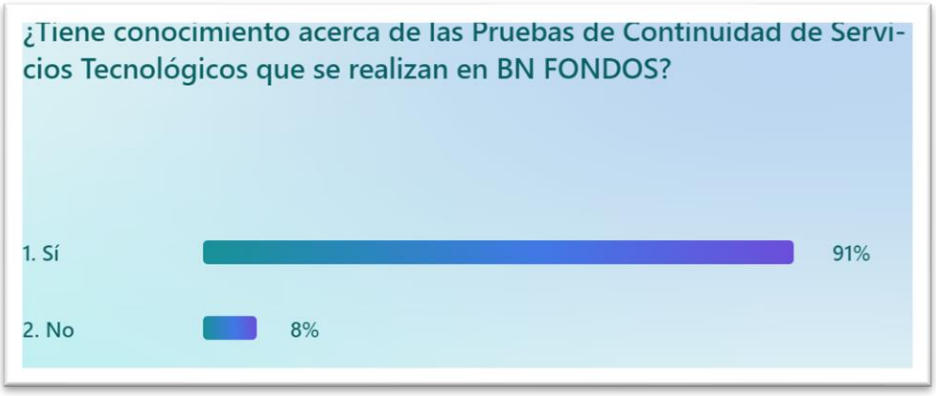
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Los funcionarios de BN FONDOS consideran la importancia de los procedimientos como un guía indispensable para seguir instrucciones en caso de un incidente de ciberseguridad, por lo tanto, se debe trabajar en la definición y claridad de procedimientos enfocados en materia de ciberseguridad.

Las pruebas de continuidad de servicio tecnológicos son pruebas esenciales para garantizar la continuidad de los servicios de BN FONDOS por ello es importante validar si el personal conoce de estas pruebas.

Figura 22

Encuesta, Pregunta No 9



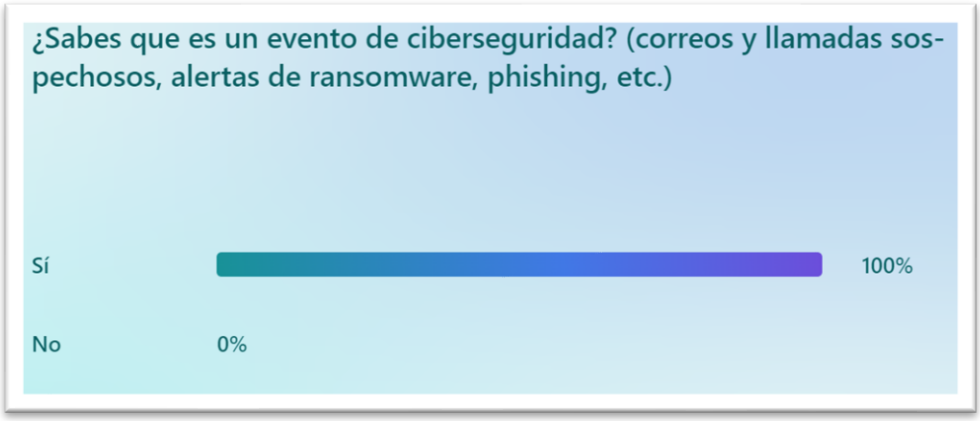
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Un 91% coincide que tienen conocimiento de las pruebas la continuidad del negocio, lo cual conlleva en mantener y reforzar este este esquema de pruebas en la organización para garantizar la confianza y seguridad de acciones en caso de presentarse un incidente en ciberseguridad.

Como parte de las campañas que se promueven en BN FONDOS son los conceptos de los eventos de ciberseguridad que existen hoy en día, por ello es necesario e importante determinar por medio de esta pregunta si los funcionarios tienen claridad al respecto de los eventos que se pueden presentar.

Figura 23

Encuesta, Pregunta No 10



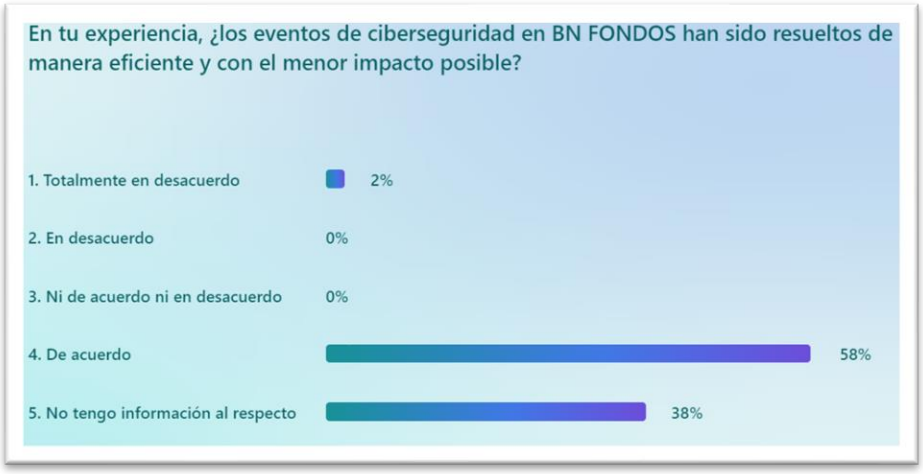
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Recurrentemente el Banco Nacional y BN FONDOS realizan campañas principalmente por correo electrónico sobre conceptos claves en materia de ciberseguridad, la muestra del 100% garantiza el conocimiento del concepto de un evento en ciberseguridad dentro del personal de BN FONDOS.

A nivel del Conglomerado Financiero del Banco Nacional la información de eventos o alertas informativas que se han presentado, pero no han llegado a materializarse como un incidente de ciberseguridad, son comunicados al personal, por ende, la consulta acerca de que si las atenciones y resoluciones han sido oportunas es vital para determinar si realmente entienden estos comunicados emitidos a lo interno.

Figura 24

Encuesta, Pregunta No 11



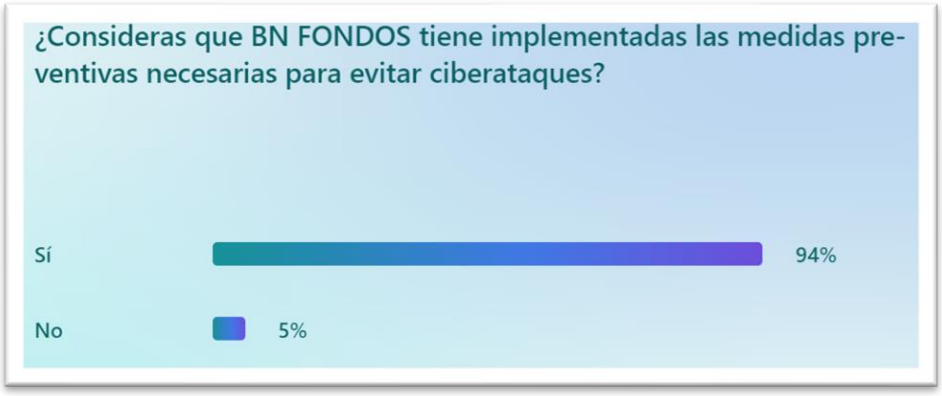
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Ante la experiencia sobre la atención de eventos de ciberseguridad sobresale un 2% que están totalmente en desacuerdo, un 58% opina que está de acuerdo y un 38% indica que no tiene información al respecto, lo que indica que se debe hacer un reforzamiento en la comunicación ya que actualmente BN FONDOS no ha sido afectado por eventos que pongan en riesgo la operativa del negocio.

La pregunta No 12 es clave para determinar si los funcionarios tienen claridad acerca de las medidas preventivas que se promueven por medio de las campañas de ciberseguridad.

Figura 25

Encuesta, Pregunta No 12



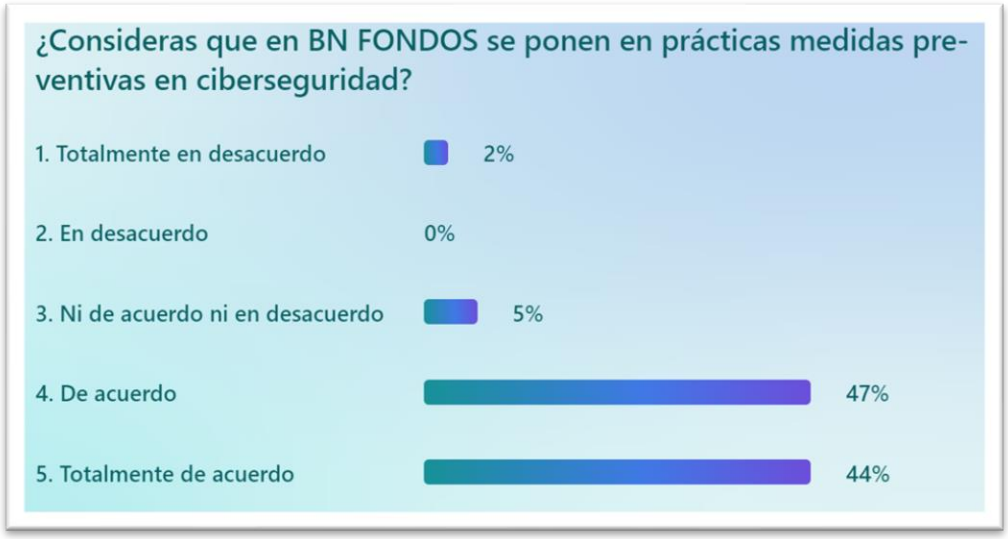
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

El conocimiento acerca de las medidas de prevención se evalúa, el resultado del 94% refleja que los funcionarios si tienen claridad sobre implementaciones tecnológicas y procedimientos que existen actualmente en BN FONDOS y que pueden ayudar en evitar ciberataques.

La siguiente pregunta se correlaciona con la anterior ya que, si el funcionario logra determinar que, si existen medidas preventivas para evitar ciberataques, perfectamente puede establecer en algún grado que si existen medidas prácticas preventivas en ciberseguridad.

Figura 26

Encuesta, Pregunta No 13



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

En cuanto al conocimiento sobre las prácticas preventivas en ciberseguridad la encuesta arrojo criterios muy diferentes y que llaman la atención, por ejemplo, un 2% está totalmente en desacuerdo y un 5% se encuentra en un punto intermedio (ni de acuerdo ni en desacuerdo), el resto del personal encuestado se divide en un 47% de acuerdo y un 44% en totalmente de acuerdo, por lo tanto, este es un tema que se debe reforzar con el personal de BN FONDOS.

Por las campañas que se promueven a lo interno el funcionario puede establecer en cierta medida que grado de preparación tiene el personal para detectar y reportar actividades sospechosas.

Figura 27

Encuesta, Pregunta No 14

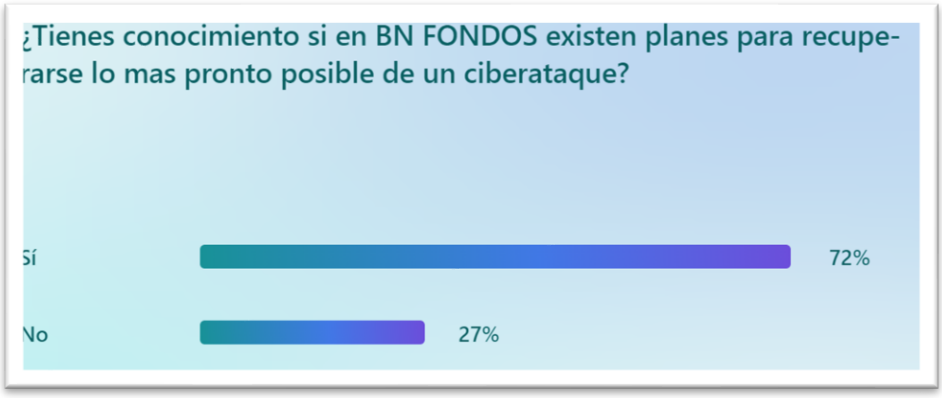
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

A pesar de existir campañas en ciberseguridad el 72% considera estar preparado para detectar y reportar actividades sospechosas, un 5% muy preparado pero un 22% menciona estar moderadamente preparado.

En los procedimientos internos de BN FONDOS existen planes de recuperación ante ciberataques, la pregunta No 15 es importante porque puede reflejar un desconocimiento de estos planes.

Figura 28

Encuesta, Pregunta No 15



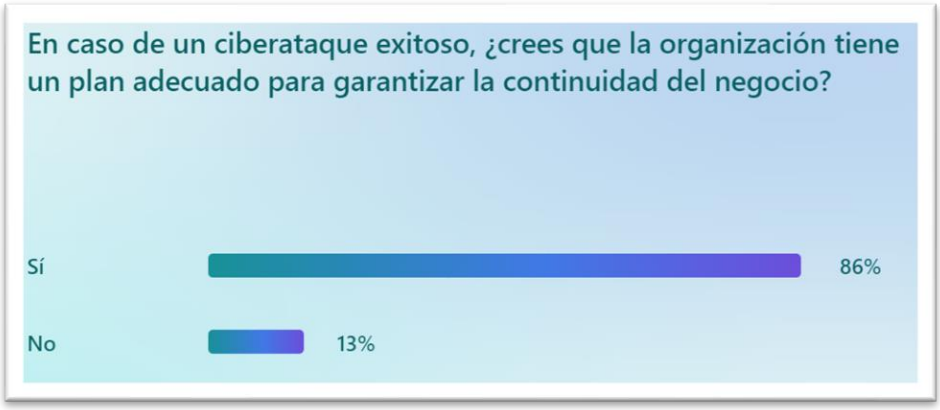
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

En cuestión de la aplicación de planes de recuperación, se tiene que un 72% de los funcionarios encuestados si tienen conocimiento sobre planes de recuperación contra un 27% que indica que no tiene conocimiento; este es otro punto de recomendación para reforzar con el personal de BN FONDOS.

El Conglomerado Financiero del Banco Nacional promueve planes para garantizar la continuidad del negocio, ya sea del banco, así como de las sociedades, en este caso BN FONDOS, por ello el personal debe tener el conocimiento de la existencia de estos planes.

Figura 29

Encuesta, Pregunta No 16



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Ante un ciberataque exitoso o que se materialice el 86% considera que la organización si tiene un plan adecuado para garantizar la continuidad del negocio contra un 13% que indica que no, tema que se debe reforzar con el personal de BN FONDOS.

La imagen de las empresas hoy en día puede verse afectadas por los ciberataques, por ello es importante determinar cuál es conocimiento que existe en el personal de BN FONDOS acerca de las medidas que existen para proteger la reputación de la sociedad.

Figura 30

Encuesta, Pregunta No 17

Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Bien es conocido que la reputación de una organización es muy importante mantenerla intachable, según los encuestados el 58% se siente seguro y un 27% se siente muy seguro ante las medidas que BN FONDOS tenga establecidas ante un ciberataque, aun así, un 13% se siente moderadamente seguro, resultado que promueve a mejorar el concepto de la reputación.

La parte financiera es clave para proveer recursos humanos y técnicos para fortalecer las medidas de ciberseguridad, es vital determinar si el personal de BN FONDOS conoce o tiene criterio de los presupuestos e inversiones que tienen disponibilidad el área técnica para brindar seguridad a la infraestructura tecnológica.

Figura 31

Encuesta, Pregunta No 18

Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Para los encuestados el 44% considera que, si están de acuerdo en que BN FONDOS reserva recursos financieros para la gestión de incidentes y ciber resiliencia, se refuerza con un 38% que están totalmente de acuerdo y un 16% menciona que ni de acuerdo ni en desacuerdo, por lo tanto, este alcance se debe mejorar dentro del personal de BN FONDOS.

Las capacitaciones son esenciales para brindar un mejor conocimiento a funcionario, acción que debe venir de parte de BN FONDOS, por lo tanto, la pregunta acerca de la frecuencia de las capacitaciones es clave para determinar si el conocimiento a hoy que tiene en personal en la ciberseguridad y los ciberataques es ideal o debe fortalecerse.

Figura 32

Encuesta, Pregunta No 19

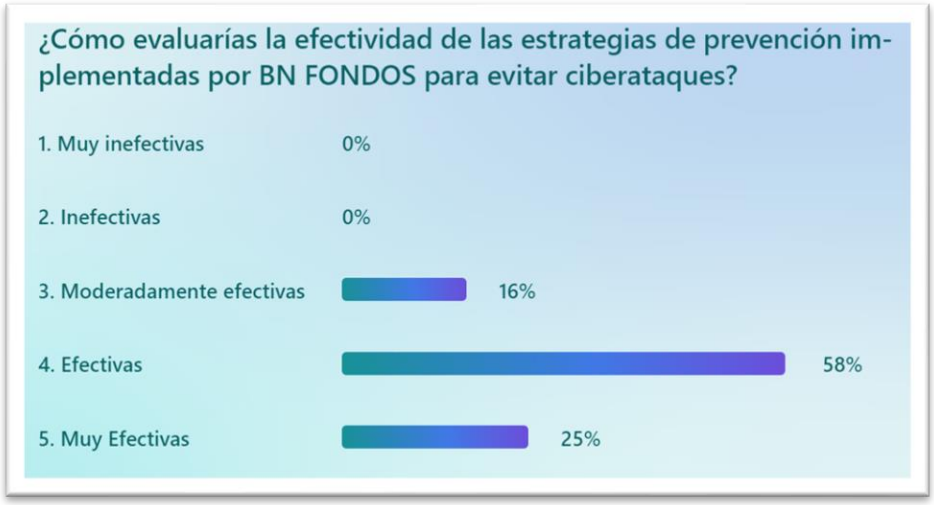
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Un 83% de los funcionarios de BN FONDOS ven como una medida de mejora en los conocimientos en ciberseguridad aumentar las capacitaciones contra un 16% que indica que no es necesario, pero dada la importancia de este tema si clave el reforzamiento de las capacitaciones.

Las inducciones, las autocapacitaciones, las pruebas de continuidad de los servicios tecnológicos, entre otros, deben ser evaluadas por el personal encuestado, así se puede concluir si realmente son estrategias efectivas o bien requieren algún cambio de mejora.

Figura 33

Encuesta, Pregunta No 20



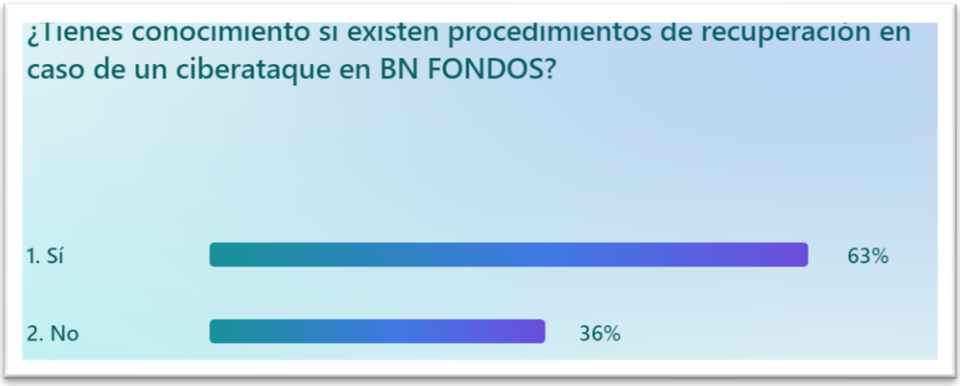
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

El 58% de los encuestados consideran efectivas las medidas preventivas que hoy en día se tienen establecidas en BN FONDOS, un16% lo consideran moderadamente efectivas y un 25% muy efectivas, el resultado se puede considerar satisfactorio.

La pregunta No 21 es muy estratégica para determinar si el personal conoce de los procedimientos de recuperación ante un ciberataque o bien si en las charlas de refrescamiento se deben de mencionar.

Figura 34

Encuesta, Pregunta No 21



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

A pesar de existir en BN FONDOS campañas de ciberseguridad se detecta que un 36% de los encuestados desconocen de los procedimientos de recuperación que están definidos para casos de ciberataques, solo un 63% indican qué si existen procedimientos, este resultado muestra que debe hacer un reforzamiento con este tema.

Las campañas que promueven la ciberseguridad contemplan el flujo o canales de comunicaciones en caso de un incidente, dado lo anterior, en vital evaluar este alcance entre los funcionarios de BN FONDOS.

Figura 35

Encuesta, Pregunta No 22

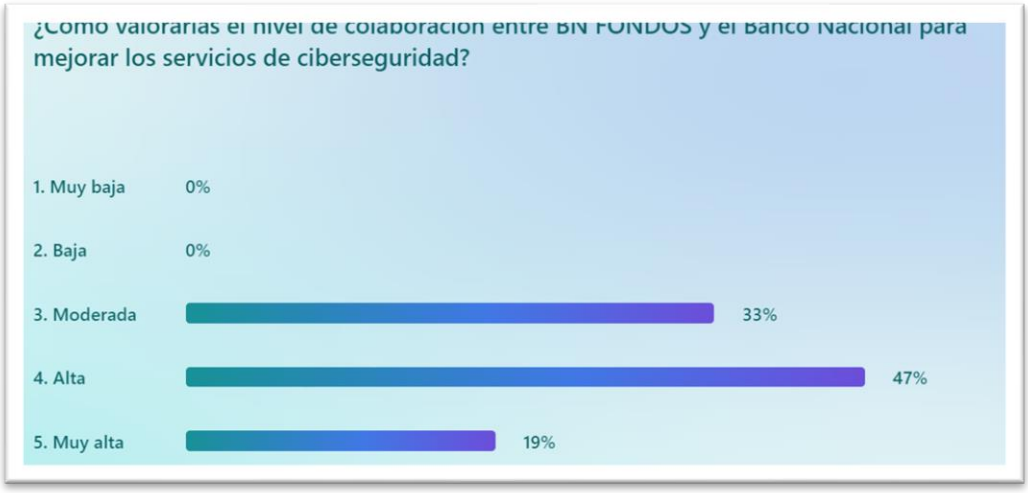
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Las campañas de ciberseguridad que se practican en BN FONDOS son con el objetivo de que el personal conozca los diferentes medios de comunicación para la atención de eventos de ciberseguridad, de los encuestados un 69% si conoce estos medios, contra un 30% que indica que no, este resultado si es muy preocupante y se debe atender con prioridad.

El concepto del Conglomerado Financiero del Banco Nacional es mostrar la integración del Banco Nacional con las diferentes Sociedades Anónimas, en nuestro caso BN FONDOS, ya sea en alcances administrativos, de compras, financieros e igualmente técnicos, por lo tanto, los funcionarios deben tener claridad de la colaboración y servicios que ofrece la casa matriz con BN FONDOS en servicios de ciberseguridad.

Figura 36

Encuesta, Pregunta No 23



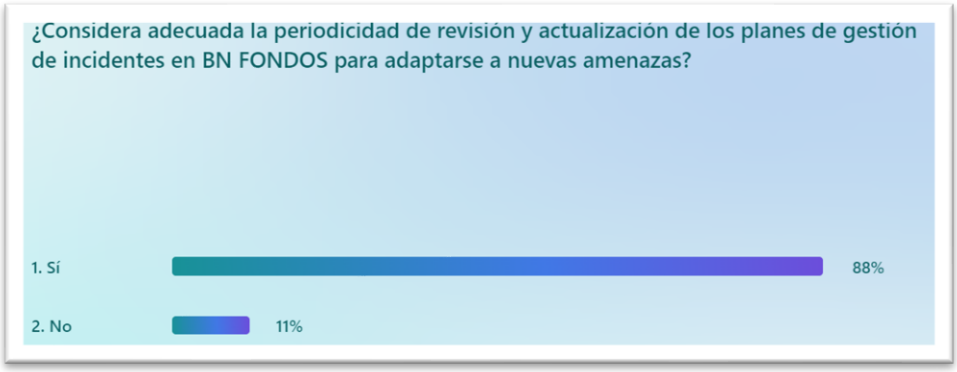
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

El Banco Nacional trabaja en constante comunicación y colaboración con las Sociedades Anónimas para mantener una estandarización en las normas y procedimientos en materia de ciberseguridad, de los encuestados se determina que un 47% la considera como alta, un 33% como moderada y un 19% muy alta, para efectos de esta encuesta se puede dar como satisfactoria las respuestas recibidas.

En BN FONDOS la revisión y actualización de procedimientos, controles, registros, entre otros, es constante, ya sea por una acción proactiva o por alguna circunstancia del momento, por lo tanto, el criterio del personal es importante para conocer qué grado consideran la revisión y actualización de los controles en materia de ciberseguridad para estas actualizados ante las ciberamenazas.

Figura 37

Encuesta, Pregunta No 24



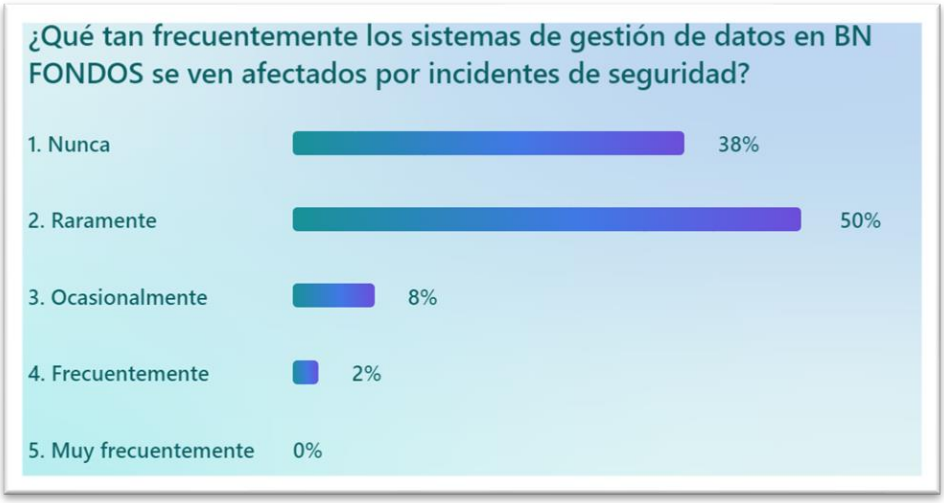
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Dados planes de revisión y actualización de procedimientos que existen en BN FONDOS un 88% considera que si existe una adecuada periodicidad en la revisión de los planes de incidentes contra un 11% que considera que no.

Las afectaciones o interrupciones de los servicios de BN FONDOS son importantes de evaluar para establecer una mejora oportuna ante incidentes de ciberseguridad.

Figura 38

Encuesta, Pregunta No 25



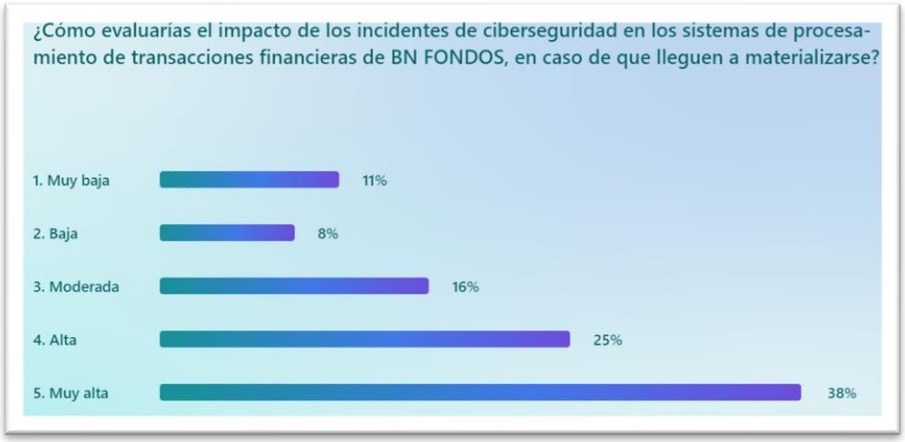
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Aunque los sistemas de BN FONDOS no han sido significativamente afectados por incidentes de ciberseguridad, según lo reflejado por el 38% de los encuestados que afirman que nunca se han visto comprometidos, llama la atención que el 50% indica que raramente han enfrentado problemas, el 8% menciona que esto ocurre ocasionalmente y un 2% afirma que sucede muy frecuentemente. Es crucial prestar atención a estos resultados, ya que podrían estar confundiendo otros eventos del servicio con incidentes de ciberseguridad.

Dado este panorama, es necesario contar con mecanismos sólidos de atención de incidentes y fortalecer la ciberresiliencia en BN FONDOS, para asegurar una respuesta eficiente en caso de que se materialice un ciberataque. Además, es fundamental evaluar si el personal comprende el impacto financiero que un incidente de ciberseguridad podría generar, lo que será abordado en la siguiente pregunta.

Figura 39

Encuesta, Pregunta No 26



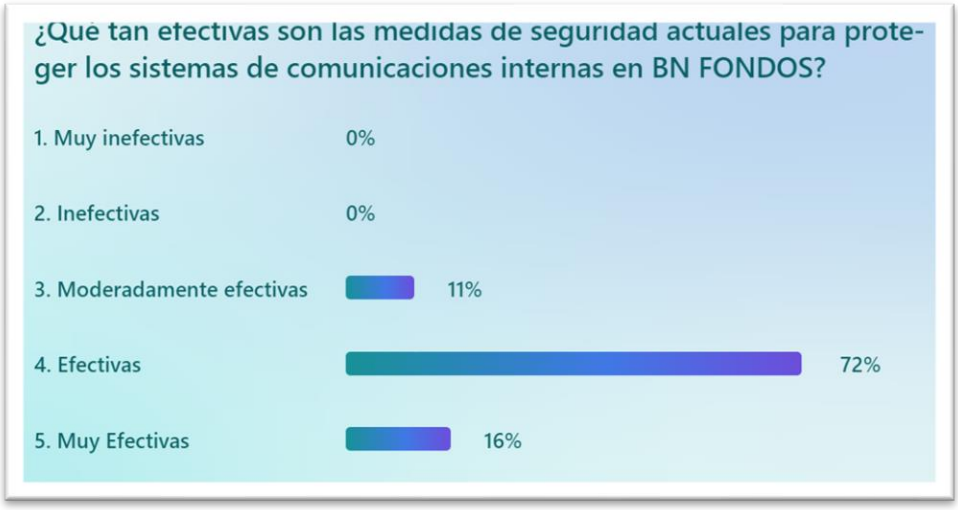
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

A pesar de las campañas de inducción y la concientización que existe con los ciberataques se detectan diferentes porcentajes, 11% muy baja, 8% baja, 16% moderada, un 25% alta y un 38% muy alta, la diversidad de respuestas muestra que se debe reforzar el impacto que puede provocar un incidente en ciberseguridad en BN FONDOS.

La siguiente pregunta pretende reflejar el conocimiento que tenga el personal con las medidas de seguridad actuales que brindan protección a los sistemas internos en BN FONDOS.

Figura 40

Encuesta, Pregunta No 27



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Un 72% de los encuestado considera como efectivas las medidas de seguridad actuales en BN FONDOS, un 11% como moderadamente efectivas y un 16% muy efectivas, las respuestas recibidas se pueden dar como satisfactorias.

La plataforma tecnológica de BN FONDOS posee un sistema de respaldo y recuperación, la cual permite al negocio una recuperación en un tiempo máximo de recuperación que permita continuar con los servicios del negocio lo más pronto posible, por lo tanto, esta pregunta es interesante para determinar el conocimiento del personal con este sistema de respaldo y recuperación.

Figura 41

Encuesta, Pregunta No 28

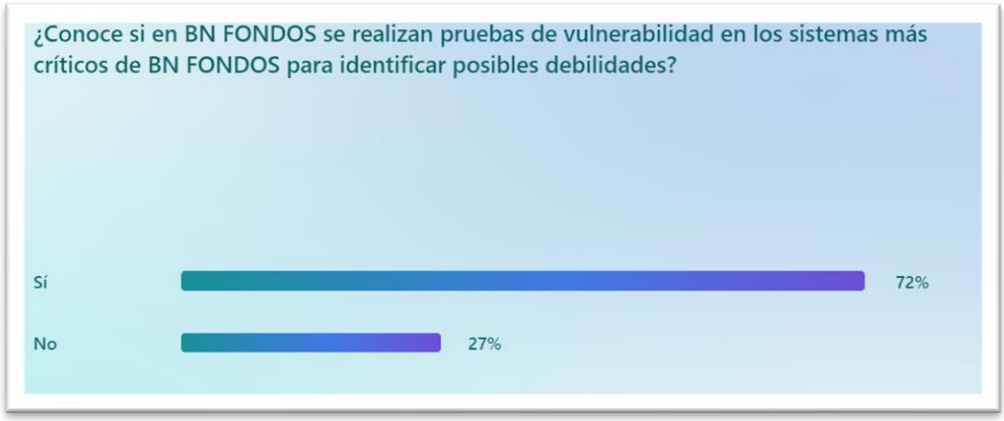
Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

En BN FONDOS existe un sistema de respaldo y recuperación de datos, que garantiza la información intacta ante un ciberataque, el 55% de los encuestados los considera sólido y un 36% muy sólido y un 8% moderadamente muy sólido, las respuestas recibidas se pueden dar por satisfactorias.

BN FONDOS posee un plan de anual de pruebas de vulnerabilidades (pruebas de intrusión) las cuales ponen a pruebas los sistemas de protección ante ciberataques, por lo tanto, la siguiente pregunta permitirá validar el grado de conocimiento que existe en el personal con estas pruebas y su alcance real.

Figura 42

Encuesta, Pregunta No 29



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Por medio de las campañas que emite BN FONDOS al personal en general si se logra detectar que un 72% de los encuestados conocen de las pruebas de vulnerabilidades y un 27% indica que no lo conocen, lo cual nos permite concluir que se debe mejorar este conocimiento al personal de BN FONDOS.

La última pregunta es de libre comentario, el objetivo es escuchar las propuestas de mejoras que los funcionarios consideren ideales para la mejora continua y así fortalecer las gestiones de ciberseguridad y ciberataques.

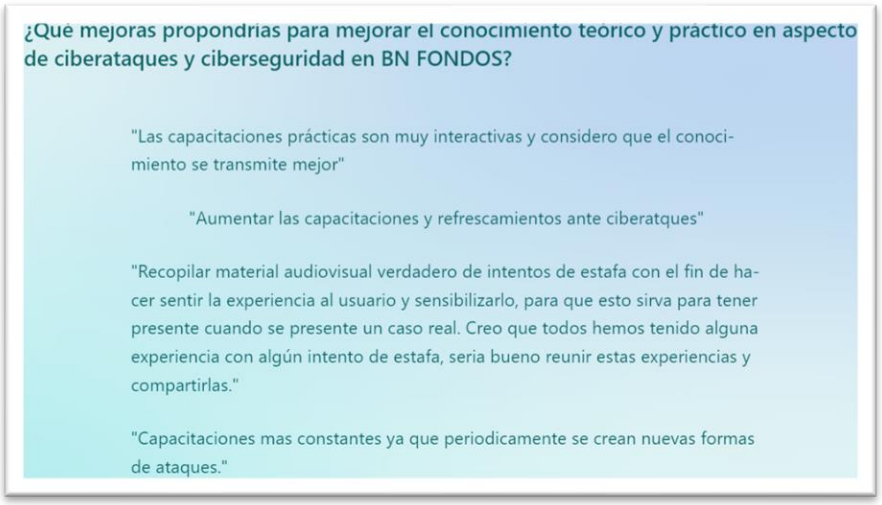
Figura 43

Encuesta, Pregunta No 30

Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 44

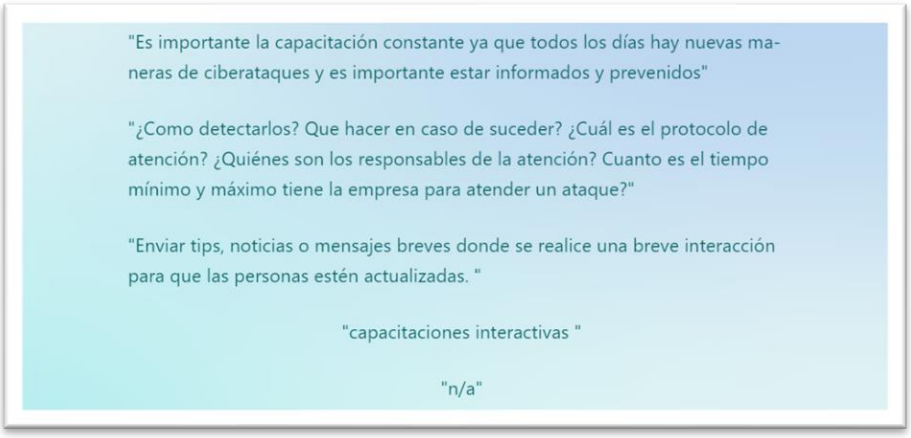
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, mediante los datos obtenidos de la encuesta.

Figura 45

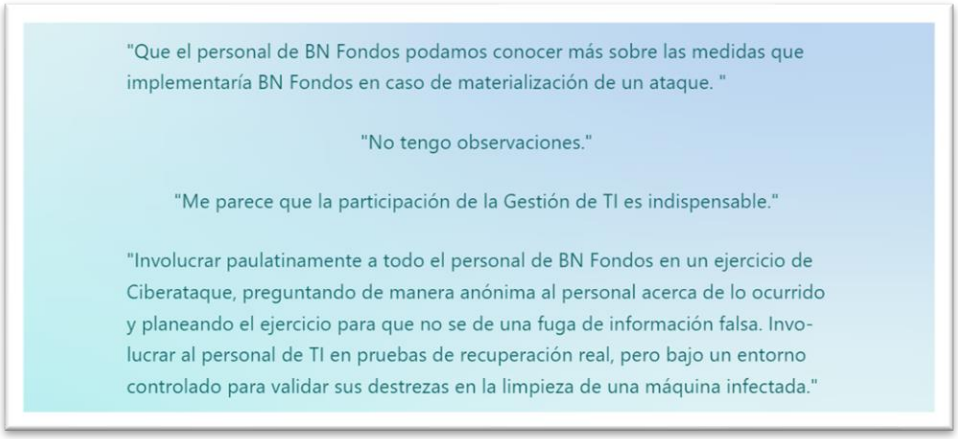
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 46

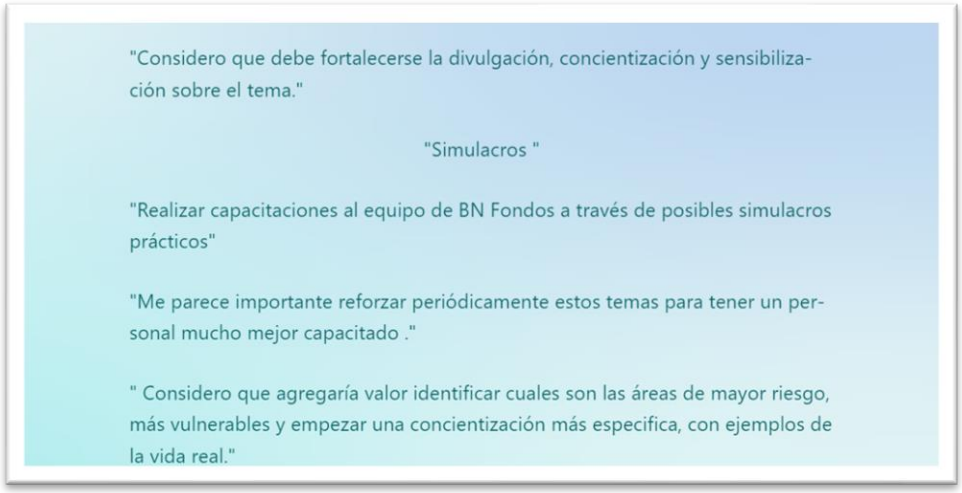
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 47

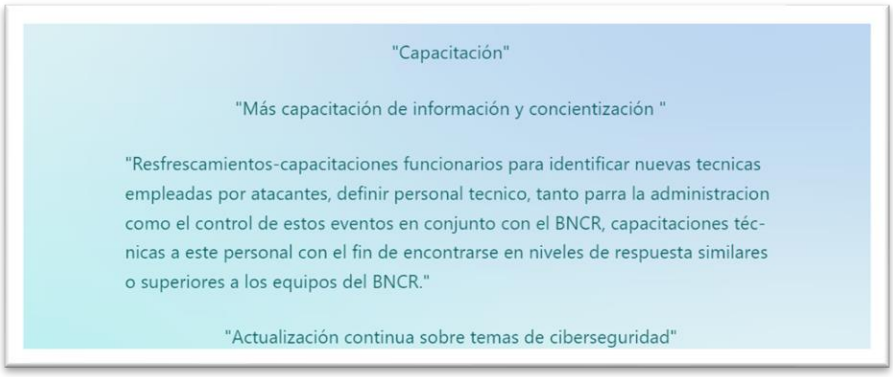
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 48

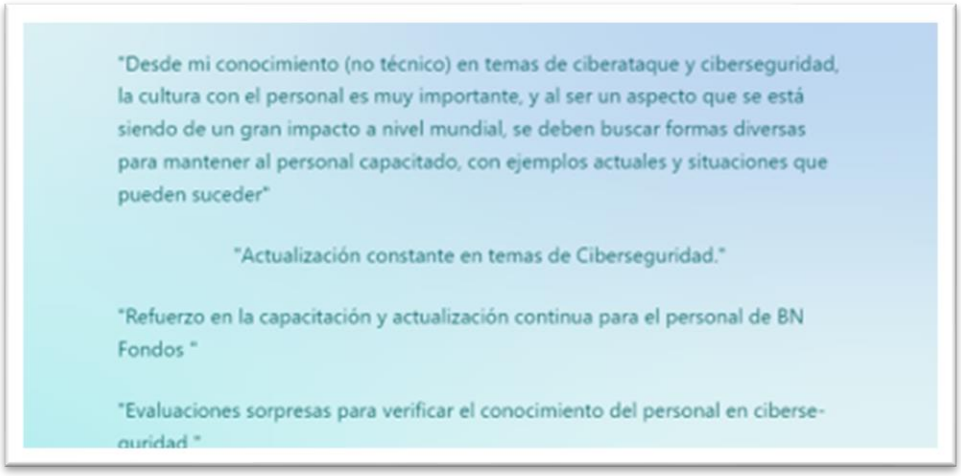
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 49

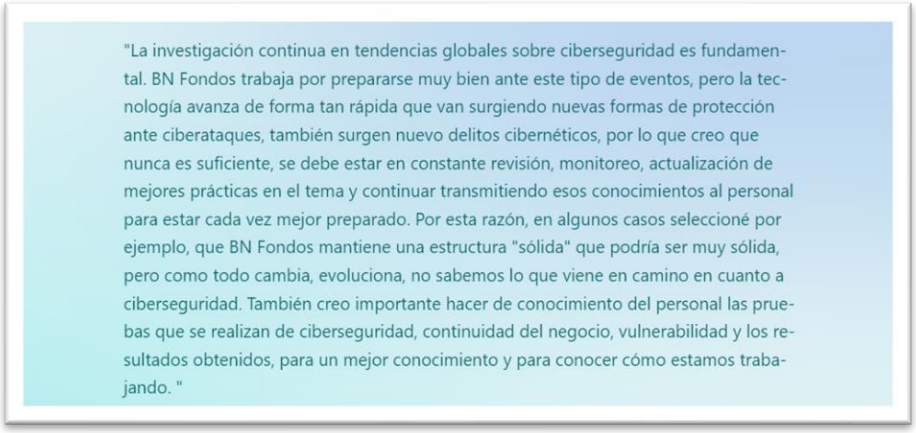
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 50

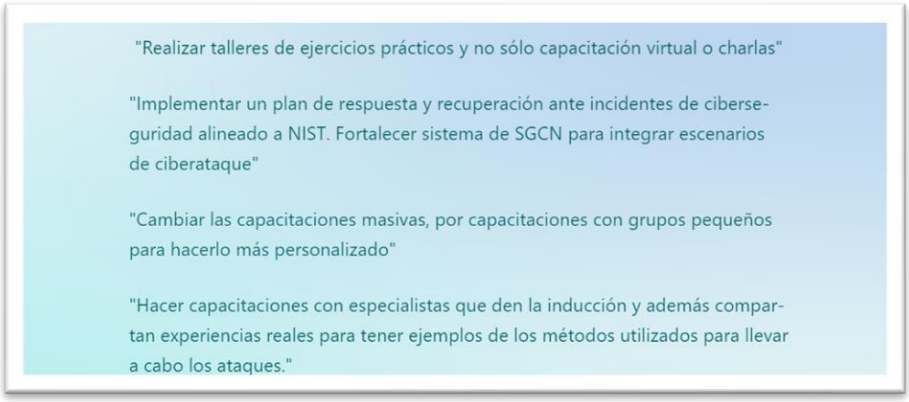
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 51

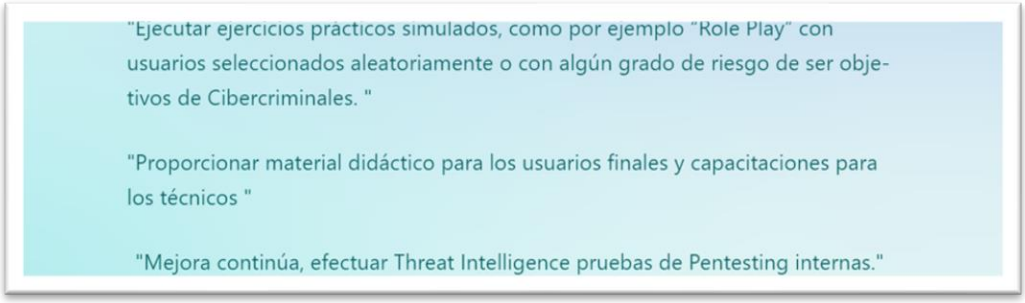
Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, datos obtenidos de la encuesta.

Figura 52

Encuesta, Pregunta No 30



Nota. Elaboración propia, 2024, mediante los datos obtenidos de la encuesta.

Ante la última pregunta, se detecta que las capacitaciones continuas, los simulacros, los ejercicios prácticos son los puntos que el personal encuestado considera de mayor importancia para mejorar el conocimiento y prevención en el área de la ciberseguridad.

Análisis de Resultados de las Entrevistas

Con respecto a los datos recaudados de la entrevista uno (1) realizada a la funcionaria encargada de la Seguridad de la Información de BN FONDOS, indica que hoy en día los ciberataques a nivel mundial se consideran una situación nefasta, la cual crece exponencialmente con el tiempo y a la vez incrementa el nivel de complejidad y especialización en los sistemas de tecnología. A nivel nacional considera que por lo menos ya se ha empezado a conocer del tema a y esto incremento a raíz de los ataques del 2022 y eso ha implicado que las empresas, instituciones y personas tomen un poco más de responsabilidad para atender estas eventualidades. Sin embargo, es del criterio que falta mucha madurez en el manejo e inyección de recursos.

Con respecto a normativa internacionales como lo es el marco NIST, determina que es un aporte muy importante del Gobierno de Estados Unidos, ya que reúne una serie de buenas prácticas que sirven de referencia a la industria tecnológica, dado su alto nivel de aplicabilidad y funcionalidad. Por conocimiento personal considera que el marco de ciberseguridad brinda una guía muy práctica y objetiva para la prevención, atención y aprendizaje de los incidentes de ciberseguridad. Igualmente opina que por los eventos presentados en Costa Rica en las instituciones públicas estas si han mejorado las gestiones de respuesta a incidentes y amenazas en ciberseguridad.

A nivel del Conglomerado Financiero del Banco Nacional se determina que, si cuenta con personal calificado, herramientas de descubrimiento y correlación de eventos, capacitaciones y se encuentra implementando marcos normativos que reúnen buenas prácticas de la industria con el objetivo de prevenir y detectar a tiempo ciberataques, estas acciones que el banco ha determinado se fortalece por que se han acatado las mejoras prácticas para evitar en la medida de lo posible ciberataques, por ejemplo, ejercicios de identificación de vulnerabilidades, pruebas de penetración, el seguimiento a la solución de las vulnerabilidades detectadas, capacitación al personal, inversión en tecnología de ciber protección, etc.

Finalmente opina que el conocimiento en general de los funcionarios del Conglomerado Financiero del Banco Nacional acerca de la ciberseguridad, las consecuencias de los ataques y el impacto que puede traer esto al core de negocio bancario es entre medio y alto en BN FONDOS y en el Conglomerado Financiero del Banco Nacional, entre bajo y medio.

La segunda entrevista se efectuó al encargado de Ciberseguridad de la Dirección de Operaciones y Servicios Tecnológicos del Banco Nacional de Costa Rica, opina que los ataques a nivel mundial lastimosamente constituyen una amenaza creciente debido a la efectividad que han tenido en los últimos años, tanto así que hoy el Negocio de la Ciberdelincuencia representa una fuerte economía mundial, si mal no recuerda, se proyecta a ser la tercera a nivel global antes de finalizar esta década, por lo tanto, existe mucho trabajo por hacer para revertir esta situación.

Con respecto a nivel nacional considera durante los últimos años, y principalmente después de las lamentables actuaciones de los grupos cibercriminales Conti y Hive contra Instituciones Públicas, se han hecho muchos esfuerzos en conjunto con diversas instituciones públicas y privadas para mejorar la respuesta ante incidentes, no obstante, el trabajo no está concluido, por otra parte, la dinámica de amenazas nos lleva a enfrentarnos a novedosos métodos

de ataque día a día, por lo que los planes de contingencia que funcionaban en el pasado, expiran continuamente lo que obliga a los equipos de respuesta a incidentes a desarrollar e implementar nuevas estrategias de defensa.

Referente al marco regulatorio NIST, menciona que este marco exige al cumplimiento de determinadas mejores prácticas de Ciberseguridad a Instituciones Públicas en Estados Unidos, y es una excelente referencia para establecer un Sistema de Seguridad de la Información en cualquier organización con enfoque en la mitigación de riesgos, tiene la ventaja de ser accedido sin restricción.

Con respecto a las mejoras en las instituciones públicas ante gestiones de respuesta a incidentes y amenazas en ciberseguridad opina que sí se han hecho grandes avances; si nos comparamos con otras latitudes en las que el tema de ciberseguridad es parte de la agenda pública desde hace muchos años y que realizan una inversión muy importante cada año en formación, investigación y colaboración, en nuestro entorno nos falta bastante para estar a ese nivel, sin embargo, recientemente se ha logrado culturizar el tema en Costa Rica, se ha empezado a hablar un mismo idioma, así como se ha mejorado la concientización de los usuarios de tecnología acerca de las amenazas en ciberseguridad, asimismo se ha empezado a fortalecer la legislación al respecto, entre otros grandes avances que finalmente repercuten en estar mejor preparados para una respuesta cada vez más resiliente ante incidentes.

Para que el Conglomerado Financiero del Banco Nacional pueda estar al día con las nuevas técnicas de los ciberdelincuentes, menciona que el Banco Nacional utiliza diferentes fuentes de apoyo como informes de CISA (Certified Information Systems Auditor), INCIBE (Instituto Nacional de Ciberseguridad de España) y MICITT (Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones). Además, investiga y toma como referencias blogs de

organizaciones privadas dedicadas a la auditoría e investigación como: KPMG, Deloitte IBMXForce, AllienVault, VirusTotal, AnyRun, Malwarebytes, entre otras.

A nivel del Conglomerado Financiero del Banco Nacional se considera que se ha hecho un enorme esfuerzo por adoptar mejores prácticas en la prestación de servicios, hasta el día se ha logrado mantener una postura de seguridad que nos permite atender eventos con una buena eficiencia de resolución, sin embargo, hay mucho más por hacer, a la lista de tareas, día a día se suman amenazas emergentes que suelen ser muy diferentes a las anteriores, por lo que la adopción de mejores prácticas no podría definirse como un proyecto que tiene un inicio y un final, sino como un proceso cíclico y evolutivo en el que es necesario mejorar continuamente.

Acerca del conocimiento en general de los funcionarios del Conglomerado Financiero del Banco Nacional, en su opinión, considera que el Banco ha logrado mejorar muchísimo la especialización de los colaboradores que se dedican a seguridad, sin embargo, este también es un proceso cíclico que se ve afectado por factores como: la rotación de personal, curvas de aprendizaje, las amenazas emergentes y la evolución tecnológica, además, la necesidad creciente de tener personal más especializado en diversas ramas de la ciberseguridad dentro de la institución supone todo un reto. Personalmente cree que se está haciendo todo lo posible, para identificar las brechas y subsanarlas.

En relación con las consecuencias, y el impacto en caso de materializarse un riesgo de ataque, depende mucho del tipo de ataque que se logre concretar, es un tanto complejo brindar una única respuesta, las instituciones más seguras atienden varios miles o millones de ataques al año, por lo que la preparación no evita que una organización sea atacada, sino ayuda a mejorar la forma en la que se resiste, es decir, identificar, contener y responder a los ataques a tiempo y en etapas tempranas es muy importante para que el impacto no pase a mayores.

Análisis de Resultados de las Pruebas de Penetración

BN FONDOS ha realizado pruebas anuales en los años 2022 y 2023, las pruebas realizadas y sus resultados son:

Pruebas de Intrusión Interna: el objetivo de estas pruebas es poder evaluar si un intruso pudiera llegar a ingresar a recursos y servicios tecnológicos internos de la infraestructura de BN FONDOS, la prueba se fundamenta en ataques y accesos controlados dentro de la red de BN FONDOS, se pone en cuestionamiento la administración de las redes, identificación, autenticación, confidencialidad, integridad y controles de configuración.

Figura 53

Pruebas Intrusión Internas 2022

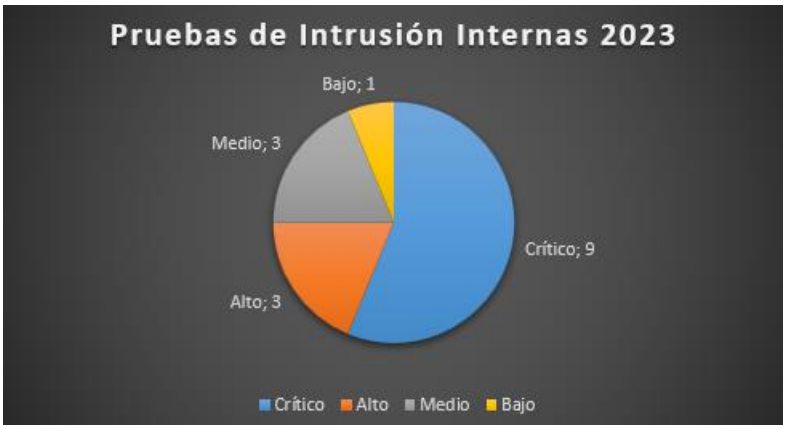
Nota. Elaboración propia, 2024, datos obtenidos de las pruebas de penetración.

Los resultados del periodo 2022 fueron clave para determinar una serie de protocolos y atenciones en la infraestructura de BN FONDOS, la prueba deparó un total de 18 hallazgos, 8 clasificados como críticos, 3 en grado alto, 7 en grado medio y 0 en nivel bajo, la calificación final de acuerdo con los hallazgos fue de un riesgo crítico; lo cual generó la atención inmediata

de los hallazgos en el orden de criticidad con el fin de cerrar en un medio a largo plazo las vulnerabilidades detectadas.

Figura 54

Pruebas Intrusión Internas 2023



Nota. Elaboración propia, 2024, datos obtenidos de las pruebas de penetración.

Los resultados del periodo 2023 fueron muy similares al año 2022, igualmente se determinar una serie de protocolos y atenciones en la infraestructura de BN FONDOS, la prueba deparó un total de 16 hallazgos, 9 clasificados como críticos, 3 en grado alto, 3 en grado medio y 1 en nivel bajo, la calificación final de acuerdo con los hallazgos fue de un riesgo crítico; lo cual generó la atención inmediata de los hallazgos en el orden de criticidad con el fin de cerrar en un medio a largo plazo las vulnerabilidades detectadas.

Pruebas de Intrusión Externas: el objetivo de estas pruebas es poder evaluar si un intruso pudiera llegar a ingresar a recursos y servicios web que se exponen en internet; las pruebas se fundamentan en ataques y accesos controlados sobre la infraestructura de BN FONDOS, se pone

en cuestionamiento la administración de roles, la autenticación, autorización de accesos, criptografía, accesos a configuraciones.

Figura 55

Pruebas Intrusión Externas 2022

Nota. Elaboración propia, 2024, datos obtenidos de las pruebas de penetración.

Los resultados del periodo 2022 fueron clave para establecer protocolos de seguridad en los servicios web de BN FONDOS, la prueba deparó un total de 3 hallazgos, 0 clasificados como críticos, 0 en grado alto, 3 en grado medio y 0 en nivel bajo, a pesar de tener una baja cantidad de hallazgos o vulnerabilidad la calificación final fue de un riesgo medio; lo cual generó la atención inmediata de los hallazgos con el fin de cerrar en un medio a largo plazo las vulnerabilidades detectadas.

Figura 56

Pruebas Intrusión Externas 2023

Nota. Elaboración propia, 2024, datos obtenidos de las pruebas de penetración.

Los resultados del periodo 2023 fueron clave para establecer protocolos de seguridad en los servicios web de BN FONDOS, la prueba deparó un total de 4 hallazgos, 0 clasificados como críticos, 0 en grado alto, 1 en grado medio y 3 en nivel bajo, a pesar de tener una baja cantidad de hallazgos o vulnerabilidad la calificación final fue de un riesgo medio; lo cual generó la atención inmediata de los hallazgos con el fin de cerrar en un medio a largo plazo las vulnerabilidades detectadas.

Para las atenciones de los hallazgos detectados, en ambos tipos de pruebas, se establecieron recomendaciones para remediación de vulnerabilidades, actualizaciones de seguridad, continuidad de pruebas periódicas, implementaciones y mejoras en aplicaciones web; todas estas atenciones conllevan mejoras en la parte de seguridad de la infraestructura tecnológica de BN FONDOS.

Estudios de Casos Análogos

Según México (s.f.) para el Banco de México la seguridad de la información o ciberseguridad es clave para brindar la confidencialidad, integridad y disponibilidad de la información, por ello la ciberseguridad tiene un rol muy importante en el sistema financiero. México (s.f.) amplía la información mencionando que el Banco de México ha adoptado una estructura organizacional que le ha permitido gestionar e implementar la ciberseguridad y ciberresiliencia de una manera efectiva en la institución, y a su vez ha sido un promotor de la ciberseguridad en el sistema financiero de México.

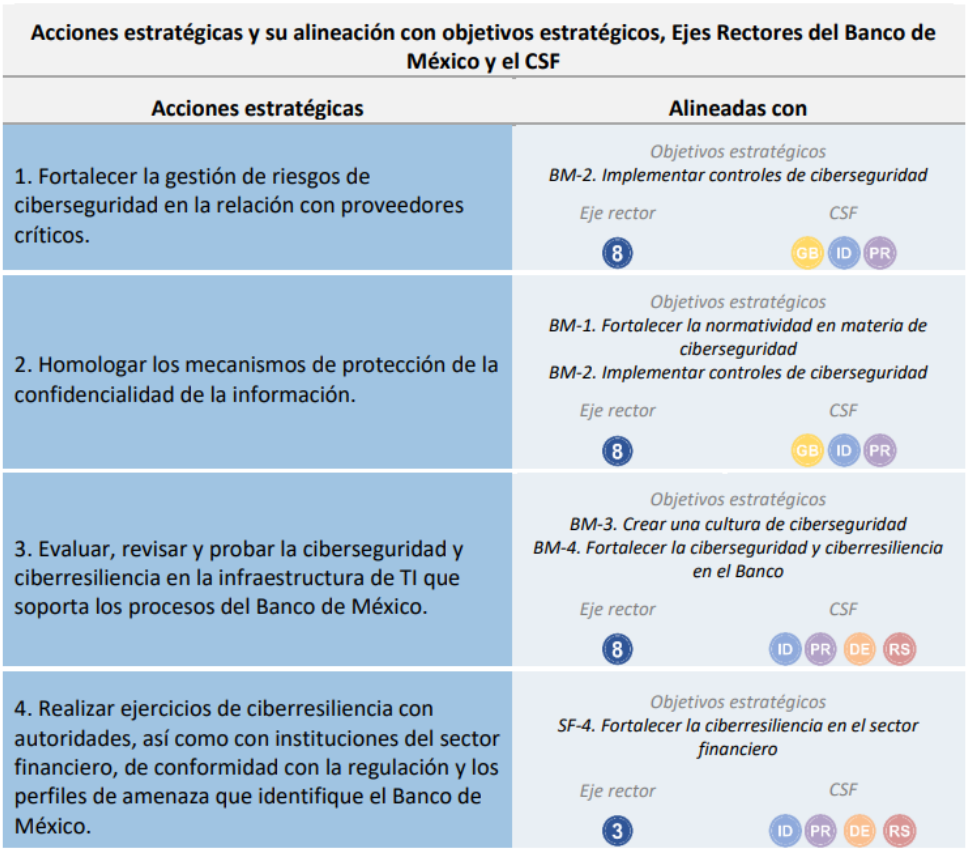
Sus buenos resultados y éxito según México (s.f.) se ha fundamentado en la implementación de procesos robustos y personal altamente capacitado; se ha enfocado en establecer una visión estrategia para garantizar en tiempos actuales y a mediano y largo plazo la seguridad de sus sistemas y principalmente el cumplimiento del servicio con cliente.

La evolución a través del tiempo según México (s.f.) se basado en la adaptación a las necesidades del momento y las nuevas ciberamenazas los cual brinda una madurez en materia de ciberseguridad. Entre 2016 a 2018 y a raíz de los crecientes incidentes internacionales de ciberseguridad en el entorno financiero, el Banco de México tomó la decisión de identificar y mejorar sus estrategias de ciberseguridad, considerando aspectos tecnológicos, humanos y de procesos. A partir del 2019 incrementó su madurez de ciberseguridad con diez procesos de seguridad de la información definiendo documentos, normas, procedimientos y lineamientos a nivel institucional. Realiza un plan de reforzamiento continuo de ciberseguridad entre el 2021 y 2023, se incorporó a grupos internacionales especializados en ciberseguridad y ciberresiliencia como lo es el Global Cyber Resilience Groups del Banco de Pagos Internacionales (BIS), su estrategia continua con una visión entre el 2024 al 2027 con el objetivo de tener un plan de

reforzamiento continuo en materia de ciberseguridad y ciberresiliencia, esto a cargo dela dirección de ciberseguridad del Banco de México; sus estrategias se alinearon con los objetivos estratégicos del marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST Cybersecurity Framework).

Figura 57

Objetivos Estratégicos Banco de México



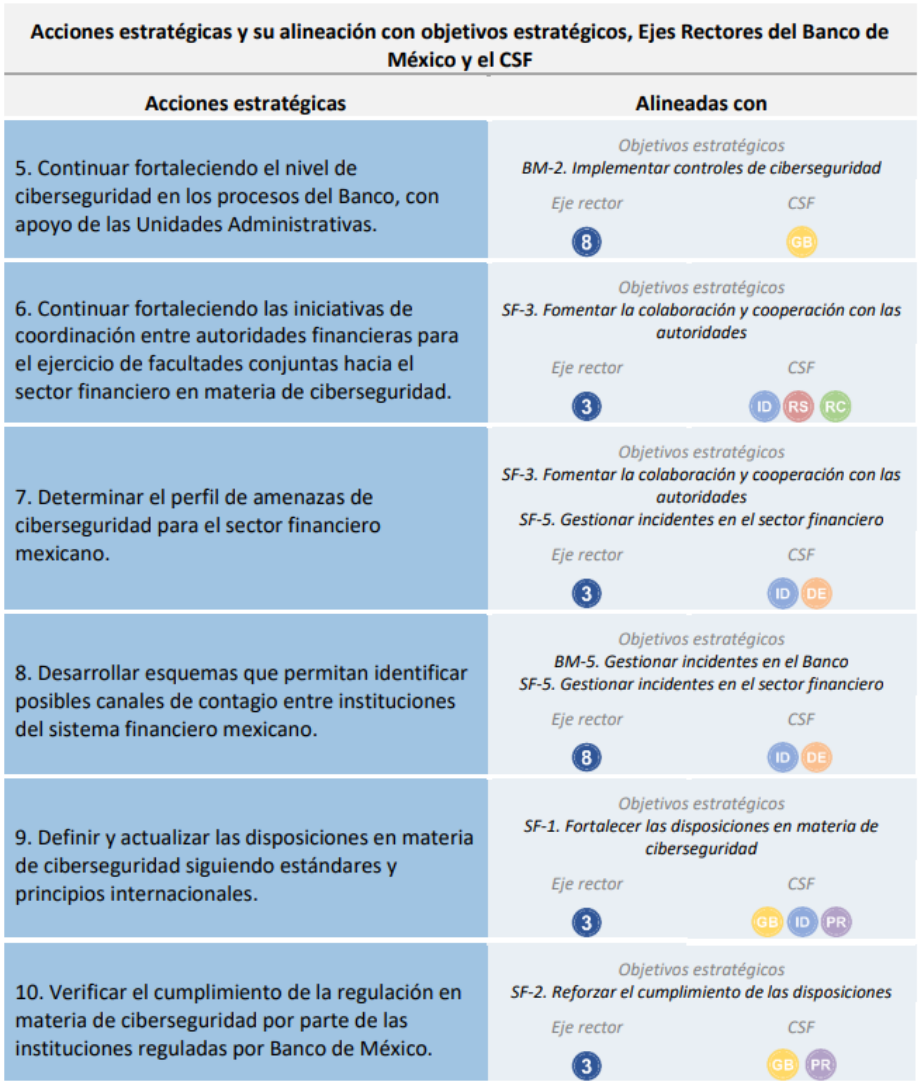
Acciones estratégicas y su alineación con objetivos estratégicos, Ejes Rectores del Banco de México y el CSF

Acciones estratégicas	Alineadas con
1. Fortalecer la gestión de riesgos de ciberseguridad en la relación con proveedores críticos.	*Objetivos estratégicos* *BM-2. Implementar controles de ciberseguridad* *Eje rector*: 8 *CSF*: GB ID PR
2. Homologar los mecanismos de protección de la confidencialidad de la información.	*Objetivos estratégicos* *BM-1. Fortalecer la normatividad en materia de ciberseguridad* *BM-2. Implementar controles de ciberseguridad* *Eje rector*: 8 *CSF*: GB ID PR
3. Evaluar, revisar y probar la ciberseguridad y ciberresiliencia en la infraestructura de TI que soporta los procesos del Banco de México.	*Objetivos estratégicos* *BM-3. Crear una cultura de ciberseguridad* *BM-4. Fortalecer la ciberseguridad y ciberresiliencia en el Banco* *Eje rector*: 8 *CSF*: ID PR DE RS
4. Realizar ejercicios de ciberresiliencia con autoridades, así como con instituciones del sector financiero, de conformidad con la regulación y los perfiles de amenaza que identifique el Banco de México.	*Objetivos estratégicos* *SF-4. Fortalecer la ciberresiliencia en el sector financiero* *Eje rector*: 3 *CSF*: ID PR DE RS

Nota. Ejemplo tomado de estrategia ciberseguridad Banco de México, tomado de México (s.f.)

Figura 58

Objetivos Estratégicos Banco de México



Acciones estratégicas y su alineación con objetivos estratégicos, Ejes Rectores del Banco de México y el CSF	
Acciones estratégicas	**Alineadas con**
5. Continuar fortaleciendo el nivel de ciberseguridad en los procesos del Banco, con apoyo de las Unidades Administrativas.	*Objetivos estratégicos* *BM-2. Implementar controles de ciberseguridad* *Eje rector*: 8 — *CSF*: GB
6. Continuar fortaleciendo las iniciativas de coordinación entre autoridades financieras para el ejercicio de facultades conjuntas hacia el sector financiero en materia de ciberseguridad.	*Objetivos estratégicos* *SF-3. Fomentar la colaboración y cooperación con las autoridades* *Eje rector*: 3 — *CSF*: ID, RS, RC
7. Determinar el perfil de amenazas de ciberseguridad para el sector financiero mexicano.	*Objetivos estratégicos* *SF-3. Fomentar la colaboración y cooperación con las autoridades* *SF-5. Gestionar incidentes en el sector financiero* *Eje rector*: 3 — *CSF*: ID, DE
8. Desarrollar esquemas que permitan identificar posibles canales de contagio entre instituciones del sistema financiero mexicano.	*Objetivos estratégicos* *BM-5. Gestionar incidentes en el Banco* *SF-5. Gestionar incidentes en el sector financiero* *Eje rector*: 8 — *CSF*: ID, DE
9. Definir y actualizar las disposiciones en materia de ciberseguridad siguiendo estándares y principios internacionales.	*Objetivos estratégicos* *SF-1. Fortalecer las disposiciones en materia de ciberseguridad* *Eje rector*: 3 — *CSF*: GB, ID, PR
10. Verificar el cumplimiento de la regulación en materia de ciberseguridad por parte de las instituciones reguladas por Banco de México.	*Objetivos estratégicos* *SF-2. Reforzar el cumplimiento de las disposiciones* *Eje rector*: 3 — *CSF*: GB, PR

Nota. Ejemplo tomado de estrategia ciberseguridad Banco de México, tomado de México (s.f.)

Comparativa de las Normativas para la Atención de Incidentes de Ciberseguridad

De acuerdo con normativas investigadas se procede a realizar y mostrar una tabla comparativa de las normativas ISO/EIC, NIST y COBIT para la atención de incidentes de ciberseguridad como modelo para implementar en BN FONDOS.

Tabla 2

Normativas Incidentes de Ciberseguridad

Normativa	Ámbito de Aplicación	Objetivos	Requisitos	Comunicación con Stakeholders	Aprendizaje de Lecciones
ISO/IEC 27001	Sistema de gestión de la seguridad	Implementar un sistema de gestión de la seguridad de la información	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
ISO/IEC 27032	Sistema de información y comunicaciones	Gestión de riesgos para sistemas de información y comunicaciones	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad

Normativa	Ámbito de Aplicación	Objetivos	Requisitos	Comunicación con Stakeholders	Aprendizaje de Lecciones
ISO/IEC 27033	Redes y comunicaciones	Gestión de seguridad de redes y comunicaciones	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
ISO/EIC 27035	Sistema de información y comunicaciones	Gestión de riesgos y respuesta a incidentes de seguridad	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
ISO/IEC 27036	Gestión de riesgos para sistemas de información y comunicaciones	Gestión de riesgos para sistemas de información y comunicaciones	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
NIST SP 800-61	Computadoras y redes	Atención de incidentes de seguridad	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad

Normativa	Ámbito de Aplicación	Objetivos	Requisitos	Comunicación con Stakeholders	Aprendizaje de Lecciones
NIST SP 800-84	Redes de computadoras	Atención de incidentes de seguridad en redes de computadoras	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
NIST SP 800-150	Sistema de información	Evaluación de riesgos para sistemas de información	Identificar y evaluar riesgos para sistemas de información	Notificar incidentes a las partes interesadas	Analizar incidentes para identificar causas y tomar medidas preventivas
COBIT 5 (2012)	Tecnología de la información y comunicaciones	Mejora para la gestión de tecnología de la información y comunicaciones	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad

Nota: Elaboración propia, 2024, información de acuerdo con lo investigado por cada una de las normativas

La clasificación de la tabla anterior nos muestra como las diferentes normas, según su especialización, pueden llegar a integrarse para proveer de la mejor manera una robustez a BN FONDOS.

Cumplimiento Normas de Atención de Incidentes de uso General

A continuación, se presenta el comparativo de uso y aplicación de las normativas para la atención de incidentes de ciberseguridad la cuales ayudan a evaluar los aspectos que podrían aplicarse para la solución del problema planteado en la investigación.

Tabla 3

Normas de Atención de Incidentes de uso General

Normativa	Facilidad de Implementación	Escalabilidad a futuro	Adaptabilidad a Diferentes Medios Productivos	Integración con Otros Procedimientos y Normas	Capacidad para implementar en Medios Empresariales
ISO/IEC 27001	Cumple	Cumple	Cumple	Cumple	Cumple
ISO/IEC 27032	Cumple	Cumple	Cumple	Cumple	Cumple
ISO/IEC 27033	Cumple	Cumple	Cumple	Cumple	Cumple
ISO/EIC 27035	Cumple	Cumple	No Cumple	Cumple	Cumple

Normativa	Facilidad de Implementación	Escalabilidad a futuro	Adaptabilidad a Diferentes Medios Productivos	Integración con Otros Procedimientos y Normas	Capacidad para implementar en Medios Empresariales
ISO/IEC 27036	Cumple	Cumple	No Cumple	Cumple	Cumple
NIST SP 800-61	No Cumple	Cumple	Cumple	Cumple	Cumple
NIST SP 800-64	No Cumple	Cumple	No Cumple	Cumple	Cumple
NIST SP 800-150	Cumple	Cumple	No Cumple	Cumple	Cumple
COBIT 5	Cumple	Cumple	Cumple	Cumple	Cumple

Nota: Elaboración propia, 2024, información de acuerdo con lo investigado por cada una de las normativas

Comparativa de Normativas para la Atención de Incidentes de Ciberseguridad de uso Bancario

Según Attacks (2024), hoy en día los bancos se enfrentan a muchos retos para poder cumplir de la mejor manera los distintos reglamentos y estándares de ciberseguridad; a su vez se hace un entorno complejo normativo por cumplir con reglamentos nacionales e internacionales.

A su vez las inversiones en materia de ciberseguridad son altas al tener que invertir en personal de tecnología calificado y tecnología (hardware, software, licencias, etc.) también de alto costo.

Por lo tanto, las anteriores normativas para la atención de incidentes de ciberseguridad son esenciales para garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas financieros.

A continuación, se presenta el comparativos de uso y aplicación de las normativas de uso bancario con el fin de determinar cuáles normas pueden servir de referencia para el desarrollo del proyecto y de beneficio para BN FONDOS:

Tabla 4

Comparativa Normativas de uso Bancario

Normativa	Ámbito de Aplicación	Objetivos	Requisitos	Comunicación con Stakeholders	Aprendizaje de Lecciones
ABA Cybersecurity Risk Management Guide	Entornos bancarios	Proteger la información tecnológica	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad

Normativa	Ámbito de Aplicación	Objetivos	Requisitos	Comunicación con Stakeholders	Aprendizaje de Lecciones
BCBS 147	Entornos bancarios	Proteger la información y la infraestructura tecnológica	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
BCBS 239	Entornos bancarios	Proteger la información y la infraestructura tecnológica	Implementar controles de seguridad para proteger la información y la infraestructura tecnológica	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
ISAC for Financial Services	Industria financiera	Proteger la información y la infraestructura tecnológica	Implementar controles de seguridad para proteger la información	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
ISO/IEC 27002	Entornos bancarios	Proteger la información y la infraestructura tecnológica	Implementar controles de seguridad para proteger la información y la infraestructura tecnológica	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad

Normativa	Ámbito de Aplicación	Objetivos	Requisitos	Comunicación con Stakeholders	Aprendizaje de Lecciones
FFIEC IT Handbook	Instituciones financieras	Proteger la información y la infraestructura tecnológica	Implementar controles de seguridad para proteger la información y la infraestructura tecnológica	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
NACHA Operating Rules	Pago y transferencia internacional	Proteger datos de transacción	Implementar controles de seguridad para proteger datos sensibles	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad
NIST 800-171	Gobierno y sector financiero	Proteger datos confidenciales en contratos	Implementar controles de seguridad para datos confidenciales	Notificar incidentes a las partes interesadas	Documentar y analizar incidentes para mejorar la seguridad

Nota: Elaboración propia, 2024, información de acuerdo con lo investigado por cada una de las normativas

.

La clasificación de la tabla anterior nos muestra como las diferentes normas para en entorno bancario, según su especialización, pueden llegar a tomarse en consideración para fortalecer los servicios de BN FONDOS.

A continuación, se presenta la tabla de cumplimientos de normas de atención de incidentes de uso bancario

Tabla 5

Cumplimientos Normas de uso Bancario

Normativa	Facilidad de Implementación	Escalabilidad a futuro	Adaptabilidad a Diferentes Medios Productivos	Integración con Otros Procedimientos y Normas	Capacidad para implementar en Medios Empresariales
ABA	Cumple	Cumple	Cumple	Cumple	Cumple
BCBS 147	No cumple	Cumple	No cumple	Cumple	Cumple
BCBS 239	Cumple	Cumple	Cumple	Cumple	Cumple
ISAC	Cumple	Cumple	Cumple	Cumple	Cumple
ISO/IEC 27002	Cumple	Cumple	Cumple	Cumple	Cumple
FFIEC IT	Cumple	Cumple	Cumple	Cumple	Cumple
NACHA	No cumple	Cumple	No cumple	Cumple	Cumple
NIST 800-171	Cumple	Cumple	Cumple	Cumple	Cumple

Nota: Elaboración propia, 2024, información de acuerdo con lo investigado por cada una de las normativas

Posterior al análisis efectuado se determina que la norma ISO 27002 puede implementarse en BN FONDOS para fortalecer los esquemas de seguridad de la información lo cual contribuye a solventar el problema planteado en esta investigación.

Comparativo de Herramientas Comerciales para la Atención de Incidentes

De acuerdo con GeekFlare (2024), la gestión de eventos e información de seguridad (SIEM) es un término de ciberseguridad en la cual los servicios y los productos se combinan en dos sistemas: la gestión de la información de seguridad (SIM) y la gestión de eventos de seguridad (SEM). Estas herramientas efectúan un análisis de seguridad en tiempo real, recopilan eventos de seguridad, datos, dispositivos de red, servidores y equipos de usuario final.

GeekFlare (2024) SIEM ofrece una tecnología para rastrear a los atacantes, obtener bitácoras de eventos anteriores y ataques asociados, identifica el origen del ataque y ayuda a encontrar la solución del evento detectado, algunos de los beneficios del SIEM son:

- Las herramientas SIEM emplean logs de eventos pasados y presentes para estimar los vectores de ataque.
- Pueden identificar la causa raíz del ataque.
- Se basa en comportamientos pasados para detectar nuevas amenazas.
- Aumentan la protección contra incidentes.
- Colaboran con el cumplimento de las normativas de la organización.

- Todos estos elementos suman para que la organización mantenga su buena reputación y confianza de los clientes.

Por lo tanto, las herramientas SIEM investigadas darán una mejor visión estratégica de cuál es el gestor ideal para implementar en BN FONDOS, tomando en consideración los lineamientos que el área de ciberseguridad del BNCR establece como plan corporativo para el Conglomerado Financiero del Banco Nacional. Otro aspecto para tomar en consideración, el cual se analiza más adelantes es el posicionamiento de estas herramientas en el Cuadrante Mágico de Gartner. A continuación, se presenta la tabla de análisis de cumplimientos de cada herramienta investigada.

Tabla 6

Análisis de Cumplimiento Herramienta SIEM

Herramienta	Facilidad de Implementación	Escalabilidad a Futuro	Adaptabilidad a Diferentes Medios Productivos	Integración con Otros Procedimientos y Normas	Capacidad en Ambientes Bancarios
Splink	Cumple	Cumple	Cumple	Cumple	Cumple
IBM QRadar	Cumple	Cumple	Cumple	Cumple	Cumple
Palo Alto	Cumple	Cumple	Cumple	Cumple	Cumple
Microsoft Azure Sentinel	Cumple	Cumple	Cumple	Cumple	Cumple

Herramienta	Facilidad de Implementación	Escalabilidad a Futuro	Adaptabilidad a Diferentes Medios Productivos	Integración con Otros Procedimientos y Normas	Capacidad en Ambientes Bancarios
McAfee MVision	Cumple	Cumple	Cumple	Cumple	Cumple
Cisco SecureX	Cumple	Cumple	Cumple	Cumple	Cumple
FireEye Helix	Cumple	Cumple	No Cumple	Cumple	Cumple
Rapid7 InsightIDR	Cumple	Cumple	Cumple	Cumple	Cumple
Service Now	Cumple	Cumple	Cumple	Cumple	Cumple

Nota: Elaboración propia, 2024, información de acuerdo con lo investigado por cada una de las herramientas SIEM

A continuación, se presenta la tabla de costos y tipos de licenciamiento para cada solución investigada.

Tabla 7

Costos y Tipos de Licenciamiento

Herramienta	Tipo de Licenciamiento	Costo Estimado (12 meses)
Splunk	Por volumen de datos procesados (GB/día)	$18.000,00 - $25.000,00
IBM QRadar	Por volumen de datos procesados	$25.000,00 - $40.000,00
Palo Alto	Por número de incidentes gestionados	$30.000,00 - $50.000,00
Microsoft Azure Sentinel	Por volumen de datos procesados (GB/mes)	$12.000,00 - $20.000,00
McAfee MVision	Por endpoint	$20.000,00 - $35.000,00
Cisco SecureX	Incluido con otros productos de Cisco	$10.000,00 - $30.000,00
FireEye Helix	Por eventos/datos procesados	$40.000,00 - $60.000,00
Rapid7 InsightIDR	Por número de usuarios o agentes	$15.000,00 - $25.000,00
Service Now	Por número de usuarios y módulos	$50.000,00 - $80.000,00

Nota: Elaboración propia, 2024, datos de acuerdo con las informaciones de los fabricantes

Benchmarking de las Herramientas Comerciales para la Atención de Incidentes

Tabla de análisis de ventajas y desventajas de las herramientas

Tabla 8

Ventajas y Desventajas de Herramientas SIEM

Herramienta	Ventajas	Desventajas	Debilidades identificadas
Splunk	Potente capacidad de análisis de grandes volúmenes de datos. Alta flexibilidad y personalización Amplia integración con otras soluciones de seguridad.	Costos elevados a medida que aumentan los volúmenes de datos procesados. Curva de aprendizaje empinada para usuarios novatos	Alta dependencia de recursos de infraestructura. Puede volverse ineficiente si no se optimizan las consultas
IBM QRadar	Fuerte en correlación de eventos y detección de amenazas avanzadas. Alta integración con soluciones empresariales y cumplimiento normativo.	Complejidad en la implementación inicial. Puede requerir inversión significativa en hardware para grandes volúmenes de datos.	Requiere conocimientos especializados para configuraciones avanzadas. Costos altos de licenciamiento para infraestructura de gran tamaño.

Herramienta	Ventajas	Desventajas	Debilidades identificadas
Palo Alto	Potente automatización de respuesta a incidentes y playbooks preconfigurados. Facilita la colaboración entre equipos de seguridad.	El licenciamiento por incidentes puede ser costoso en entornos con alta actividad. La personalización avanzada puede requerir tiempo y recursos adicionales.	Depende de la calidad de los playbooks y puede requerir ajustes constantes. Puede no ser tan efectiva si no se integra bien con otras soluciones SIEM/SOAR.
Microsoft Azure Sentinel	Solución nativa en la nube, altamente escalable. Se integra fácilmente con otras herramientas y productos de Microsoft.	Los costos pueden escalar rápidamente con grandes volúmenes de datos. Dependiente de la infraestructura en la nube de Azure.	Dependencia total de la infraestructura de Azure, limitando la flexibilidad en entornos híbridos o multinube. Alto consumo de ancho de banda y almacenamiento en análisis de datos grandes.

Herramienta	Ventajas	Desventajas	Debilidades identificadas
McAfee MVision	Gestión integral de endpoints y buena visibilidad en tiempo real. Integración con soluciones de DLP y EDR de McAfee.	Requiere una infraestructura de red sólida para maximizar su eficacia. Puede ser menos flexible para integrarse con herramientas de otros proveedores.	Integración limitada con algunas soluciones de terceros no compatibles con McAfee. Gestión complicada en redes heterogéneas con múltiples plataformas.
Cisco SecureX	Proporciona un entorno unificado para la visibilidad de amenazas. Automatización de flujos de trabajo y análisis avanzados.	Depende de otros productos de Cisco para desplegar toda su capacidad.	Puede ser limitado si no se utiliza en conjunto con otros productos de Cisco. Falta de integración profunda con soluciones de terceros fuera del ecosistema Cisco.
FireEye Helix	Fuerte en la detección de amenazas avanzadas (APT) y análisis forense. Incluye capacidades SIEM y SOAR en una sola solución.	Alto costo para grandes empresas con alta actividad de eventos. Menos flexible en entornos fuera del campo de ciberseguridad avanzada.	Puede no ser adecuado para empresas pequeñas o medianas por su costo elevado. Enfocado más en amenazas avanzadas, menos útil para amenazas cotidianas.

Herramienta	Ventajas	Desventajas	Debilidades identificadas
Rapid7 InsightIDR	Rápida implementación y fácil uso. Buen equilibrio entre funcionalidad de SIEM y EDR.	Funcionalidades más limitadas en comparación con otros SIEM avanzados. Puede no ser la mejor opción para grandes empresas con infraestructura compleja.	Limitaciones en grandes entornos con alta cantidad de eventos. No tiene capacidades avanzadas de respuesta automática comparado con otros SIEM/SOAR.
ServiceNow Security Operations	Integración con el resto de la suite de ServiceNow, proporcionando una plataforma unificada para IT y seguridad. Amplia automatización y orquestación de incidentes.	El costo puede ser alto, especialmente con múltiples módulos implementados. Dependencia de la plataforma de ServiceNow, lo que puede no ser ideal si no se usa ampliamente en la empresa.	Dependencia del ecosistema de ServiceNow y puede no ser adecuada si no se utiliza la plataforma completa. Puede requerir personal con experiencia en ServiceNow para aprovechar todas sus capacidades.

Nota: Elaboración propia, 2024, datos obtenidos por medio del análisis efectuado a las herramientas SIEM

Análisis FODA de las Herramientas

A continuación, se establece para las herramientas investigadas un análisis FODA:

Tabla 9

Análisis FODA

Herramientas	Fortalezas	Oportunidades	Debilidades	Amenazas
Splunk	Alta capacidad de análisis de grandes volúmenes de datos. Personalización y flexibilidad en la creación de paneles y alertas.	Expansión hacia nuevas áreas de análisis predictivo y aprendizaje automático. Integración con tecnologías emergentes de seguridad y cloud computing.	Alto costo para grandes volúmenes de datos. Requiere un equipo especializado para su administración y optimización.	Creciente competencia con otras soluciones SIEM más accesibles. Dependencia de recursos de infraestructura que pueden no ser escalables en ciertos entornos.

Herramientas	Fortalezas	Oportunidades	Debilidades	Amenazas
IBM QRadar	Fuerte en correlación de eventos y análisis de seguridad en tiempo real. Alta confiabilidad para ambientes altamente regulados.	Mayor integración con tecnologías de IA para mejorar la respuesta a incidentes. Expansión hacia la automatización avanzada y respuesta a incidentes.	Complejidad en la implementación y gestión. Requiere conocimientos avanzados para configuraciones personalizadas.	Costos elevados de licenciamiento y mantenimiento. La competencia de otros SIEM más simples y económicos puede ser una amenaza para su cuota de mercado.
Palo Alto Cortex XSOAR	Automatización de respuestas a incidentes y playbooks eficientes. Integración fluida con otros productos de Palo Alto Networks y SIEM.	Creciente demanda por automatización en la respuesta a incidentes en el sector bancario. Aumento del uso en la integración con entornos híbridos y nativos en la nube.	Costo elevado en entornos con alta cantidad de incidentes. Complejidad en la creación y personalización de playbooks avanzados.	El mercado competitivo de SOAR con nuevas soluciones ágiles y económicas. Competencia de SOAR que combinan capacidades SIEM, siendo una solución completa.

Herramientas	Fortalezas	Oportunidades	Debilidades	Amenazas
Microsoft Azure Sentinel	Solución nativa en la nube con escalabilidad flexible. Integración perfecta con el ecosistema de Microsoft.	Expansión con soluciones de automatización e IA de Microsoft. Creciente adopción de soluciones en la nube en sectores bancarios.	Dependencia exclusiva de la infraestructura de Azure. Alto costo de almacenamiento de grandes volúmenes de datos a largo plazo.	Competencia de SIEM híbridos que no dependen exclusivamente de la nube. Amenaza de proveedores más especializados en la nube y con costos más bajos.
McAfee MVISION	Fuerte protección de endpoints y visibilidad en tiempo real. Integración con otras soluciones de seguridad de McAfee como EDR y DLP.	Expansión hacia soluciones integradas de protección en la nube. Creciente demanda por soluciones de ciberseguridad unificadas en entornos bancarios.	Integración limitada con soluciones de terceros. Alta dependencia de la infraestructura de red para maximizar su eficiencia.	Proveedores más flexibles y con mayor compatibilidad con herramientas de terceros. Competencia de soluciones ágiles y compatibles con una mayor variedad de infraestructuras.

Herramientas	Fortalezas	Oportunidades	Debilidades	Amenazas
Cisco SecureX	Entorno unificado de visibilidad de amenazas. Automatización de flujos de trabajo y análisis avanzados.	Expansión en la integración con más productos fuera del ecosistema de Cisco. Potencial para ampliar su integración con servicios en la nube y soluciones de terceros.	Dependencia de otros productos de Cisco para desplegar toda su funcionalidad. Limitado cuando no se utiliza junto a otros productos de Cisco.	Amenaza de soluciones con integración nativa que no dependen de un ecosistema específico. La competencia de plataformas más abiertas e integradoras puede desplazar su uso si no se adapta.
FireEye Helix	Fuerte en la detección de amenazas avanzadas y capacidades forenses. Combina SIEM y SOAR en una única solución.	Aumento en la demanda de análisis forense avanzado en sectores financieros. Expansión hacia la inteligencia artificial para la detección de amenazas.	Costo elevado, especialmente para organizaciones pequeñas. Menos adecuado para amenazas cotidianas de bajo nivel.	Nuevos competidores que ofrecen soluciones SIEM y SOAR a costos más accesibles. Mayor competencia de soluciones SIEM especializadas en análisis de datos.

Rapid7 InsightIDR	Implementación rápida y fácil de usar. Buen equilibrio entre SIEM y EDR en una única solución.	Mayor demanda en medianas empresas que requieren SIEM sin gran complejidad. No es la mejor opción para grandes empresas con necesidades avanzadas.	Funcionalidades limitadas comparadas con otros SIEM avanzados. No es la mejor opción para grandes empresas con necesidades avanzadas.	Competencia de soluciones SIEM con mayor capacidad de automatización y flexibilidad. Amenaza de SIEM más completos y avanzados para grandes organizaciones.
ServiceNow Security Operations	Plataforma unificada para IT y seguridad, con alta automatización. Integración con otros módulos de ServiceNow, facilitando la orquestación y automatización.	Aumento en la adopción de soluciones integradas de IT y seguridad. Expansión hacia la automatización avanzada en la respuesta a incidentes y gestión de riesgos.	Costoso, especialmente con múltiples módulos implementados. Dependencia del ecosistema de ServiceNow.	Competencia de soluciones de seguridad con menores costos y mayor integración con sistemas externos. Proveedores de soluciones más especializadas en ciberseguridad y con enfoque menos generalista.

Nota: Elaboración propia, 2024, datos obtenidos por medio del análisis efectuado a las herramientas SIEM

Cuadrantes Mágicos de Gartner

Según Gartner (2024) un Cuadro Mágico de Gartner consolida la investigación de un mercado en específico con el fin de proporcionar una visión panorámica de las posiciones relativas de los competidores a nivel mundial. Por medio de la representación gráfica se puede llegar a determinar rápidamente como los proveedores de tecnología están bien posicionados en el mercado tecnológico y así invertir en sus productos.

Un cuadro de Gartner está formado un gráfico de dos ejes, el eje vertical representa el conocimiento en el mercado, y el eje horizontal muestra la habilidad de ejecución. A su vez se segmenta en cuatro (4) tipos de proveedores de tecnología:

- Líderes: proveedores que están bien posicionados en el mercado con buena proyección a futuro.
- Visionarios: proveedores que conocen a dónde va el mercado, pueden cambiar su estrategia si lo ameritan, pero su capacidad de acción es limitada.
- Jugadores de nicho: se centran en el éxito en pequeño segmento, no se preocupan por innovar.
- Retadores o aspirantes: se desempeñan bien un mercado específico, pero no tienen claridad hacia donde se dirige el mercado.

En resumen, un cuadrante mágico de Gartner ayuda a:

- Determinar que proveedores de tecnología compiten en el mercado y su capacidad de ofrecer al usuario final el requerimiento deseado.

- Comprender como los proveedores de tecnología son competitivos en cierto mercado y como sus estrategias son enfocadas en la necesidad del usuario final.
- Tener un parámetro de comparación para identificar las fortalezas de los proveedores de tecnología.

La siguiente imagen muestra la estructura de un Cuadro Mágico de Gartner:

Figura 59

Cuadro Mágico de Gartner

Nota. Estructura Cuadrante Garner, tomado de Gartner (2024)

Gartner, Tendencias en Ciberseguridad

De acuerdo con Gartner (2024), la ciberseguridad es la práctica para disponer de personal, creación de procesos, políticas y tecnologías para proteger las organizaciones y su información confidencial a ciberataques. Menciona que los responsables de TI deben mantenerse

al día con las nuevas tendencias y buenas prácticas para enfrentar las amenazas de los ciberdelincuentes.

La empresa Gartner realizó una encuesta sobre las principales tendencias de ciberseguridad para el año 2024, identificando de la siguiente manera:

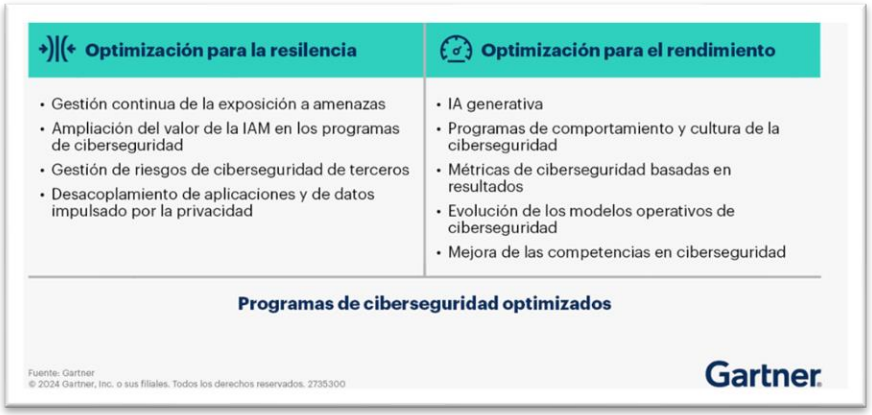
- Surge la IA como una herramienta generalizada.
- La continua brecha entre la oferta y la demanda de personas expertas en seguridad.
- El crecimiento de servicios en la nube cambia radicalmente los sistemas tradicionales.
- Se da el incremento de normativas, reglamentos y la supervisión de los gobiernos en temas de ciberseguridad y privacidad de los datos.

El informe de las principales tendencias en ciberseguridad de Gartner para el año 2024 sobresalen cuatro actividades para reforzar la resiliencia:

- Programas de gestión continua de la exposición a amenazas.
- Evolución de la gestión de identidades y accesos.
- Gestión de riesgos de ciberseguridad de terceros.
- Desacoplamiento de datos y aplicaciones impulsado por la privacidad.

Figura 60

Tendencias en ciberseguridad para 2024



Nota. Clasificación de Tendencias en Ciberseguridad, tomado de Gartner (2024)

Cuadrante Mágico de Gartner, Información de Seguridad y Gestión de Eventos

Según Labrador (2023), Gartner clasifica el SIEM como una tecnología que analiza datos de eventos de seguridad y datos de flujo en tiempo real para la gestión de amenazas en una organización, tomando en consideración amenazas externas e internas. Estas herramientas recopilan, almacenan, analizan y notifican datos para atender la respuesta a incidentes, análisis forenses y cumplimiento normativo. Dado estos alcances lo proveedores se especializan en mejorar continuamente las herramientas para proveer mejoras tecnológicas para prevenir las amenazas y análisis de seguridad. A continuación, se muestra el Cuadrante Mágico de Gartner para la Información de Seguridad y Gestión de Eventos correspondiente al año 2024:

Figura 61

Cuadrante Mágico Gartner

Nota. Clasificación de fabricantes SIEM en el Cuadrante Gartner, tomado de Labrador (2023)

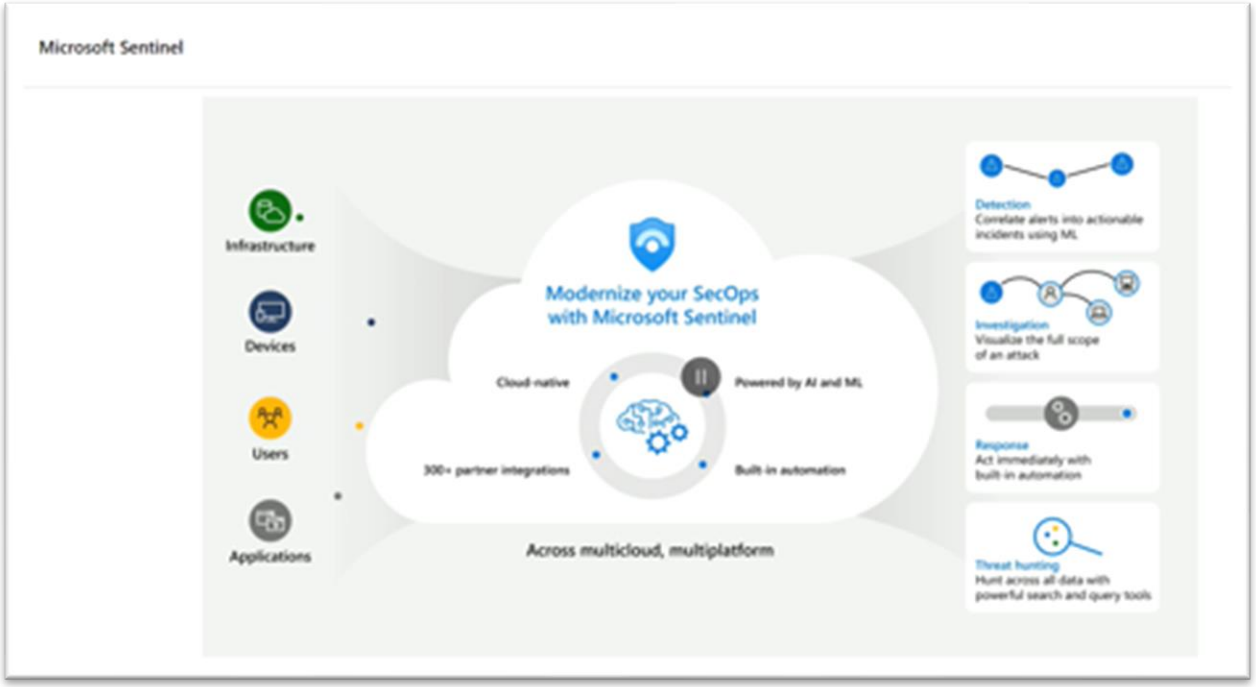
El Cuadrante Mágico de Gartner para la Información de Seguridad y Gestión de Eventos correspondiente al año 2024 destaca en el cuadrante de Líderes a empresas como Splunk y Microsoft como proveedoras de soluciones para gestionar la seguridad y eventos (SIEM) de 22 soluciones que conforman el cuadrante mágico para el año 2024.

Para la propuesta de una solución de monitoreo en materia de ciberseguridad que optimice el servicio de detección temprana de amenazas de ciberataques, se determina que para

BN FONDOS la solución SIEM de Microsoft Sentinel es viable dado que permite el análisis de datos y flujos de trabajo para acelerar de una manera oportuna la detección de amenazas que pueden afectar el servicio interno y hacia el cliente final; la compatibilidad con otras herramientas de la suite de Microsoft Office 365 es un gran beneficio para la integración nativa y así obtener los mejores beneficio a corto plazo, su portal unificado es otra ventaja ya que en una sola consola de gestión en tiempo real se pueden atender los requerimientos necesarios

Figura 62

Microsoft Sentinel



Nota. Esquema de servicios del Sentinel, tomado de Microsoft (s.f.)

Estudio de Factibilidad

Según Ariosto (2021) un estudio de factibilidad colabora con las empresas a que validen si un proyecto que se pretende implementar es viable o no, así como cuales son las condiciones

que deben presentar para que se materialice y que situaciones pueden enfrentar para confrontarlas.

Basados en la cita anterior, este estudio de factibilidad presenta información detallada son las implicaciones técnicas, económicas, legales, recursos, mercados, operacional y de tiempo, las cuales sirvieron como base para tomar las decisiones referentes para la solución de esta investigación y su posterior implementación.

Factibilidad técnica

A fin de determinar la factibilidad técnica para la implementación de un modelo de atención y gestión de respuesta a incidentes y amenazas para BN FONDOS se realizó un análisis de los recursos técnicos existentes actualmente para determinar si son suficientes para la realización de la propuesta o bien si se deben contemplar recursos de hardware y software:

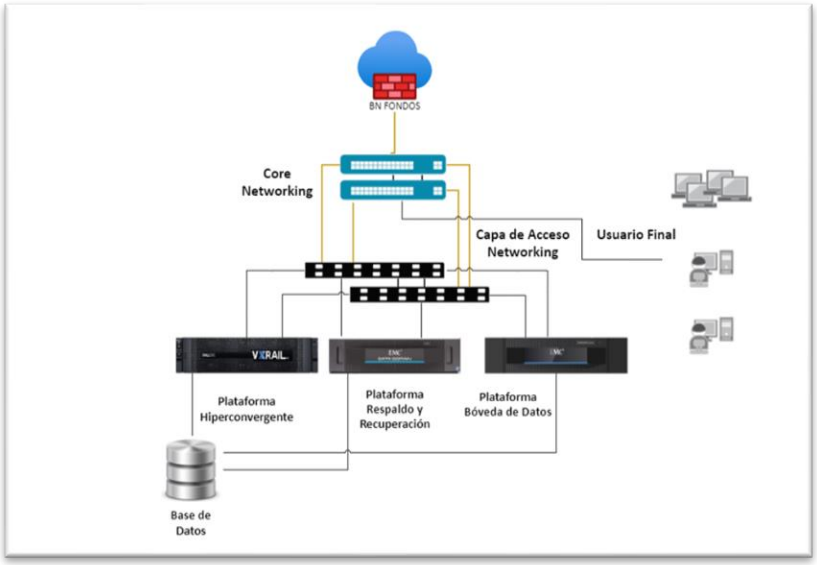
- Recursos de hardware: la actual plataforma Hiperconvergente de BN FONDOS cuenta con recursos suficientes, tales como de almacenamiento, memoria y core, lo cual contribuye en la propuesta para la adquisición de un software especializado para la atención de incidentes en ciberseguridad (con características SIEM).
- Recursos de software: actualmente BN FONDOS cuenta con licenciamiento de Windows Server 2019R2, sistemas operativos base para el soporte de software especializado para la atención de incidentes en ciberseguridad (con características SIEM), por lo tanto, no se amerita incurrir o invertir en adquisición de licencias para sistemas operativos WIN SERVER.

- Software especializado para la atención de incidentes en ciberseguridad (SIEM): BN FONDOS debe contemplar con el análisis y viabilidad técnica de adquirir un sistema SIEM con su respectivo licenciamiento o suscripción para el uso de la herramienta siguiendo los lineamientos que establezca el área de Ciberseguridad del BNCR

Otro aspecto a toma en consideración es fortalecer el área con un encargado de soporte técnico especializado en el área de ciberseguridad para que desempeñe labores nativas de seguridad informática como análisis de eventos, logs, interpretación de alertas de amenazas, análisis de vulnerabilidades y pruebas de intrusión, parcheo de sistemas operativos para máquinas de usuario final y para servidores (físicos y virtuales), para firmware y/o ISO de las diferentes plataformas tecnológicas de BN FONDOS; la siguiente topología técnica representa la implementación a realizar con la herramienta SIEM:

Figura 63

Topología Plataforma Tecnológica BN FONDOS



Nota. Plataforma tecnológica de BN FONDOS, elaboración propia, 2024

Factibilidad Económica

El estudio de factibilidad económica se basó en un análisis de relación costo-beneficio, para lo cual se cuantificó la inversión de un software especializado SIEM para la gestión de respuesta a incidentes y amenazas para BN FONDOS versus tener un especialista dedicado a esta labor de correlación de eventos.

La siguiente tabla muestra la proyección de inversión a 1 año que se debe considerar para poner en producción un sistema SIEM en BN FONDOS:

Tabla 10

Factibilidad Económica

Item	Descripción	Precio Total
1	Inversión de la Solución 1 año	$ 45.000,00
2	Salario de Especialista en ciberseguridad 1 año (con cargas sociales)	$ 84.000,00

Nota: Elaboración propia, 2024

Según Zendesk (2024) el retorno de inversión (ROI) hace referencia a la ganancias o beneficios que una empresa puede obtener posterior a haber realizado una inversión, la fórmula para calcular el ROI es la siguiente:

Figura 64

Fórmula ROI

Nota: Fórmula ROI tomada de Zendesk (2024)

De acuerdo con el concepto del ROI y con el objetivo de garantizar un proyecto rentable para BN FONDOS se procede con el estimar el ROI (Retorno de Inversión), al aplicar la fórmula correspondiente el retorno de inversión (ROI) en adquirir una solución SIEM de acuerdo con los valores de la Tabla 10 es de un 95.34%, lo cual permite automatizar los servicios y confiabilidad de los resultados; por lo tanto, el proyecto es viable para BN FONDOS

Factibilidad Legal

El proyecto por establecer e implementar forma parte del plan estratégico del área de tecnología de BN FONDOS, cuenta con el respaldo del staff gerencial, adicionalmente se integra a las recomendaciones que se recibieron por parte de un auditor externo con la atención de hallazgos y recomendaciones para el Conglomerado Financiero del Banco Nacional, por lo tanto, el proyecto es viable legalmente, el diseño propuesto se alinea con los reglamentos internos, jurídicos, legales y con las normativas de ciberseguridad que se emiten por entidades nacionales como lo es el MICITT y el CONASSIF y que las entidades financieras de Costa Rica deben acatar; adicionalmente cumple con los estándares internacionales de normas como ISO 27000, COBIT y NIST.

Factibilidad de Recursos

Para desarrollar las labores de la solución propuesta se destinará el siguiente personal de la Gerencia de Sistemas de Tecnología:

Tabla 11

Proyección Personal TI

Miembro del Equipo	Porcentaje de tiempo en el proyecto
Jefatura Producción Sistemas	15%
Técnico en Ciberseguridad	90%
Especialista en Ciberseguridad	90%
Especialista en Infraestructura	50%
Especialista en Redes	50%
Técnicos de Mesa de Servicio	45%
Técnicos de Monitoreo	80%

Nota. Elaboración propia, 2024

Se establecerá con el Project Manager un plan de trabajo en el cual se determinarán las fases del proyecto con sus respectivas tareas, a su vez se llevará un control de las horas del personal que realice las diferentes tareas y el control financiero del proyecto.

Factibilidad de Mercado

En la actualidad, los proveedores de tecnología en el país representan a reconocidas casas fabricantes de herramientas SIEM (Security Information and Event Management) investigadas, las cuales son ampliamente utilizadas para la gestión de eventos de seguridad. Estos proveedores también ofrecen servicios especializados bajo demanda, lo que incluye acompañamiento en el

diseño e implementación de un manual de gestión para la respuesta a incidentes y amenazas dirigido a BN FONDOS. El análisis realizado confirma que los productos ofrecidos para la prevención de incidentes en ciberseguridad no solo son efectivos, sino que también cuentan con un sólido posicionamiento a nivel global, lo que garantiza su capacidad para cubrir las necesidades de seguridad de la organización.

Esto respalda la viabilidad de adoptar estas soluciones en BN FONDOS para fortalecer su ciberresiliencia y capacidad de respuesta ante incidentes.

Factibilidad Operacional

El proyecto en menciona se asocia a la estrategia de BN FONDOS, forma parte vital de los cumplimientos de implementación de servicios tecnológicos que garanticen la continuidad del negocio y mantenga la buena reputación que posee hoy en día.

Factibilidad de Tiempo

El diseño e implementación de un modelo para la gestión de respuesta a incidentes y amenazas para BN FONDOS es una solución de alta prioridad la cual debe ser atendida en el primer semestre del 2025; dada el incremento de los ciberataques a entidades financieras esta solución cuenta con el apoyo de la Gerencia General, cuenta con contenido presupuestario, y forma parte de los primeros proyectos a calendarizar y efectuar en el 2025; la cual estará a cargo de la Gerencia de Sistemas y Tecnología de BN FONDOS.

Recomendación y Aprobación

Finalizado el estudio de factibilidad técnico, económico, legal, recursos, mercado, operacional y de tiempo sobre el diseño de un modelo integral de gestión de incidentes y ciber

resiliencia para BN FONDOS, de concluye que se cuenta con la información necesaria para determinar el que proyecto representa una buena oportunidad para fortalecer a la organización contra los ciberataques, ya que la infraestructura actual (hardware y software) posee los recursos tecnológicos para la implementación del proyecto, se cuenta con el apoyo de la Gerencia General para invertir en los insumos que ameriten contenido presupuestario.

Esta solución viene a colaborar y dar una solución con los problemas actuales y críticos que atraviesan las entidades financieras contra las amenazas cibernéticas dando beneficios entre corto y mediano plazo.

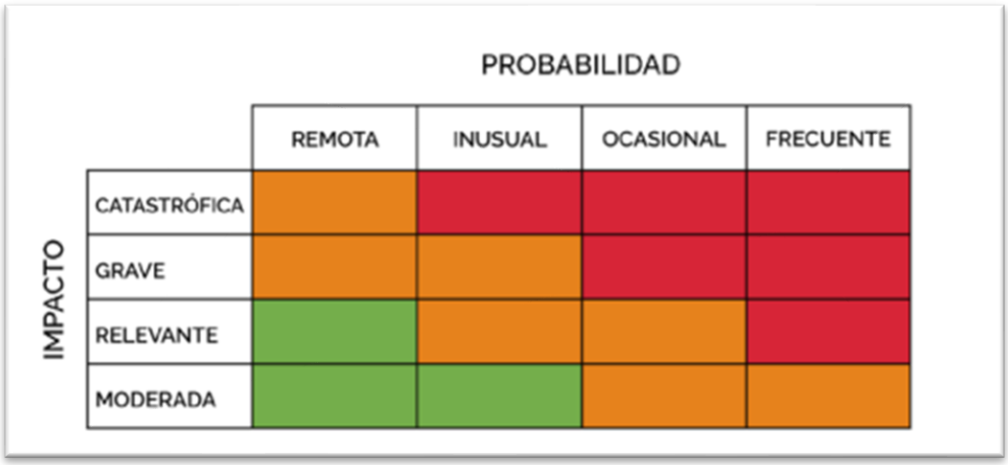
Mapa de Riesgos de Seguridad de la Información

Hoy en días las instituciones deben ser más eficientes en los diferentes procesos y gestiones que realiza la organización con el objetivo de garantizar la disponibilidad, integridad y confidencialidad de los datos, una forma práctica de poder determinar loa riesgos asociados al impacto y probabilidad de que se materialicen es diseñar un mapa de riesgos de seguridad de la información, según Riesgos (2019) un mapa de riesgos es una herramienta que permite llegar a la toma de decisiones de una forma visual, el mapa mostrará una perspectiva de la organización y su orden de prioridad, el objetivo es mejorar la comprensión del riesgo determinado, la naturaleza del mismo y el impacto que puede provocar en la organización. Los riesgos identificados que pueden afectar a la organización se muestran en una matriz de riesgo o bien conocida como mapa de calor, definida por la probabilidad del suceso y su impacto en la organización.

Un ejemplo de un mapa de riesgos es el siguiente:

Figura 65

Ejemplo de Mapa de Riesgos



Nota. Mapa de Riesgo tomado de Riesgos (2019).

De acuerdo con la investigación en proceso se determina un mapa de riesgos para implementar el modelo de atención de incidentes para BN FONDOS, por lo tanto se establecen 14 riesgos debidamente clasificados con el impacto, probabilidad y riesgo que se materialice, a su vez se determina el plan de atención o mitigación del riesgo identificado.

Tabla 12

Tabla de Riesgo

#	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Plan de tratamiento al riesgo
1	Falta de apoyo de la alta gerencia en materia de ciberseguridad	Alta	Crítico	Extremo	Realizar reuniones periódicas con la alta gerencia para explicar beneficios, alineación con los objetivos estratégicos y retorno esperado.
2	Falta de personal capacitado para operar el modelo de gestión de incidentes	Media	Alto	Alto	Implementar un plan de capacitación integral en ciberseguridad basado en roles y responsabilidades
3	Insuficiencia en la infraestructura tecnológica para implementar herramientas clave	Media	Alto	Alto	Realizar un análisis de brechas tecnológicas y adquirir o actualizar herramientas críticas como SIEM o sistemas de monitoreo (NOC).
4	Carencia de procedimientos estandarizados para la gestión de incidentes	Alta	Alto	Extremo	Diseñar y documentar procedimientos estandarizados basados en marcos de trabajo reconocidos como NIST CSF.

#	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Plan de tratamiento al riesgo
5	Resistencia al cambio por parte del personal	Media	Medio	Moderado	Implementar un plan de gestión del cambio con comunicación efectiva, formación y talleres participativos
6	Exposición a ciberataques durante la implementación del modelo	Bajo	Crítico	Alto	Establecer controles provisionales de seguridad, realizar análisis de vulnerabilidades y monitoreo continuo durante la implementación
7	Falta de presupuesto asignado para la implementación	Media	Crítico	Extremo	Elaborar un caso de negocio sólido que justifique los costos y beneficios del proyecto para asegurar los fondos necesarios
8	Retrasos en la adquisición de tecnología necesaria	Media	Alto	Alto	Priorizar los equipos críticos en el plan de adquisiciones y trabajar con proveedores confiables para garantizar entregas oportunas

#	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Plan de tratamiento al riesgo
9	Riesgos regulatorios asociados con la implementación y manejo de datos sensibles	Baja	Alto	Moderado	Asegurar que el proyecto cumpla con todas las normativas aplicables (GDPR, PCI DSS) desde el inicio del diseño del modelo
10	Ineficiencia en la coordinación entre departamentos	Media	Medio	Moderado	Nombrar un líder de proyecto y establecer un comité interdepartamental para la supervisión y comunicación efectiva
11	Incapacidad para realizar pruebas efectivas del modelo implementado	Alta	Alto	Extremo	Programar simulacros y pruebas de penetración periódicas para garantizar la efectividad del modelo y ajustar según resultados obtenidos
12	Pérdida de datos o errores durante la migración a nuevas herramientas	Baja	Crítico	Alto	Realizar copias de seguridad completas antes de la migración y pruebas en entornos controlados para validar la integridad de los datos

#	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Plan de tratamiento al riesgo
13	Dependencia excesiva de un único proveedor para herramientas de gestión de incidentes	Baja	Medio	Moderado	Diversificar proveedores y considerar soluciones abiertas o híbridas para mitigar riesgos asociados con la dependencia tecnológica
14	Falta de indicadores clave de rendimiento (KPI) para evaluar el éxito del modelo implementado	Media	Medio	Moderado	Diseñar e implementar métricas específicas para medir tiempos de respuesta, impacto reducido y mejora continua del modelo

Nota. Elaboración propia, 2024

Niveles de riesgo:

Moderado: puede gestionarse con controles existentes y monitoreo ocasional.

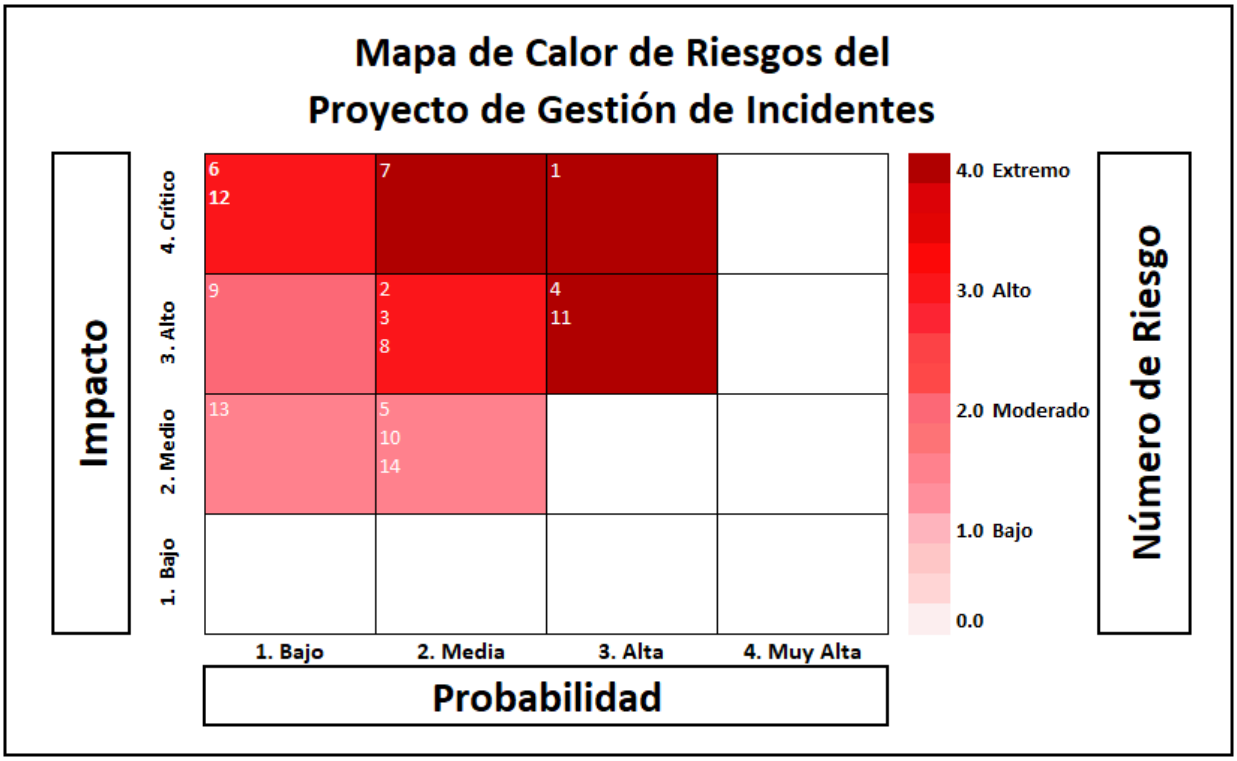
Alto: requiere acciones inmediatas para reducir el impacto o la probabilidad

Extremo: es prioritario y debe tratarse con un enfoque urgente y dedicado

De acuerdo con la tabla anterior se determina el siguiente mapa de calor:

Figura 66

Mapa de Calor de Riesgos del Proyecto



Nota: Elaboración propia, 2024

De acuerdo con el mapa de calor definido se logra evidenciar que de los 14 riesgos establecidos con prioridad de atención son los riegos 1, 7, 4 y 11 ya que quedaron clasificados como un riesgo extremo que puede afectar el desarrollo del proyecto.

Capítulo V: Conclusiones y Recomendaciones

En este apartado se expone las conclusiones derivadas del desarrollo de la investigación, en la cual se abordó la implementación de un modelo integral de gestión de incidentes y ciber resiliencia para BN Fondos. En esta sección se sintetizan los hallazgos más relevantes, los cuales evidencian el nivel de preparación actual de la organización para enfrentar incidentes de ciberseguridad y el grado de efectividad de las recomendaciones propuestas. Asimismo, se resaltan los aportes clave de este estudio en el fortalecimiento de la seguridad de la información en BN FONDOS, proporcionando una visión general de los beneficios potenciales y de las áreas de mejora futuras en la gestión de incidentes dentro del contexto financiero.

Conclusiones

El análisis realizado responde a la pregunta de investigación al demostrar que la implementación de un modelo integral de gestión de incidentes y ciberresiliencia es una solución efectiva para BN FONDOS frente a los riesgos cibernéticos. Los resultados confirman que dicho modelo puede mejorar significativamente la capacidad de la organización para mitigar riesgos, mantener la continuidad del negocio y proteger su reputación. A continuación, se detallan las conclusiones específicas con base en los objetivos planteados.

- Análisis de amenazas cibernéticas: Se identificaron las principales amenazas cibernéticas que podrían afectar a BN FONDOS, lo que permitió determinar los riesgos críticos que el modelo de gestión debe abordar. La recopilación de datos históricos de ciberataques en Latinoamérica y Costa Rica resaltó que las amenazas más recurrentes son ataques de ransomware y phishing, lo que exige atención inmediata. Este análisis también destacó la

necesidad de un presupuesto adecuado para la tecnología de seguridad y la capacitación continua del personal de TI, áreas que se ven frecuentemente descuidadas.

- Evaluación de la infraestructura tecnológica: La evaluación de la infraestructura actual de BN FONDOS reveló que, aunque las tecnologías implementadas ofrecen un alto grado de protección, todavía existen vulnerabilidades que podrían comprometer la continuidad del negocio. Las auditorías y pruebas de penetración demostraron que la entidad cuenta con mecanismos adecuados de protección, pero deben ser complementados con sistemas más robustos de monitoreo y actualización constante.
- Desarrollo de estrategias de prevención, respuesta y recuperación: Se diseñó una estrategia integral que sigue las mejores prácticas de ciberseguridad y se alinea con estándares internacionales como NIST. Esta estrategia incluye medidas de prevención, respuesta rápida ante incidentes y planes de recuperación que permitirán a BN FONDOS mitigar eficazmente el impacto de ciberataques. La implementación de este modelo integral refuerza la capacidad de resiliencia de la entidad, permitiendo garantizar la continuidad operativa y proteger la reputación institucional.
- Propuesta de monitoreo y detección temprana de amenazas: Se propuso un sistema avanzado de monitoreo y detección de amenazas basado en inteligencia artificial y análisis predictivo, que fortalecerá la capacidad de BN FONDOS para detectar y responder rápidamente a incidentes de seguridad. El uso de herramientas SIEM, como Microsoft Sentinel y ServiceNow, demostró ser crucial para reducir el tiempo de respuesta y mejorar la eficiencia en la gestión de incidentes.
- Capacitación del personal en ciberseguridad: Se desarrolló un plan de capacitación continuo para el personal de BN FONDOS, que incluye simulaciones de ciberataques y

formación especializada en gestión de incidentes. Este programa es esencial para asegurar una respuesta coordinada y eficiente ante posibles ciberataques, lo que refuerza la cultura de seguridad dentro de la organización.

La implementación del modelo integral de gestión de incidentes y ciberresiliencia en BN FONDOS no solo es viable, sino necesaria para garantizar una protección efectiva ante la creciente complejidad de las amenazas cibernéticas, asegurar la continuidad del negocio y proteger la reputación de la entidad.

Recomendaciones

- Capacitación continua: Fortalecer las capacitaciones al personal administrativo y técnico, enfocándose en ciberseguridad y uso de herramientas SIEM para mejorar la capacidad de respuesta a incidentes.
- Monitoreo constante: Implementar un plan de monitoreo continuo del sistema de gestión de incidentes para garantizar que se cumplan los estándares de ciberseguridad y regulaciones locales.
- Escalabilidad del sistema: Asegurar que el sistema de gestión de incidentes sea escalable, preparado para manejar un mayor volumen de datos y nuevas amenazas.
- Adopción de nuevas tecnologías: Evaluar e implementar tecnologías emergentes como la inteligencia artificial y el machine learning para la detección proactiva de amenazas.
- Fomento de la cultura de ciberseguridad: Promover una cultura organizacional enfocada en la seguridad informática a través de campañas de concienciación.

Capítulo VI: Propuesta de Diseño

La propuesta de diseño aquí presentada busca fortalecer la capacidad de BN FONDOS para gestionar incidentes de seguridad de manera eficiente en cumplimiento con la normativa NIST, que fue identificada como la mejor alternativa para responder al problema de la investigación planteada.

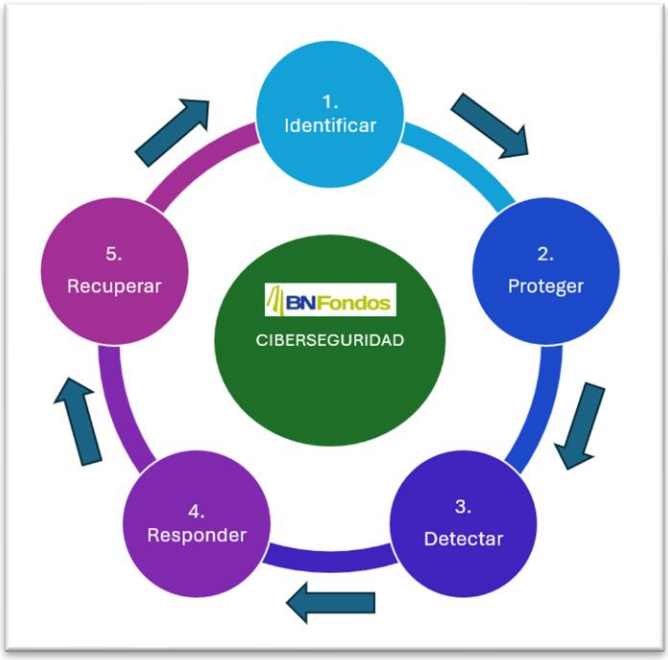
Para ello, a continuación, se plantean los productos y soluciones óptimas en respuesta a los requerimientos identificados en BN FONDOS como son manuales, plantillas e instrucciones de trabajo, así como la selección e implementación de herramientas adecuadas.

Marco de Ciberseguridad NIST CSF 2.0

Como uno de los grandes aspectos identificados durante la investigación la normativa NIST CFS 2.0 facilitó el desarrollo de los siguientes entregables específicos para solucionar el problema de investigación y de esta forma solucionar el requerimiento crítico de atención de incidentes de ciberseguridad para BN FONDOS.

Figura 67

Gestión de Atención de Incidentes



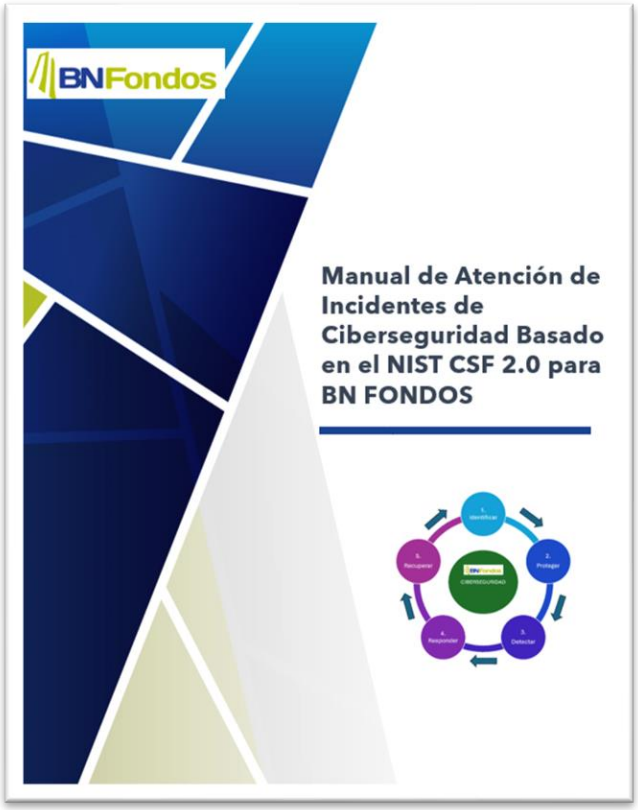
Nota. Ciclo de atención de incidentes para BN FONDOS, elaboración propia, 2024

Propuesta de Manual de Atención de Incidentes de Ciberseguridad Basado en el NIST CSF 2.0 para BN FONDOS

El propósito de este manual es suministrar una guía estructurada para la atención de incidentes de ciberseguridad en BN Fondos, basada en el marco de trabajo NIST Cybersecurity Framework (CSF) 2.0. El manual garantiza la alineación con las mejores prácticas internacionales y cumple con los requisitos regulatorios locales e internos de BN FONDOS.

Figura 68

Manual de Atención de Incidentes de Ciberseguridad



Nota. Portada Manual Atención de Incidentes, elaboración propia. 2024

Los objetivos del manual se definen a continuación:

- Definir los pasos para identificar, contener, erradicar y recuperarse de un incidente de ciberseguridad.
- Establecer roles y responsabilidades para el equipo de respuesta ante incidentes.
- Garantizar la protección de los activos críticos de BN FONDOS, minimizando el impacto de los incidentes de seguridad.

- Implementar procesos continuos de mejora basados en la retroalimentación obtenida de incidentes previos.

El manual se fundamenta en el marco de trabajo NIST CSF 2.0, por lo tanto, se estructura en torno a las cinco funciones clave del NIST CSF 2.0:

Identificar: Reconocimiento de los activos, riesgos y vulnerabilidades que pueden dar lugar a un incidente de ciberseguridad.

Proteger: Implementación de medidas de protección y control para reducir el impacto de los incidentes.

Detectar: Monitorización continua para la identificación temprana de anomalías y eventos de seguridad.

Responder: Planificación y ejecución de actividades de mitigación y contención.

Recuperar: Establecimiento de planes de recuperación y restauración de los servicios afectados.

Proceso de Atención de Incidentes

El proceso de atención de incidentes propone establecerse en las siguientes 5 fases:

Identificación de Incidentes, a continuación, se listan las acciones a seguir para la identificación de identificación de incidentes:

Detección y Notificación: cualquier miembro del personal de BN FONDOS que identifique una actividad sospechosa debe notificarla inmediatamente al Equipo de Respuesta ante Incidentes (CSIRT).

Clasificación y Priorización: el CSIRT evaluará el incidente con base en su gravedad, impacto potencial y urgencia, clasificando los incidentes en niveles: Crítico, Alto, Medio y Bajo.

Contención del Incidente, a continuación, se enuncian los métodos de contención de incidentes:

Contención Temporal: aislar los sistemas comprometidos para evitar que el incidente se propague, garantizando la continuidad de las operaciones críticas.

Contención a Largo Plazo: implementar soluciones temporales hasta que se establezcan las acciones correctivas definitivas.

Erradicación del Incidente, para la erradicación de incidentes se debe tomar en consideración:

Eliminación de la Causa Raíz: identificar la causa del incidente y eliminar cualquier malware, acceso no autorizado o vulnerabilidad.

Validación de Limpieza: asegurarse de que todos los sistemas estén limpios y restaurados a su estado seguro.

Recuperación, para la recuperación o restauración se debe considerar los siguientes puntos:

Restauración de Sistemas: Reintegrar los sistemas y servicios afectados, asegurando que las actualizaciones de seguridad estén instaladas y configuradas correctamente.

Monitoreo Post-Incidente: Realizar un seguimiento detallado para asegurar que no haya recurrencias del incidente.

Lecciones Aprendidas, a continuación, se muestran las acciones a seguir para las lecciones aprendidas:

Análisis Post-Incidente: Documentar el incidente, las acciones tomadas y las lecciones aprendidas. Este análisis se utilizará para mejorar los procesos y fortalecer las defensas de ciberseguridad.

Reporte y Comunicación: Proveer un informe final a la alta gerencia, incluyendo recomendaciones para prevenir futuros incidentes similares.

Roles y Responsabilidades

Los roles y responsabilidades de este manual se establecen de la siguiente manera:

CSIRT (Equipo de Respuesta a Incidentes): Responsable de coordinar todas las actividades relacionadas con la gestión de incidentes, desde la detección hasta la recuperación.

Equipo de TI: Apoyar con la contención técnica y la recuperación de sistemas.

Departamento Legal: Asesorar sobre los aspectos regulatorios y de cumplimiento.

Comunicación y Relaciones Públicas: Manejo de la comunicación interna y externa, asegurando una respuesta clara y coordinada.

Capacitación y Simulacros

Para la capacitación y simulacro se debe tomar en consideración:

Capacitación Continua: Todo el personal de BN Fondos debe recibir formación periódica sobre la detección de incidentes de ciberseguridad y los procedimientos de respuesta.

Simulacros: Realizar simulacros regulares para probar la efectividad del proceso de respuesta a incidentes.

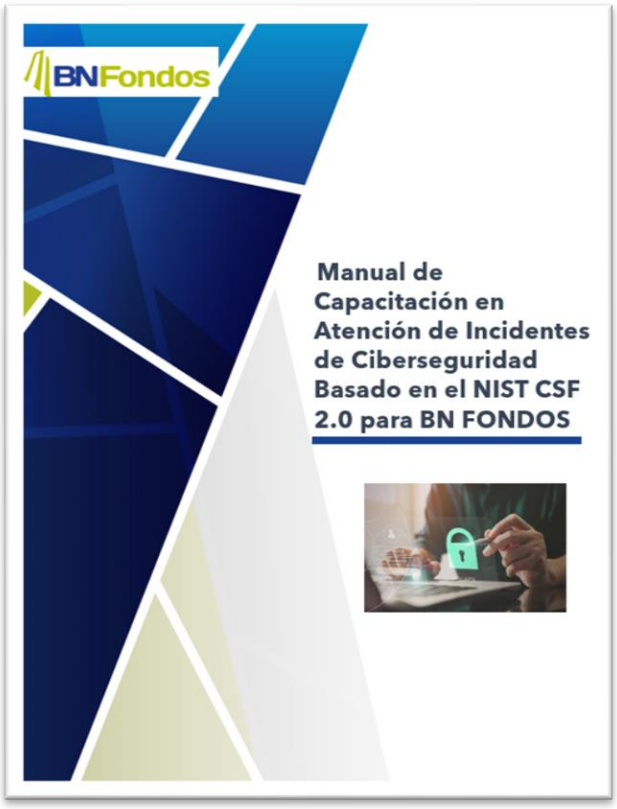
Propuesta de Manual de Capacitación en Atención de Incidentes de Ciberseguridad Basado en el NIST CSF 2.0 para BN FONDOS

El presente manual tiene como objetivo proporcionar un programa de capacitación estructurado para el personal de BN FONDOS, con el fin de fortalecer la capacidad de respuesta ante incidentes de ciberseguridad. La capacitación se basa en el marco de trabajo NIST

Cybersecurity Framework (CSF) 2.0, enfocándose en las cinco funciones esenciales para gestionar los riesgos de ciberseguridad.

Figura 69

Manual de Capacitación en Atención de Incidentes de Ciberseguridad



Nota. Portada Manual Capacitación Atención Incidentes, elaboración propia. 2024

Los objetivos del manual de capacitación se pueden definir en:

- Capacitar al personal de BN Fondos en la detección, respuesta y gestión efectiva de incidentes de ciberseguridad.
- Fomentar una cultura organizacional orientada a la ciberseguridad.

- Garantizar que todos los empleados conozcan sus roles y responsabilidades en caso de un incidente.
- Reforzar la capacidad de recuperación de BN Fondos frente a incidentes de ciberseguridad.

El programa de capacitación se divide en módulos temáticos basados en las cinco funciones del NIST CSF 2.0: Identificar, Proteger, Detectar, Responder y Recuperar. Cada módulo está diseñado para cubrir tanto conceptos teóricos como ejercicios prácticos.

Módulo 1: Identificar, el objetivo de este módulo es de capacitar al personal para reconocer activos críticos, evaluar riesgos y comprender vulnerabilidades que podrían desencadenar un incidente; el contenido de este módulo se fundamenta en:

- Inventario de activos.
- Evaluación de riesgos y análisis de impacto.
- Identificación de vulnerabilidades y amenazas.
- Ejercicio práctico: realizar la elaboración de un mapa de riesgos para un sistema crítico de BN FONDOS.

Módulo 2: Proteger, en este módulo se proveerán los conocimientos sobre las medidas de protección y control que BN FONDOS debe implementar para mitigar incidentes de ciberseguridad; el contenido será:

- Control de acceso y gestión de identidades.
- Prácticas seguras de gestión de la información.
- Mecanismos de protección de datos y sistemas.

- Ejercicio práctico: efectuar la configuración de controles de acceso en un sistema simulado.

Módulo 3: Detectar, en este módulo se pretende capacitar al personal en la detección oportuna de incidentes de ciberseguridad a través de la monitorización continua y el análisis de eventos; el contenido será:

- Herramientas y tecnologías de monitoreo.
- Indicadores de compromiso (IoCs).
- Proceso de notificación y escalación de incidentes.
- Ejercicio práctico: realizar una simulación de detección de anomalías en un entorno de red controlado.

Módulo 4: Responder, el objetivo de este módulo es enseñar al personal los procedimientos adecuados para contener, mitigar y comunicar incidentes de ciberseguridad; como contenido se propone:

- Proceso de gestión de incidentes: preparación, detección, análisis, contención, erradicación y recuperación.
- Roles y responsabilidades en el equipo de respuesta a incidentes (CSIRT).
- Comunicación durante y después del incidente.
- Ejercicio práctico: efectuar una simulación de respuesta a un incidente crítico en BN FONDOS.

Módulo 5: Recuperar, en este módulo se pretende instruir al personal sobre las estrategias de recuperación de sistemas y restauración de operaciones tras un incidente de ciberseguridad; el contenido de este módulo es:

- Desarrollo y aplicación de planes de recuperación.
- Restauración de datos y sistemas comprometidos.
- Validación post-incidente y análisis de lecciones aprendidas.
- Ejercicio práctico: simulación de recuperación de un sistema crítico con validación de la integridad de los datos.

Roles y Responsabilidades Durante la Capacitación

Los roles y responsabilidades de este manual se establecen de la siguiente manera:

CSIRT (Equipo de Respuesta a Incidentes): Coordinará los entrenamientos prácticos y brindará apoyo técnico durante los simulacros.

Departamento de TI: Apoyará con la infraestructura necesaria para realizar las simulaciones y pruebas de conceptos.

Personal de BN FONDOS: Participará activamente en todas las actividades de formación, simulacros y evaluaciones para asegurar el conocimiento integral de las prácticas de respuesta a incidentes.

Evaluación de la Capacitación

Cada módulo incluirá evaluaciones para medir el grado de conocimiento adquirido por los participantes. Las evaluaciones pueden consistir en:

Pruebas teóricas: Evaluar la comprensión de conceptos clave de ciberseguridad.

Ejercicios prácticos: Medir la capacidad de aplicar los conocimientos en situaciones simuladas.

Simulacros de Incidentes: Evaluar la respuesta colectiva del equipo ante escenarios de ciberseguridad.

Simulacros y Pruebas Continuas

La capacitación incluye simulacros regulares de incidentes de ciberseguridad, donde se simulan diversos tipos de ataques para poner a prueba los conocimientos y procedimientos establecidos que estos simulacros permitirán:

Mejorar la coordinación entre los diferentes departamentos involucrados en la respuesta a incidentes.

Detectar áreas de mejora en la respuesta y gestión de incidentes.

Hay que asegurar que los procedimientos establecidos sean eficaces y estén actualizados.

Revisión y Actualización del Manual de Capacitación

El manual de capacitación debe revisarse de manera periódica, al menos una vez al año o después de cualquier incidente mayor, para incorporar mejoras basadas en las lecciones aprendidas y los cambios en el entorno de amenazas.

Propuesta de Procedimiento de Gestión de Roles y Responsabilidades para la Atención de Incidentes de Ciberseguridad Basado en el NIST CSF 2.0 para BN FONDOS

Este documento propone un procedimiento para la gestión de roles y responsabilidades en la atención de incidentes de ciberseguridad en BN FONDOS, conforme al marco de trabajo NIST Cybersecurity Framework (CSF) 2.0.

Figura 70

Procedimiento Roles y Responsabilidades

Nota. Portada Manual Procedimiento de Gestión y Roles, elaboración propia. 2024

El objetivo es asegurar una respuesta coordinada y eficiente ante cualquier incidente, estableciendo claramente las funciones de cada participante involucrado en el proceso de atención; como objetivos del procedimiento se determina:

- Definir los roles y responsabilidades del personal que participa en la atención de incidentes de ciberseguridad.
- Asegurar una respuesta rápida y coordinada para minimizar el impacto de los incidentes.

- Promover una estructura organizacional clara para la gestión de incidentes.
- Facilitar la rendición de cuentas y la mejora continua en el proceso de gestión de incidentes.

Estructura de Roles y Responsabilidades

Los roles y responsabilidades de este manual se establecen de la siguiente manera:

Comité de Respuesta a Incidentes de Ciberseguridad (CSIRT)

Las responsabilidades del comité son:

- Coordinar la respuesta general a incidentes de ciberseguridad.
- Definir las políticas y procedimientos para la gestión de incidentes.
- Tomar decisiones estratégicas relacionadas con la contención, mitigación y comunicación del incidente.
- Supervisar la implementación de mejoras después de cada incidente.

El comité de respuesta debe estar compuesto de la siguiente manera:

- Director de TI: líder del comité y responsable de la toma de decisiones finales.
- Responsable de Seguridad de la Información (CISO): responsable de la supervisión de las acciones técnicas y del aseguramiento del cumplimiento de normativas.
- Responsable de Operaciones: coordina las actividades operativas afectadas por el incidente.
- Departamento Legal: asegura que la respuesta cumple con las regulaciones locales y las políticas internas.

- Relaciones Públicas: gestiona la comunicación pública relacionada con el incidente.

Equipo Técnico de Respuesta a Incidentes (Equipo CSIRT Operativo)

Las responsabilidades del equipo técnico de respuesta a incidentes son:

- Detección, contención, mitigación y erradicación del incidente.
- Análisis técnico detallado de los sistemas afectados.
- Implementación de medidas técnicas para contener la amenaza.
- Coordinación con terceros (proveedores o consultores) en caso de que sea necesario soporte externo.

Los roles claves se determinan a continuación:

- Ingeniero de Redes: Encargado de gestionar el tráfico de red para identificar y contener anomalías.
- Administrador de Sistemas: Responsable de la integridad y recuperación de los sistemas afectados.
- Especialista en Seguridad: Realiza análisis forense y recomienda medidas de seguridad adicionales.
- Responsable de Monitoreo: Monitorea la infraestructura crítica para detectar comportamientos sospechosos.

Personal de Soporte

Las responsabilidades del personal de soporte son:

- Proporcionar apoyo en las actividades de recuperación y normalización de las operaciones.
- Colaborar en la implementación de medidas de seguridad tras el incidente.
- Notificar al equipo de respuesta sobre posibles anomalías o eventos sospechosos.

Los roles claves del personal de soporte son:

- Soporte Técnico de Primer Nivel: recepción inicial de reportes de incidentes y escalamiento hacia el equipo CSIRT operativo.
- Soporte Técnico de Segundo Nivel: brinda asistencia técnica avanzada y ejecuta tareas de recuperación bajo la dirección del equipo CSIRT.

Proceso de Gestión de Roles y Responsabilidades

El proceso de gestión de roles y responsabilidades se detalla a continuación:

Identificación del Incidente

- Responsable: personal de soporte y equipo de monitoreo.
- Acciones: detectar posibles incidentes, recolectar información inicial y escalar según la criticidad.

Activación del CSIRT

- Responsable: ingeniero de redes o administrador de sistemas.
- Acciones: posterior a la identificación de un incidente, se activará el CSIRT operativo, quien realizará una evaluación inicial del incidente.

Clasificación y Priorización del Incidente

- Responsable: CISO y director de TI.

- Acciones: evaluar el impacto del incidente sobre las operaciones y clasificarlos según su gravedad (Crítico, Alto, Medio, Bajo).

Contención del Incidente

- Responsable: equipo CSIRT operativo.
- Acciones: implementar medidas inmediatas de contención para evitar la propagación del incidente, como aislar sistemas o bloquear accesos no autorizados.

Erradicación y Recuperación

- Responsable: administrador de sistemas y especialista en seguridad.
- Acciones: erradicar la causa raíz del incidente, restaurar los sistemas a su estado seguro y validar que no existan amenazas persistentes.

Comunicación Interna y Externa

- Responsable: relaciones públicas y CISO.
- Acciones: informar al personal interno y a las partes externas interesadas, según la política de comunicación establecida por el CSIRT.

Documentación y Lecciones Aprendidas

- Responsable: CISO y equipo técnico de respuesta.
- Acciones: documentar el incidente, las acciones tomadas y las lecciones aprendidas para futuras mejoras del proceso de gestión de incidentes.

Mantenimiento y Actualización de Roles y Responsabilidades

A continuación, se detallas las acciones de mantenimiento y actualización de roles y responsabilidades:

Actualización Periódica: Los roles y responsabilidades deben revisarse y actualizarse anualmente o cuando ocurran cambios importantes en la estructura organizativa o en el entorno de amenazas.

Capacitación Continua: Todos los empleados deben recibir capacitación periódica sobre sus roles específicos y participar en simulacros de incidentes para asegurar una preparación constante.

Simulacros y Evaluación del Desempeño

Es fundamental realizar simulacros periódicos para asegurar que todos los roles y responsabilidades estén claramente definidos y que el personal esté preparado para actuar en caso de incidentes reales. Los simulacros incluirán evaluaciones del tiempo de respuesta y la efectividad de la coordinación entre los distintos equipos.

Propuesta de Procedimiento Recuperación ante Desastres para la Atención de Incidentes de Ciberseguridad Basado en el NIST CSF 2.0 para BN FONDOS

Este documento propone un plan de recuperación ante desastres (Disaster Recovery Plan, DRP) para la atención de incidentes de ciberseguridad en BN FONDOS, basado en el marco NIST Cybersecurity Framework (CSF) 2.0.

Figura 71

Procedimiento Recuperación ante Desastres

Nota. Portada Manual Procedimiento Recuperación ante Desastres, elaboración propia. 2024

Este plan busca restaurar las operaciones críticas afectadas por incidentes de ciberseguridad, minimizando el impacto sobre los activos, la reputación y los servicios financieros proporcionados por la entidad; el objetivo del Plan de Recuperación Ante Desastres se determina por medio de las siguientes acciones:

- Restaurar rápidamente las funciones críticas de negocio tras un incidente de ciberseguridad.
- Minimizar el tiempo de inactividad y el impacto en las operaciones.

- Hay que asegurar que los procesos de recuperación sean eficaces, consistentes y coordinados con los roles establecidos.
- Cumplir con las normativas regulatorias y las mejores prácticas de la industria.

Fase de Recuperación ante desastres BN FONDOS con base en NIST CSF 2.0

Para BN FONDOS y según lo indicado por el marco NIST CSF 2.0 se establece que la fase de Recuperación debe planificarse en los siguientes aspectos:

Planificación y Estrategias de Recuperación: Desarrollo de procedimientos claros para la restauración de sistemas y operaciones.

Mejora Continua: Evaluación y aprendizaje de los incidentes para mejorar los planes de recuperación.

Comunicación: Gestión de la comunicación efectiva durante y después del incidente.

Elementos Clave del Plan de Recuperación

Identificación de los Activos Críticos, es esencial identificar los sistemas y servicios que BN FONDOS considera críticos para sus operaciones:

Sistemas Financieros: Bases de datos y aplicaciones que gestionan las transacciones de clientes.

Sistemas de Seguridad: Herramientas que protegen la confidencialidad e integridad de la información.

Infraestructura de Comunicaciones: Redes, servidores y sistemas de respaldo.

Los objetivos de Tiempo de Recuperación (RTO) y Punto de Recuperación (RPO)

RTO: Tiempo máximo aceptable para restaurar un sistema después de un incidente (24 horas para los sistemas financieros, por ejemplo).

RPO: Punto en el tiempo al que los datos deben ser recuperados tras una interrupción (máximo 1 hora de pérdida de datos en sistemas críticos).

Procedimientos de Recuperación Ante Desastres

El procedimiento de recuperación ante desastres se enuncia a continuación:

Activación del Plan de Recuperación

Responsable: El CISO activará el plan cuando un incidente de ciberseguridad comprometa los sistemas críticos de BN FONDOS. Como acciones inmediatas se consideran:

- Evaluar el alcance del daño.
- Determinar si el incidente amerita la activación total del DRP o solo una recuperación parcial.
- Activar los recursos de emergencia y el personal designado.

Restauración de Sistemas

Fase 1: Contención Inicial, la acción consiste en asegurar que la amenaza ha sido contenida antes de proceder a la recuperación de los sistemas afectados. Esto puede incluir la desconexión de redes, eliminación de malware, bloqueo de accesos no autorizados.

Fase 2: Restauración, la acción se determina en implementar las estrategias de respaldo y restauración previamente definidas; restaurar copias de seguridad de datos desde sistemas locales o en la nube y verificar la integridad de los datos restaurados antes de volver a poner los sistemas en línea.

Fase 3: Validación, acción se determina una vez restaurados los sistemas, se debe realizar una validación exhaustiva para asegurarse de que el sistema funciona correctamente y está libre de vulnerabilidades residuales.

Recuperación de Datos

Las acciones de recuperación de datos deben tomar en consideración:

Backup Regular: Asegurar que los datos críticos se respalden de manera regular conforme al RPO definido.

Herramientas: Utilización de herramientas automatizadas de respaldo y recuperación para garantizar que los datos se restauren de manera rápida y eficiente.

Comunicación Durante la Recuperación

Para efectuar la comunicación durante la recuperación se debe atender las siguientes acciones:

Responsable: El equipo de Relaciones Públicas coordinará la comunicación externa, mientras que el CSIRT gestionará las comunicaciones internas.

Comunicación Interna: Informar al personal afectado sobre el estado de la recuperación y las acciones que deben tomar.

Comunicación Externa: Informar a los clientes y las autoridades regulatorias de manera transparente si es necesario, asegurando el cumplimiento normativo.

Plan de Mejora Continua

Para el plan de mejora continua se deben tomar en consideración las siguientes acciones:

Lecciones Aprendidas: después de cada incidente, es crucial realizar una revisión exhaustiva del evento y del proceso de recuperación; las áreas a revisar incluyen:

- Evaluación del tiempo de recuperación real frente a los RTO y RPO definidos.
- Identificación de los puntos débiles en la infraestructura o los procedimientos.
- Actualización del plan de recuperación con base en las lecciones aprendidas.

Actualización del Plan

El plan de recuperación debe revisarse periódicamente, al menos una vez al año o tras incidentes significativos, para reflejar cambios en la infraestructura, tecnología y amenazas.

Simulacros y Pruebas de Recuperación

Las acciones para los simulacros y pruebas de recuperación se determinan a continuación:

Simulacros Regulares: Realizar simulacros de recuperación para asegurar que el personal esté preparado y que las estrategias de recuperación funcionen según lo previsto.

Evaluación del Desempeño: Medir la efectividad de los simulacros y ajustar los procedimientos según sea necesario.

Responsabilidades Clave en la Recuperación

Las responsabilidades se determinan de la siguiente manera:

Director de TI

- Responsabilidad: Supervisar la ejecución global del plan de recuperación.
- Tareas: Asegurar que los sistemas críticos se restauren en el tiempo definido.

Equipo CSIRT

- Responsabilidad: Implementar las estrategias de contención y recuperación.
- Tareas: Ejecutar las restauraciones, validar los sistemas y comunicar el estado de la recuperación.

Departamento de Operaciones

El departamento de operaciones se le definen las siguientes acciones:

- Responsabilidad: Coordinar la reactivación de las operaciones afectadas.
- Tareas: Garantizar que los servicios financieros se restablezcan según lo planeado.

Revisión del Plan de Recuperación

El plan será evaluado y actualizado periódicamente:

- Frecuencia: Al menos una vez al año, o después de cualquier incidente mayor.
- Responsable: CISO y el Comité de Gestión de Riesgos.

Ejemplos de Plantillas

Como parte de la propuesta de diseño se recomienda el uso y aplicación del ciclo de mejora continua de Deming de todas las plantillas indicadas, a continuación, con el objetivo de llevar controles detallados y actualizados del cumplimiento de los manuales, políticas y procedimientos diseñados como respuesta al proceso de investigación dado en el presente documentos.

Figura 72

Plantillas

Nota. Portada Manual Ejemplos de Plantillas, elaboración propia. 2024

Tabla 13

Plantilla para la Función "Identificar"

Categoría	Subcategoría	Descripción	Estado Actual	Plan de Mejora	Responsable	Fecha de Evaluación
Gobernanza de Ciberseguridad	ID. GV-1: Políticas y Procedimientos	Implementación de políticas de ciberseguridad	Completo	Revisión anual	CISO	01/10/2024
Gestión de Riesgos	ID.RM-1: Evaluación de Riesgos	Evaluación continua de riesgos para activos clave	Incompleto	Realizar una evaluación trimestral	Director de TI	15/09/2024
Gestión de Activos	ID.AM-2: Inventario de Activos	Mantener un inventario actualizado de hardware y software	Parcial	Implementar solución automatizada	Responsable de TI	01/08/2024

Nota. Elaboración propia. 2024

Tabla 14

Plantilla para la Función "Proteger"

Categoría	Subcategoría	Descripción	Estado Actual	Plan de Mejora	Responsable	Fecha de Evaluación
Protección de Datos	PR.DS-1: Protección de Datos en Tránsito y Reposo	Implementar cifrado de datos en tránsito y reposo	Parcial	Completar cifrado en servidores	Responsable de Redes	05/09/2024
Capacitación de Personal	PR.AT-2: Capacitación de Ciberseguridad	Capacitar al personal en procedimientos de seguridad	Completo	Revisión y actualización anual	Recursos Humanos	10/10/2024
Control de Acceso	PR.AC-1: Políticas de Control de Acceso	Revisión de políticas de acceso a sistemas	Parcial	Implementar control basado en roles	Administrador de Sistemas	20/08/2024

Nota: Elaboración propia, 2024, datos obtenidos por medio del análisis efectuado a la normativa NIST

Tabla 15

Plantilla para la Función "Detectar"

Categoría	Subcategoría	Descripción	Estado Actual	Plan de Mejora	Responsable	Fecha de Evaluación
Monitoreo de Anomalías	DE.AE-1: Monitoreo de Actividades	Implementación de monitoreo de tráfico en la red	Completo	Revisión mensual	Ingeniero de Redes	01/10/2024
Detección de Incidentes	DE.CM-1: Detección de Eventos	Detección de anomalías en sistemas clave	Incompleto	Configurar alertas automatizadas	Especialista en Seguridad	15/09/2024
Análisis Forense	DE.CM-7: Análisis Post-Incidente	Implementar herramientas para análisis forense	Parcial	Adquirir herramientas especializadas	Director de TI	30/09/2024

Nota: Elaboración propia, 2024, datos obtenidos por medio del análisis efectuado a la normativa NIST

Tabla 16

Plantilla para la Función "Responder"

Categoría	Subcategoría	Descripción	Estado Actual	Plan de Mejora	Responsable	Fecha de Evaluación
Planificación de Respuesta	RS.RP-1: Plan de Respuesta a Incidentes	Definir el plan de acción ante incidentes de seguridad	Completo	Revisión trimestral	CISO	01/07/2024
Análisis de Incidentes	RS.AN-1: Análisis de Impacto	Evaluar el impacto de los incidentes detectados	Parcial	Implementar evaluación automatizada	Equipo CSIRT	15/09/2024
Comunicación en Incidentes	RS.CO-2: Comunicación con Partes Externas	Definir protocolos de comunicación con terceros	Incompleto	Crear plan de comunicación externa	Relaciones Públicas	10/10/2024

Nota: Elaboración propia, 2024, datos obtenidos por medio del análisis efectuado a la normativa NIST

Tabla 17

Plantilla para la Función "Recuperar"

Categoría	Subcategoría	Descripción	Estado Actual	Plan de Mejora	Responsable	Fecha de Evaluación
Recuperación de Servicios	RC.RP-1: Estrategias de Recuperación	Implementar procesos de restauración para sistemas críticos	Parcial	Completar implementación de copias de seguridad automáticas	Administrador de Sistemas	01/09/2024
Mejora Continua	RC.IM-2: Lecciones Aprendidas	Evaluación post-incidente para mejorar el plan de recuperación	Incompleto	Establecer revisión post-incidente	CISO	15/10/2024
Comunicación de Recuperación	RC.CO-3: Comunicación Post-Incidente	Informar a las partes afectadas sobre la recuperación de sistemas	Completo	Revisión trimestral	Relaciones Públicas	20/09/2024

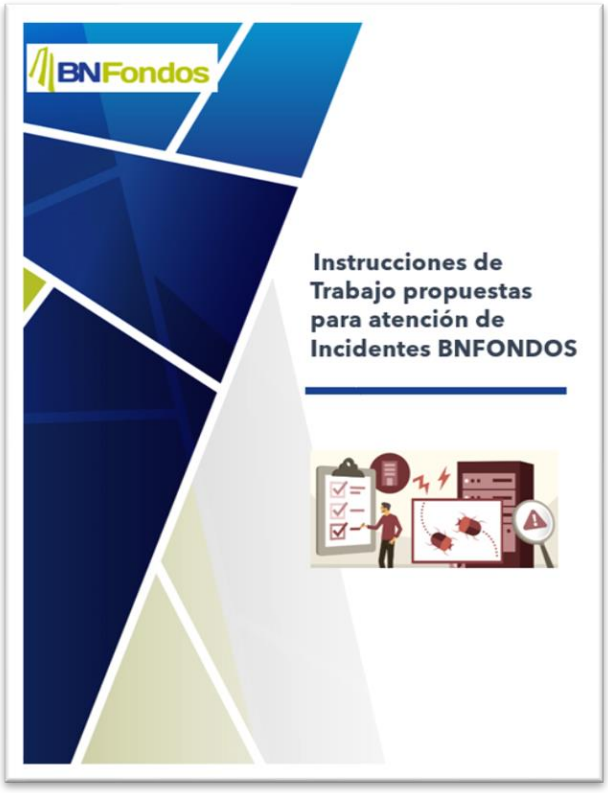
Nota: Elaboración propia, 2024, datos obtenidos por medio del análisis efectuado a la normativa NIST

Instrucciones de Trabajo propuestas para atención de Incidentes BNFONDOS

A continuación, se presenta la propuesta de instrucciones de trabajo que acompañan a los manuales para su correcta implementación y aplicación en cada una de las fases.

Figura 73

Instrucciones de Trabajo



Nota. Portada Manual Instrucciones de Trabajo para atención de incidentes, elaboración propia. 2024

Instrucciones para la Función "Identificar"

Figura 74

Función Identificar

Nota. Fase 1 Identificar, elaboración propia. 2024

Gestión de Activos

El objetivo de esta gestión es mantener un inventario actualizado de activos que permita identificar vulnerabilidades y riesgos en los sistemas. Se basa en las siguientes instrucciones:

Crear inventario de activos:

- Identificar todos los activos de hardware y software dentro de la organización.
- Asignar responsables para cada activo.

Actualizar el inventario trimestralmente:

- Revisar y actualizar cualquier cambio en la infraestructura (nuevas adquisiciones, bajas o actualizaciones).

Asignar clasificaciones a los activos según su importancia (alta, media, baja).

Documentar la dependencia de los activos críticos para el negocio.

Reportar cualquier discrepancia o activo no registrado.

Gestión de Riesgos

El objetivo es evaluar y gestionar los riesgos de ciberseguridad para minimizar la probabilidad y el impacto de incidentes. Sus instrucciones son:

- Realizar evaluaciones de riesgos semestralmente.
- Identificar amenazas para cada activo crítico.
- Calcular el nivel de riesgo combinando la probabilidad de ocurrencia y el impacto potencial.
- Revisar las medidas de mitigación actuales y recomendar mejoras.
- Documentar los resultados de la evaluación y entregar informes al equipo directivo.

Instrucciones para la Función "Proteger"

Figura 75

Función Proteger

Nota. Fase 2 Proteger, elaboración propia. 2024

Control de Acceso

Su objetivo es garantizar que solo usuarios autorizados tengan acceso a los sistemas y datos sensibles, sus instrucciones son:

- Implementar autenticación multifactor (MFA) en todas las aplicaciones y sistemas críticos.
- Revisar los permisos de acceso trimestralmente.
- Aplicar políticas de contraseñas seguras: longitud mínima de 12 caracteres, renovación cada 90 días.
- Revocar inmediatamente los accesos cuando un empleado sea desvinculado.
- Monitorear actividades inusuales relacionadas con accesos no autorizados y generar alertas.

Protección de Datos

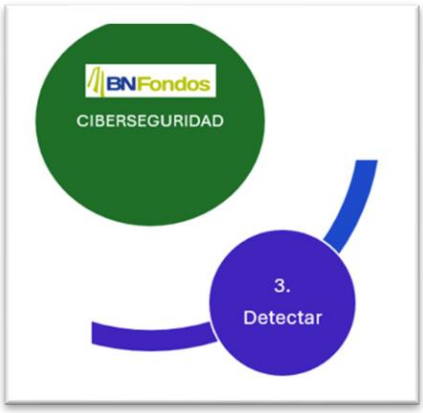
Su objetivo es proteger los datos sensibles tanto en tránsito como en reposo para prevenir accesos no autorizados; sus instrucciones son:

- Implementar cifrado de datos en reposo y en tránsito utilizando estándares como AES-256.
- Monitorear y revisar el cifrado de datos en reposo trimestralmente.
- Crear copias de seguridad automáticas de datos críticos diariamente y almacenarlas en una ubicación segura.
- Restringir el acceso a las copias de seguridad solo a personal autorizado.
- Documentar las políticas de retención y destrucción de datos sensibles.

Instrucciones para la Función "Detectar"

Figura 76

Función Detectar



Nota. Fase 3 Detectar, elaboración propia. 2024

Monitoreo Continuo

El objetivo es detectar de manera proactiva actividades anómalas y posibles incidentes de seguridad; sus instrucciones se basan en:

- Configurar herramientas de monitoreo (ejemplo herramientas SIEM) para la supervisión de tráfico y eventos.
- Establecer umbrales de alertas para detectar actividades inusuales.
- Revisar los registros de eventos diariamente para identificar posibles incidentes.
- Realizar pruebas de detección cada trimestre para verificar la efectividad de los controles.
- Notificar inmediatamente al equipo de respuesta ante incidentes cuando se detecte una actividad sospechosa.

Análisis de Vulnerabilidades

Su objetivo es identificar vulnerabilidades en los sistemas que puedan ser explotadas por atacantes; sus instrucciones son:

- Ejecutar escaneos de vulnerabilidades trimestralmente en todos los sistemas críticos.
- Analizar los resultados del escaneo e identificar las vulnerabilidades críticas.
- Asignar responsables para la mitigación de cada vulnerabilidad identificada.
- Reparar las vulnerabilidades de alta criticidad dentro de los primeros 7 días.
- Documentar el ciclo de vida de la vulnerabilidad desde su descubrimiento hasta su resolución.

Instrucciones para la Función "Responder"

Figura 77

Función Responder

Nota. Fase 4 Responder, elaboración propia. 2024

Plan de Respuesta a Incidentes

Su objetivo es desarrollar un plan de respuesta efectivo para minimizar el impacto de los incidentes de ciberseguridad; sus instrucciones son:

- Definir un equipo de respuesta a incidentes (CSIRT) con roles claros.
- Crear un protocolo de escalación para incidentes según su nivel de severidad.
- Documentar todos los pasos seguidos durante la respuesta a un incidente.
- Probar el plan de respuesta mediante simulaciones anuales de incidentes.
- Evaluar el impacto de la respuesta post-incidente y ajustar el plan según sea necesario.

Análisis Post-Incidente

El objetivo es realizar un análisis detallado de los incidentes para identificar lecciones aprendidas; sus instrucciones son:

- Recolectar toda la información disponible sobre el incidente.
- Analizar la causa raíz del incidente.
- Determinar el impacto en los activos críticos y en la operación del negocio.
- Recomendar mejoras en los controles de seguridad para prevenir incidentes similares.
- Entregar un informe detallado al equipo directivo con las lecciones aprendidas.

Instrucciones para la Función "Recuperar"

Figura 78

Función Recuperar

Nota. Fase 5 Recuperar, elaboración propia. 2024

Restauración de Sistemas

El objetivo es restaurar los sistemas afectados de BN FONDOS de manera eficiente tras un incidente; sus instrucciones son:

- Priorizar los sistemas críticos para la restauración.
- Utilizar copias de seguridad para restaurar datos afectados por el incidente.
- Verificar la integridad de los sistemas y datos restaurados antes de volver a la operación normal.
- Coordinar con el equipo de TI para asegurar que todas las dependencias estén en funcionamiento.
- Documentar el proceso de restauración y las lecciones aprendidas.

Comunicación Post-Incidente

El objetivo es garantizar una comunicación efectiva con las partes interesadas después de un incidente, sus instrucciones son:

- Informar a los directivos inmediatamente sobre la resolución del incidente.
- Notificar a las partes afectadas (clientes, socios) sobre el estado de los sistemas restaurados.
- Coordinar con el equipo de relaciones públicas para emitir comunicados externos si es necesario.
- Realizar una revisión post-incidente con el equipo para evaluar el proceso de recuperación.
- Actualizar las políticas de comunicación según las lecciones aprendidas del incidente.

Políticas propuestas

Como parte de los resultados obtenidos se requiere implementar las siguientes políticas de atención de incidentes en BNFONDOS:

Política de Atención de Incidentes de Ciberseguridad para BN FONDOS

El propósito de esta política tiene es establecer un marco formal y estructurado para la detección, respuesta y recuperación ante incidentes de ciberseguridad en BN FONDOS, alineado con el Marco NIST Cybersecurity Framework (CSF) 2.0. Esta política busca minimizar los impactos operativos, financieros y reputacionales, garantizando una respuesta rápida y efectiva ante incidentes que puedan comprometer la seguridad de la información y los sistemas.

Figura 79

Política de Atención de Incidentes

Nota. Portada Manual Política de Atención de Incidentes, elaboración propia. 2024

El alcance de esta política aplica a todo el personal de BN FONDOS, incluyendo empleados, proveedores, contratistas y socios de terceros que tengan acceso a los sistemas y datos de la organización. Cubre todos los activos de información, sistemas de TI, aplicaciones, redes y datos manejados por la empresa, así como el tratamiento de incidentes de ciberseguridad que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de estos.

Definiciones:

Incidente de Ciberseguridad: evento que compromete la seguridad de los sistemas de información, incluyendo ataques de malware, robo de datos, accesos no autorizados, violaciones de políticas de seguridad, entre otros.

Equipo de Respuesta a Incidentes (CSIRT): grupo de expertos responsables de gestionar incidentes de ciberseguridad dentro de la organización.

NIST CSF 2.0: marco de trabajo desarrollado por el National Institute of Standards and Technology que establece las mejores prácticas para la gestión de riesgos de ciberseguridad.

Objetivos

- Identificar los riesgos y amenazas de ciberseguridad que puedan afectar los activos críticos de BN Fondos.
- Proteger los sistemas y datos críticos mediante controles de seguridad adecuados.
- Detectar de manera oportuna los incidentes de ciberseguridad a través de monitoreo continuo.
- Responder de forma rápida y coordinada ante incidentes para mitigar su impacto.
- Recuperar los sistemas afectados y restaurar las operaciones normales en el menor tiempo posible.

Principios Generales

- Gestión de Riesgos Proactiva: se implementará una evaluación continua de riesgos para identificar, priorizar y mitigar amenazas antes de que se conviertan en incidentes.
- Cumplimiento Normativo: todos los procedimientos de atención de incidentes cumplirán con las normativas locales e internacionales aplicables, así como con las mejores prácticas definidas por el NIST CSF 2.0.

- Mejora Continua: la respuesta ante incidentes será evaluada regularmente para mejorar la efectividad de las medidas de protección y respuesta.
- Confidencialidad y Minimización de Impacto: se garantizará que la atención de incidentes proteja la confidencialidad de los datos afectados y se minimicen las repercusiones operativas.

Roles y Responsabilidades

Responsables del CSIRT:

- Liderar la gestión de incidentes de ciberseguridad.
- Coordinar la respuesta técnica, legal y comunicacional.
- Documentar y reportar el ciclo de vida de los incidentes.

Personal de TI:

- Implementar y monitorear controles de seguridad para prevenir incidentes.
- Colaborar en la identificación y clasificación de incidentes.
- Proporcionar soporte técnico en la recuperación de sistemas.

Gestores de Riesgos:

- Realizar evaluaciones periódicas de riesgos de ciberseguridad.
- Revisar las lecciones aprendidas tras los incidentes y actualizar las políticas.

Directores de BN FONDOS:

- Aprobar los recursos necesarios para la implementación de medidas de ciberseguridad.
- Garantizar que se mantenga la alineación con los objetivos estratégicos de la organización.

Directrices de Respuesta a Incidentes

- Detección y Clasificación de Incidentes:
- Todos los incidentes de ciberseguridad deben ser reportados inmediatamente al CSIRT.

Los incidentes serán clasificados en función de su criticidad: bajo, medio o alto impacto, basado en el nivel de afectación a los activos críticos y a la operación.

Comunicación y Escalamiento:

- El equipo CSIRT debe notificar a la alta dirección sobre incidentes de alto impacto.
- Se debe mantener una comunicación continua con las partes interesadas internas y, en caso necesario, con autoridades regulatorias y terceros afectados.

Registro y Documentación:

- Cada incidente debe ser registrado en un sistema de seguimiento de incidentes.
- La documentación incluirá detalles sobre la causa raíz, acciones tomadas, tiempo de respuesta y plan de recuperación.

Coordinación con Terceros:

- En casos en los que proveedores o socios sean parte del incidente, se coordinarán las acciones de respuesta en conjunto con ellos para mitigar el impacto.

Fases de Atención de Incidentes

La política de atención de incidentes sigue las cinco fases del NIST CSF 2.0:

- Identificar: Identificación proactiva de activos y riesgos, mediante evaluaciones periódicas y análisis de vulnerabilidades, Implementación de un inventario actualizado de activos y dependencias críticas.

- Proteger: Medidas preventivas como controles de acceso, segmentación de redes, cifrado de datos, políticas de seguridad y capacitaciones continuas para el personal; la realización de simulacros periódicos de incidentes para fortalecer las capacidades de protección.
- Detectar: monitoreo continuo de eventos de seguridad mediante herramientas SIEM y otros sistemas de detección de anomalías, implementación de alertas automáticas para actividades sospechosas.
- Responder: aplicación inmediata de procedimientos de contención, erradicación y mitigación de incidentes y comunicación constante con el equipo CSIRT y actualización del plan de respuesta basado en el tipo de incidente.
- Recuperar: restauración de los sistemas comprometidos, asegurando que no persistan vulnerabilidades, realización de análisis post-incidente para mejorar la postura de ciberseguridad y comunicación a las partes afectadas sobre la resolución del incidente.

Revisión y Actualización

Esta política será revisada anualmente por el equipo de gestión de ciberseguridad y ajustada según sea necesario para reflejar cambios en las amenazas, la tecnología y el marco regulatorio. Asimismo, cualquier incidente significativo que ocurra puede motivar una revisión y actualización inmediata de la política.

Capacitación y Concienciación

Todo el personal de BN FONDOS debe recibir capacitación anual en temas de ciberseguridad, con un enfoque en la detección y respuesta ante incidentes. El equipo CSIRT y

otros responsables clave recibirán entrenamientos especializados y participarán en ejercicios de simulación de incidentes para reforzar su capacidad de respuesta.

Política de Atención de Incidentes de Ransomware para BN FONDOS

El propósito de esta política es establecer un conjunto de directrices para la prevención, detección, respuesta y recuperación ante incidentes de ransomware en BN FONDOS, conforme a las mejores prácticas del Marco NIST Cybersecurity Framework (CSF) 2.0. El enfoque está orientado a minimizar el impacto operativo, financiero y reputacional, garantizando una respuesta rápida y efectiva ante incidentes que comprometan la seguridad de los sistemas y datos.

Figura 80

Política Atención Incidentes Ransomware

Nota. Portada Manual Política Atención Incidentes Ransomware, elaboración propia. 2024

El alcance de esta política aplica a todo el personal de BN FONDOS, incluyendo empleados, contratistas y terceros que tengan acceso a los sistemas y datos de la organización. Se dirige específicamente a la gestión de ataques de ransomware que puedan comprometer la disponibilidad, integridad o confidencialidad de la información y los sistemas de la organización.

Definiciones

- Ransomware: Tipo de malware que cifra los archivos de una organización, denegando el acceso a los mismos y exigiendo un pago (rescate) para restaurar el acceso.
- Incidente de Ransomware: Cualquier evento en el que el ransomware afecte a los sistemas de BN Fondos, comprometiendo la operación o seguridad de los datos.
- NIST CSF 2.0: Marco de trabajo desarrollado por el NIST que proporciona un enfoque estructurado para la gestión de ciberseguridad, incluyendo la preparación y respuesta ante incidentes como ransomware.

Objetivos

- Identificar las vulnerabilidades y riesgos que puedan facilitar un ataque de ransomware.
- Proteger los sistemas de TI y datos mediante controles robustos que prevengan el acceso no autorizado y la propagación de ransomware.
- Detectar de forma temprana cualquier signo de ataque de ransomware a través de monitoreo continuo.
- Responder de manera inmediata y coordinada para mitigar los efectos del ransomware y evitar su expansión.

- Recuperar los datos y restaurar los sistemas afectados de manera segura y en el menor tiempo posible, minimizando la interrupción de las operaciones.

Principios Generales

- Gestión Proactiva de Riesgos: BN Fondos implementará medidas preventivas y evaluaciones periódicas de riesgos para identificar y mitigar las vulnerabilidades explotables por ransomware.
- Mejora Continua: El ciclo de respuesta ante incidentes será revisado y ajustado regularmente para garantizar su efectividad ante las nuevas amenazas de ransomware.
- Cumplimiento Normativo: Esta política cumple con los lineamientos del NIST CSF 2.0 y las regulaciones locales, asegurando que las acciones de atención de ransomware sean consistentes con las mejores prácticas internacionales.

Roles y Responsabilidades

Equipo de Respuesta a Incidentes (CSIRT):

- Coordinar la respuesta inmediata ante incidentes de ransomware.
- Supervisar la contención y erradicación del ransomware.
- Gestionar la comunicación interna y externa durante y después del incidente.
- Proveer informes posts-incidentes para identificar oportunidades de mejora.

Personal de TI:

- Implementar y mantener controles de seguridad como soluciones antivirus, firewalls y sistemas de prevención de intrusiones (IPS).

- Ejecutar planes de contingencia para la recuperación rápida de los sistemas afectados.
- Hay que asegurar que los backups se realicen periódicamente y se almacenen de manera segura.

Gestores de Riesgos:

- Evaluar periódicamente los riesgos asociados con el ransomware.
- Analizar las lecciones aprendidas de cada incidente para actualizar los planes y políticas de ciberseguridad.

Altos Directivos de BN FONDOS:

- Aprobar recursos y estrategias de respuesta ante incidentes de ransomware.
- Tomar decisiones informadas sobre la posible negociación con los atacantes o la restauración de los sistemas desde copias de seguridad.

Directrices de Respuesta a Incidentes de Ransomware

Las directrices de respuesta a incidentes de ransomware se basan en las Fases de Respuesta según el NIST CSF 2.0

Identificar: Realizar análisis de riesgos continuos para identificar los activos más críticos que podrían ser blanco de ataques de ransomware, Mantener un inventario actualizado de los activos digitales y de las vulnerabilidades potenciales, Evaluar la exposición al ransomware mediante auditorías de seguridad regulares y pruebas de penetración.

Proteger: Implementar controles preventivos como soluciones de seguridad de endpoint (antivirus, EDR), segmentación de redes y políticas de administración de accesos, Capacitar a los empleados sobre cómo reconocer intentos de phishing y otros vectores de ataque relacionados

con ransomware, Asegurar que todos los sistemas estén actualizados con los últimos parches de seguridad y realizar copias de seguridad de todos los datos críticos en una infraestructura fuera de línea y asegurarse de que estas copias sean recuperables.

Detectar: monitoreo continuo de los sistemas y redes para identificar comportamientos sospechosos o señales tempranas de ataques de ransomware, establecer alertas automáticas que notifiquen al CSIRT en caso de actividad inusual, como la aparición de grandes cantidades de archivos cifrados o intentos de conexión a dominios conocidos de ransomware.

Responder: contención inmediata: Aislar los sistemas infectados para evitar que el ransomware se propague, análisis del incidente: Determinar el alcance del ataque, los sistemas afectados y la variante específica de ransomware utilizada, comunicación y escalamiento: Notificar a la alta dirección, partes afectadas y posibles autoridades regulatorias si el incidente tiene un impacto significativo.

Erradicación: Limpiar el malware de los sistemas afectados utilizando herramientas de desinfección especializadas y aplicar medidas para cerrar las vulnerabilidades explotadas.

Recuperar: restaurar los sistemas y datos desde copias de seguridad verificadas, verificar que los sistemas restaurados estén completamente libres de ransomware y actualizados con las medidas de seguridad adecuadas, implementar planes de recuperación de operaciones críticas, asegurando que se reanuden las actividades normales de forma segura, realizar un análisis post-incidente para documentar las lecciones aprendidas y mejorar la preparación para futuros ataques.

Procedimientos específicos ante ransomware

Proceso de Contención: desconectar los dispositivos infectados de la red de manera inmediata, suspender temporalmente los servicios no críticos para evitar la propagación del malware y limitar el acceso a las cuentas de usuario hasta que se confirme la seguridad de los sistemas.

Evaluación de Daños: determinar si los datos han sido cifrados o si el ransomware ha sido detectado en una fase temprana sin afectación a los archivos, identificar las cuentas y sistemas comprometidos.

Decisión sobre Pago de Rescate: BN FONDOS, como política general, no pagará rescates. Sin embargo, en casos excepcionales, la decisión final será tomada por la alta dirección, basada en una evaluación de riesgos y tras consultar con expertos legales y de ciberseguridad.

Restauración desde Copias de Seguridad: Garantizar que se utilicen copias de seguridad no comprometidas, verificar que el sistema restaurado esté totalmente funcional y no afectado por el ransomware antes de reintegrarlo a la red.

Capacitación y Simulacros

Todo el personal de BN FONDOS deberá recibir formación regular sobre prevención de ransomware, incluyendo prácticas seguras de manejo de correos electrónicos, navegación y acceso remoto. Además, se realizarán simulacros periódicos de ataques de ransomware para evaluar y mejorar la capacidad de respuesta del equipo CSIRT.

Revisión y Actualización

Esta política será revisada anualmente o después de cualquier incidente significativo de ransomware, para garantizar su adecuación a las nuevas amenazas y cambios en el entorno de

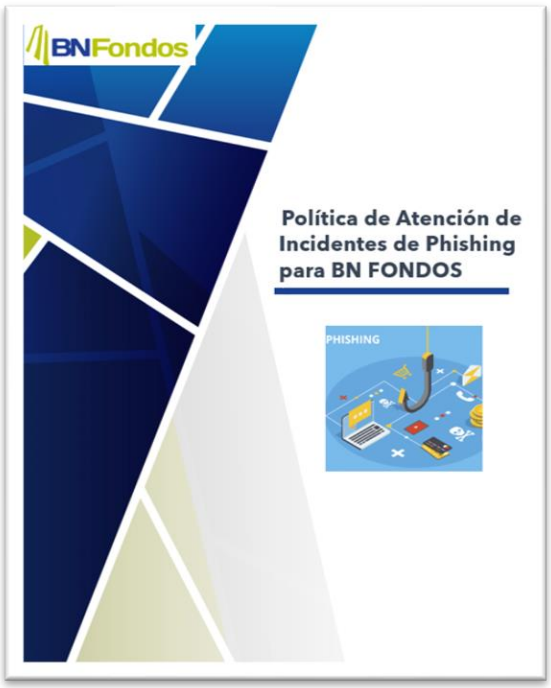
ciberseguridad. Las lecciones aprendidas se incorporarán en las revisiones para fortalecer la postura de ciberseguridad de BN FONDOS.

Política de atención de incidentes de phishing para BN FONDOS

El propósito es establecer una política que guíe la detección, respuesta y recuperación ante incidentes de phishing en BN Fondos, asegurando la protección de la información sensible y los activos críticos de la organización. Esta política está alineada con las mejores prácticas del NIST Cybersecurity Framework (CSF) 2.0 y busca mitigar el impacto operativo, financiero y reputacional que puedan generar estos ataques.

Figura 81

Política Atención Incidentes Phishing



Nota. Portada Manual Política Atención Incidentes Phishing, elaboración propia. 2024

El alcance de esta política aplica a todos los empleados, contratistas, proveedores y socios que tengan acceso a los sistemas de BN FONDOS, y está diseñada para gestionar cualquier tipo de ataque de phishing, incluyendo correos electrónicos, mensajes de texto o llamadas telefónicas que intenten engañar al personal para que revele información sensible o permita acceso no autorizado a los sistemas de la organización.

Definiciones

- Phishing: técnica de ingeniería social utilizada para engañar a las personas a fin de que revelen información confidencial, como credenciales de acceso o detalles financieros, mediante la suplantación de identidad en correos electrónicos, mensajes o llamadas.
- Spear Phishing: variante del phishing en la que los atacantes dirigen los ataques a individuos específicos dentro de la organización, simulando ser una fuente confiable.
- NIST CSF 2.0: marco de trabajo de ciberseguridad del National Institute of Standards and Technology (NIST), que incluye directrices para la preparación, respuesta y recuperación ante incidentes de ciberseguridad.

Objetivos

- Identificar las vulnerabilidades y comportamientos que puedan llevar a ataques de phishing.
- Proteger la infraestructura y los datos críticos de BN Fondos mediante medidas preventivas, como la concientización y formación del personal.
- Detectar y responder oportunamente a cualquier intento de phishing.

- Responder a incidentes de phishing de forma inmediata para contener el ataque y mitigar posibles daños.
- Recuperar la normalidad operativa de manera eficiente y minimizar el impacto del ataque en los sistemas y operaciones de la organización.

Principios Generales

- Educación y Concientización Continua: todo el personal debe recibir formación periódica sobre cómo identificar y reportar intentos de phishing.
- Mejora Continua en la Detección: el monitoreo y análisis de incidentes de phishing se ajustarán y actualizarán regularmente para adaptarse a nuevas tácticas de ataque.
- Resiliencia Operacional: BN FONDOS debe asegurar la continuidad de sus operaciones mediante la implementación de procesos que faciliten la respuesta rápida y la recuperación de sistemas ante incidentes de phishing.

Roles y Responsabilidades

Equipo de Respuesta a Incidentes (CSIRT): coordinar la investigación y respuesta a intentos de phishing, implementar medidas correctivas y preventivas para mitigar futuros ataques, proveer análisis post-incidente y reportes sobre la efectividad de la respuesta.

Personal de TI: implementar soluciones de seguridad como filtros de correos electrónicos y firewalls que bloqueen intentos de phishing, monitorizar y alertar sobre patrones inusuales que sugieran posibles ataques de phishing, garantizar la integridad de los sistemas y datos afectados después de un incidente.

Usuarios Finales: reportar cualquier correo o mensaje sospechoso de phishing siguiendo los procedimientos establecidos, no interactuar con enlaces, archivos adjuntos o solicitudes de información en correos no verificados.

Altos Directivos: asegurar la disponibilidad de recursos necesarios para prevenir y gestionar incidentes de phishing, aprobar y respaldar las decisiones críticas durante la respuesta a un ataque de phishing.

Fases de Respuesta según NIST CSF 2.0

Identificar: realizar evaluaciones periódicas de riesgos para identificar vulnerabilidades que puedan ser explotadas por phishing, mantener un inventario actualizado de todos los sistemas, usuarios y accesos susceptibles de ser atacados mediante técnicas de phishing.

Proteger: implementar autenticación multifactor (MFA) para proteger el acceso a los sistemas más sensibles, configurar filtros avanzados de correos electrónicos que bloqueen mensajes sospechosos antes de que lleguen a los usuarios y actualizar regularmente los sistemas de seguridad y políticas de protección de información para mitigar la exposición.

Detectar: utilizar sistemas automáticos de detección de amenazas para identificar correos electrónicos sospechosos, capacitar al personal para que pueda detectar rápidamente correos, enlaces o archivos adjuntos maliciosos, implementar alertas automáticas que notifiquen al equipo de ciberseguridad sobre cualquier intento fallido de phishing.

Responder: aislar cualquier cuenta o sistema que haya sido comprometido por un ataque de phishing, analizar el alcance del ataque y determinar si se han filtrado datos o credenciales, restablecer las credenciales comprometidas de forma inmediata y bloquear cualquier acceso no autorizado, comunicar el incidente a los empleados y, si es necesario, a las autoridades regulatorias.

Recuperar: reiniciar las operaciones críticas y restaurar el acceso seguro a los sistemas comprometido, revisar y fortalecer las políticas de protección de accesos y la formación del personal, documentar el incidente, identificando las áreas de mejora para prevenir futuros ataques.

Proceso Específico de Atención a Incidentes de Phishing

Identificación y Reporte: los usuarios que reciban un correo sospechoso deben reportarlo inmediatamente al equipo de TI utilizando los canales establecidos, el equipo de TI evaluará el correo o mensaje sospechoso y tomará medidas inmediatas para bloquear el remitente si es necesario.

Análisis de Impacto: determinar si se han expuesto credenciales, datos sensibles o si se ha permitido acceso no autorizado a sistemas, evaluar el nivel de compromiso de la cuenta del usuario afectado y tomar medidas correctivas.

Restauración de Cuentas: restablecer las credenciales comprometidas, he de asegurar que el usuario afectado reciba formación sobre cómo prevenir futuros intentos de phishing.

Notificación: notificar a todos los empleados de la naturaleza del intento de phishing para aumentar la conciencia general y reducir el riesgo de nuevos ataques.

Capacitación y Simulacros

Todo el personal de BN Fondos debe participar en capacitaciones periódicas sobre el reconocimiento de correos y mensajes de phishing. Además, se realizarán simulacros de ataques de phishing para evaluar la capacidad de respuesta y reforzar la cultura de seguridad en la organización.

Revisión y Actualización

Esta política será revisada y actualizada anualmente, o después de cualquier incidente significativo de phishing, para asegurar que cumple con las mejores prácticas y los cambios en las amenazas de seguridad. La retroalimentación y lecciones aprendidas de cada incidente se incorporarán en la revisión para mejorar continuamente la postura de seguridad de BN Fondos.

Política de Atención de Incidentes que Afecten la Ley de Protección de Datos Personales Basado en el NIST CSF 2.0 para BN FONDOS

El propósito de esta política es garantizar que BN FONDOS gestione de manera eficiente cualquier incidente de ciberseguridad que comprometa la protección de los datos personales, en cumplimiento con la Ley de Protección de Datos Personales y alineado con el NIST Cybersecurity Framework (CSF) 2.0. Esta política define procedimientos claros para la prevención, detección, respuesta y recuperación de incidentes que afecten la privacidad de los datos personales.

Figura 82

Política Ley Protección de Datos

Nota. Portada Manual Política Ley de Protección de Datos Personales, elaboración propia. 2024

El alcance de esta política se aplica a todos los empleados, contratistas, proveedores y cualquier tercero que gestione, procese o tenga acceso a los datos personales bajo la responsabilidad de BN FONDOS. Cubre cualquier violación que comprometa la integridad, confidencialidad o disponibilidad de los datos personales.

Definiciones

- Incidente de Seguridad Relacionado con Datos Personales: Evento que compromete la confidencialidad, integridad o disponibilidad de los datos personales protegidos por la ley.

- Datos Personales: Información que identifica o puede identificar a una persona, incluyendo nombre, identificación, información financiera, dirección, entre otros.
- Violación de Datos: Acceso no autorizado, divulgación, alteración, pérdida o destrucción de datos personales.

Objetivos

- Proteger los datos personales bajo la responsabilidad de BN FONDOS mediante controles de seguridad adecuados.
- Prevenir y detectar incidentes de seguridad que comprometan los datos personales.
- Responder rápidamente a incidentes que afecten la protección de datos personales, minimizando el impacto sobre los individuos y la organización.
- Cumplir con las normativas legales vigentes sobre la protección de datos personales y notificar a las autoridades competentes en caso de incidentes.

Principios Generales

Cumplimiento Normativo: BN FONDOS se compromete a cumplir con la Ley de Protección de Datos Personales y otras regulaciones aplicables.

Privacidad por Diseño: La protección de datos personales será integrada en los procesos y sistemas desde su concepción, aplicando principios de privacidad por diseño y por defecto.

Respuesta Eficiente: Los incidentes serán atendidos de manera rápida y efectiva para limitar el daño a los titulares de los datos.

Roles y Responsabilidades

Oficial de Protección de Datos (DPO): supervisar la implementación de esta política y garantizar el cumplimiento de la Ley de Protección de Datos Personales, coordinar la

notificación de las violaciones de datos a las autoridades de protección de datos y a los individuos afectados, según sea requerido.

Equipo de Respuesta a Incidentes de Ciberseguridad (CSIRT): detectar, investigar y mitigar cualquier incidente que afecte los datos personales, colaborar con el DPO en la implementación de acciones correctivas y preventivas.

Departamento de TI: mantener medidas de seguridad para proteger los datos personales de accesos no autorizados y otras amenazas y asegurar la integridad y confidencialidad de los sistemas que gestionan los datos personales.

Empleados y Usuarios Finales: cumplir con las políticas internas de seguridad de la información y reportar inmediatamente cualquier actividad sospechosa o incidente relacionado con datos personales.

Fases de Respuesta Basadas en el NIST CSF 2.0

Identificar: realizar análisis de riesgos de manera continua para identificar vulnerabilidades que puedan comprometer los datos personales, mantener un inventario actualizado de los sistemas y procesos que gestionan los datos personales, evaluar los riesgos inherentes a la recolección, almacenamiento y procesamiento de los datos personales.

Proteger: implementar medidas de protección de datos tales como la encriptación y control de acceso para los datos personales, aplicar controles de seguridad física y lógica a los sistemas que gestionan los datos personales, asegurar que el acceso a los datos personales esté limitado solo al personal autorizado, según las necesidades de su función.

Detectar: monitorear en tiempo real los sistemas que gestionan datos personales para identificar comportamientos sospechosos o accesos no autorizados, implementar herramientas de

detección de intrusiones que alerten sobre intentos de acceso no autorizado o manipulación de datos personales.

Responder: en caso de una violación de datos personales, aislar rápidamente los sistemas afectados para evitar una mayor exposición, notificar al Oficial de Protección de Datos (DPO) y al CSIRT para iniciar el proceso de respuesta. iniciar un análisis forense para identificar la causa del incidente, el alcance de la violación y los individuos afectados, notificación de Incidentes: BN Fondos notificará a las autoridades regulatorias y a los titulares de los datos si la violación compromete datos personales sensibles, de acuerdo con las leyes vigentes.

Recuperar: implementar acciones correctivas para asegurar que los datos comprometidos no vuelvan a ser vulnerables, restaurar los sistemas afectados utilizando copias de seguridad seguras, asegurando que los datos personales sean completamente restaurados, actualizar las políticas y procedimientos de protección de datos basados en las lecciones aprendidas.

Procedimientos Específicos para Incidentes que Comprometan Datos Personales

Detección y Notificación Inmediata: cualquier violación de datos personales será reportada inmediatamente al DPO y al CSIRT. El DPO determinará si el incidente requiere notificación a las autoridades regulatorias y a los individuos afectados, siguiendo los plazos establecidos por la ley.

Investigación y Análisis: se realizará un análisis exhaustivo del incidente para identificar la causa raíz, los sistemas comprometidos y el tipo de datos expuestos. El análisis incluirá un mapeo de los datos comprometidos y un informe detallado que será presentado a la gerencia.

Notificación a las Partes Afectadas: si los datos personales de los clientes o empleados han sido comprometidos, se notificará a los titulares afectados explicando el tipo de datos expuestos, los riesgos potenciales y las medidas que se deben tomar, BN FONDOS

proporcionará asistencia para mitigar los efectos del incidente, como ofrecer servicios de monitoreo de identidad si es necesario.

Medidas Correctivas: implementar medidas de seguridad adicionales para prevenir futuros incidentes similares, tales como la revisión de los controles de acceso o la actualización de software, reforzar la capacitación del personal en buenas prácticas de protección de datos personales.

Cumplimiento Legal

Esta política está alineada con la legislación local e internacional aplicable sobre protección de datos personales, incluyendo las normativas de privacidad y confidencialidad relevantes para BN FONDOS. Cualquier incidente que comprometa la seguridad de los datos personales será gestionado de acuerdo con las normativas vigentes.

Capacitación y Sensibilización

Todo el personal de BN Fondos que gestione o acceda a datos personales recibirá capacitación continua sobre las mejores prácticas para la protección de datos y la gestión de incidentes. Además, se realizarán simulacros para probar la efectividad de los procedimientos de respuesta a incidentes que involucren datos personales.

Revisión y Actualización

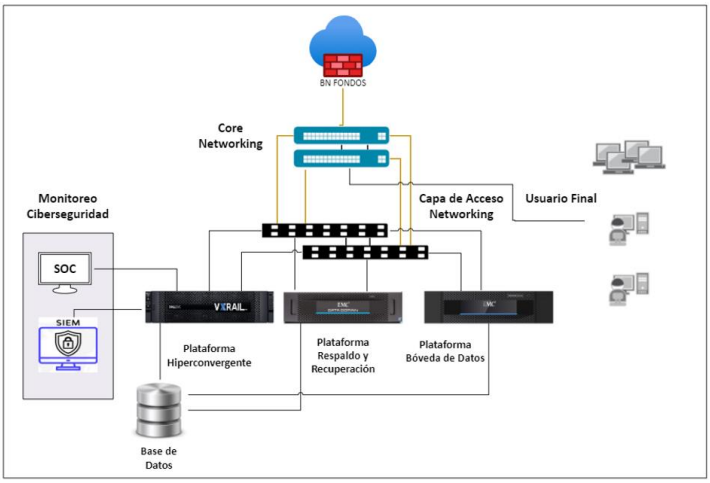
Esta política será revisada y actualizada anualmente o después de cualquier incidente significativo que involucre datos personales para asegurar que siga siendo efectiva y adecuada al entorno regulatorio y operativo de BN Fondos.

Propuesta de Monitoreo y Detección Temprana de Amenazas para BN FONDOS

La implementación de una gestión de eventos e información de seguridad (SIEM) aportó a BN FONDOS una serie de beneficios que lo ubican a la vanguardia para la prevención y mitigación de posibles incidentes en ciberseguridad. La oportuna detección y atención de alertas en tiempo real hacen que la infraestructura tecnológica se mantenga en operación y sin afectaciones garantizando la continuidad del negocio, mantiene el servicio al cliente final y su reputación no se ve afectada.

Figura 83

Propuesta Diseño Monitoreo Ciberseguridad



Nota. Propuesta SOC y SIEM en BN FONDOS, elaboración propia. 2024

Objetivo de la Propuesta

El objetivo de este sistema de monitoreo es detectar, analizar y responder las amenazas de seguridad en tiempo real, minimizando el impacto en las operaciones y protegiendo la integridad de los activos digitales de BN FONDOS. La propuesta se alinea con las mejores prácticas de

ciberseguridad, especialmente aquellas del marco NIST CSF, y se adapta a las necesidades específicas del sector financiero.

Componentes del sistema de monitoreo y detección

La implementación de un sistema de información y gestión de eventos de seguridad (SIEM) conlleva las siguientes ventajas:

- Centralización de logs: recopilación de logs y eventos de seguridad de todas las aplicaciones, sistemas operativos, dispositivos de red y bases de datos críticos en una única plataforma SIEM.
- Análisis en tiempo real: procesamiento y análisis de eventos en tiempo real para identificar patrones de comportamiento inusuales y posibles amenazas.
- Correlación de eventos: uso de correlación avanzada para detectar incidentes complejos que podrían no ser evidentes en un solo sistema, tales como intentos de acceso no autorizado o actividades anómalas en cuentas privilegiadas.

Un sistema de monitoreo SIEM posee una integración de inteligencia de amenazas (Threat Intelligence) lo que le puede permitir realizar:

- Suscripción a servicios de inteligencia de amenazas: incorporar servicios de inteligencia que proporcionen información actualizada sobre nuevas vulnerabilidades, malware y vectores de ataque específicos del sector financiero.
- Correlación con eventos locales: vinculación de la inteligencia de amenazas con los eventos detectados por el SIEM para evaluar la relevancia y el riesgo de cada amenaza en el contexto específico de BN FONDOS.

Otros sistemas que se complementan al SIEM son por la detección de intrusos (IDS) y un sistema de prevención de intrusos (IPS) logrando efectuar:

- Detección de firmas de ataques conocidos: configuración de un IDS para monitorear el tráfico de red en busca de patrones de ataques conocidos (por ejemplo, inyecciones SQL, ataques DDOS, etc.).
- Prevención activa de ataques: implementación de un IPS que pueda bloquear o contener automáticamente ataques identificados de acuerdo con políticas de seguridad predefinidas.

El monitoreo de comportamiento de usuarios y entidades facilita el:

- Análisis basado en anomalías: implementación de herramientas que pueda analizar los comportamientos de usuarios y entidades en la red, esto permite detectar actividades atípicas que podrían indicar accesos no autorizados o amenazas internas.
- Alertas basadas en riesgo: generación de alertas priorizadas según el nivel de riesgo, evaluando tanto la criticidad del activo como el contexto de la actividad detectada.

La automatización de respuestas ante amenazas (SOAR) permite:

- Orquestación de respuestas: uso de plataformas SOAR (Security Orchestration, Automation, and Response) para automatizar flujos de trabajo en respuesta a amenazas comunes, como ataques de phishing o intentos de acceso fallidos.
- Playbooks de respuesta: desarrollo de playbooks específicos para distintos tipos de incidentes, permitiendo respuestas rápidas y coordinadas que incluyan la contención, mitigación y, si es necesario, escalamiento de los incidentes.

Pruebas y simulaciones de incidentes

Como objetivos para las pruebas y simulaciones de incidentes se establece:

- Simulación de ataques: realizar simulaciones de ataques cibernéticos de manera periódica para probar la efectividad del sistema de monitoreo y la capacidad de respuesta.
- Evaluación de tiempos de respuesta: medición de los tiempos de detección y respuesta para asegurar que el sistema cumple con los niveles de servicio definidos (SLA) y realizar ajustes según sea necesario.

Proceso de implementación

La implementación de esta propuesta se dividirá en varias fases:

- Fase 1evaluación y selección de herramientas: identificación de herramientas SIEM, IDS/IPS, SOAR que mejor se adapten a las necesidades de BN FONDOS.
- Fase 2 integración y configuración: configuración de herramientas y establecimiento de conexiones con activos críticos para el monitoreo de eventos.
- Fase 3 capacitación y desarrollo de playbooks: capacitación al personal en el uso de herramientas y en la ejecución de playbooks de respuesta ante amenazas.
- Fase 4 pruebas y optimización continua: realización de pruebas iniciales y optimización basada en la retroalimentación de simulaciones y datos en tiempo real.

Métricas de desempeño

El éxito del sistema de monitoreo y detección temprana de amenazas se medirá mediante las siguientes métricas:

- Tiempo de detección (MTTD): promedio de tiempo desde el inicio de un evento hasta su detección.
- Tiempo de respuesta (MTTR): tiempo promedio para contener y mitigar un incidente.
- Número de falsos positivos: evaluación de la precisión de las alertas generadas por el sistema.
- Cumplimiento de SLA: verificación de que los tiempos de respuesta y mitigación cumplen con los niveles de servicio acordados.

Propuesta de Modelo de Ciberresiliencia para BN FONDOS

El objetivo del modelo de ciberresiliencia el modelo tiene como fin establecer un enfoque integral que permita a BN FONDOS resistir, responder y recuperarse ante incidentes de ciberseguridad, minimizando el impacto en sus operaciones y en la seguridad de sus activos digitales. esto se alinea con los principios del marco NIST CSF 2.0 y busca una mejora continua que adapte la organización a las amenazas emergentes.

Componentes del modelo de ciberresiliencia:

La identificación de activos críticos y evaluación de riesgos involucra:

- Realizar un inventario detallado de activos críticos (infraestructura, datos sensibles, aplicaciones) que soportan las operaciones de BN FONDOS.

- Implementar una evaluación continua de riesgos para identificar y priorizar las vulnerabilidades que podrían afectar la seguridad y la continuidad del negocio.

Con respecto a las políticas y procedimientos de gestión de incidentes se debe:

- Establecer políticas de gestión de incidentes y respuestas estándar para diferentes tipos de eventos, que incluyan acciones preventivas y correctivas.
- Definir roles y responsabilidades específicas para el equipo de ciberseguridad y otras áreas relevantes, asegurando claridad en la cadena de comunicación.

La automatización y monitoreo continuo brindará:

- Implementar herramientas de monitoreo continuo para la detección temprana de amenazas en tiempo real.
- Automatizar respuestas a incidentes de bajo riesgo (por ejemplo, ataques de fuerza bruta) para optimizar los tiempos de respuesta y reducir la carga en el equipo de ciberseguridad.
- Integrar herramientas de análisis de inteligencia de amenazas que provean información sobre posibles ataques específicos al sector financiero.

La capacitación y simulaciones de incidentes ayudará a:

- Desarrollar programas de capacitación periódica en ciberseguridad para el personal de BN FONDOS, asegurando que todos comprendan los procedimientos de respuesta.
- Realizar simulaciones de incidentes de ciberseguridad (ejemplo: ejercicios de ransomware o ataques de phishing) para evaluar la capacidad de respuesta y mejorar los tiempos de reacción.

La continuidad del negocio y recuperación ante desastres permitirá:

- Establecer un plan de continuidad del negocio (BCP) y un plan de recuperación ante desastres (DRP) específicos para incidentes cibernéticos, asegurando la rápida restauración de operaciones críticas.
- Definir objetivos de recuperación (RPO) y tiempos de recuperación (RTO) para cada sistema crítico, adaptados a los requerimientos de BN FONDOS.

Revisión y mejora continua

- Realizar auditorías periódicas y análisis post-incidente para identificar lecciones aprendidas y oportunidades de mejora en los procedimientos y tecnologías utilizadas.
- Monitorear los cambios en el panorama de amenazas y adaptar las estrategias del modelo de ciberresiliencia para responder a nuevas amenazas o vulnerabilidades emergentes.

Implementación y métricas de éxito

Con el fin de asegurar el éxito del modelo, se propone un plan de implementación en fases, que inicie con los activos críticos y se expanda gradualmente al resto de la infraestructura. las métricas de éxito incluyen:

- Tiempo de respuesta a incidentes: medición de la velocidad de detección, contención y resolución de incidentes.
- Cumplimiento del RPO y RTO: verificación de los tiempos de recuperación establecidos en el DRP para cada sistema.

- tasa de detección temprana: evaluación de la efectividad de las herramientas de monitoreo para identificar amenazas potenciales.
- niveles de conocimiento del personal: evaluación del personal en simulaciones y pruebas de conocimiento en ciberseguridad.

Referencias Bibliográficas

ABA. (2024). *American Banjers Association*. Obtenido de https://www.aba.com/

Aguilar, J. M. (2021). *Reto y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenzas a la seguridad nacioanl y política exterior.* Obtenido de https://www.scielo.cl/pdf/rei/v53n198/0719-3769-rei-53-198-00169.pdf

Alonso, C. (27 de septiembre de 2023). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. Obtenido de GlobalSuite Solutions: https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/

Araujo, A. (10 de junio de 2021). *Hackmetrix*. Obtenido de 6 pasos para armar un plan de continuidad del negocio (BCP) para tu startup: https://blog.hackmetrix.com/plan-de-continuidad-del-negocio-6-pasos/

Ariosto, M. (25 de agosto de 2021). *¿Qué es el análisis de factibilidad?* Obtenido de https://testamarketing.com/blog/articulos/que-es-el-analisis-de-factibilidad

Arroyo Guardeño, D. (2020). *Ciberseguridad.* CSIC. Obtenido de https://elibro.net/es/lc/ucentral/titulos/172144

ATLAS.ti. (s.f.). *Guía fundamental de la investigación cualitativa - Parte 1: Conceptos básicos*. Obtenido de Team ATLAS.ti: https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/consideraciones-eticas

Attacks, F. (25 de junio de 2024). *La dura labor de la banca de cumplir estándares*. Obtenido de https://fluidattacks.com/es/blog/regulaciones-ciberseguridad-bancaria/

AWS. (2023). *¿Qué es la ciberseguridad?* Obtenido de https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20pr%C3%A1ctica,cliente%20y%20cumplir%20la%20normativa.

Bittencourt, D. (5 de enero de 2024). *Diferencias entre COBIT, ISO 27001 y NIST*. Obtenido de https://diegobittencourt-org.translate.goog/en/2024/01/05/differences-between-cobit-iso-27001-and-nist/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

BNCR. (s.f.). *Banco Nacional de Costa Rica*. Obtenido de https://www.bncr.fi.cr/

BNFONDOS. (s.f.). *Página WEB BN FONDOS*. Obtenido de https://www.bnfondos.com/

Canals Ametller, D. (2021). *Ciberseguridad: un nuevo reto para el Estado y los gobiernos locales.* Obtenido de https://elibro.net/es/lc/ucentral/titulos/181960

Cano, J. (2022). *El ransomware: una estrategia de desestabilización geopolítica. El Caso de Costa Rica*. (Global Strategy Report) Recuperado el 19 de junio de 2024, de https://global-strategy.org/el-ransomware-una-estrategia-de-desestabilizacion-geopolitica-el-caso-de-costa-rica/

Carrasco, L. d. (03 de abril de 2015). *Dialnet.* Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=7685521

Ciberseguridad, C. (28 de febrero de 2024). *La importancia del uso de Blockchain en Ciberseguridad*. Obtenido de https://www.campusciberseguridad.com/blog/item/161-la-importancia-del-uso-de-blockchain-en-ciberseguridad

Consulting, C. (10 de febrero de 2023). *Benchmarking: ¿qué es y cómo hacer este análisis en tu empresa?* Obtenido de https://www.csrconsulting.com.mx/2023/02/10/benchmarking-que-es-y-como-hacer-este-analisis-en-tu-empresa/

Datacom.Global. (s.f.). *Cisco SecureX: introducción a la solución*. Obtenido de https://datacom.global/cisco-securex-introduccion-a-la-solucion/

Dominguez, M. (25 de abril de 2023). *Aplicaciones y beneficios de Big Data en Ciberseguridad*. Obtenido de https://cybersecuritynews.es/aplicaciones-y-beneficios-de-big-data-en-ciberseguridad/

ENISA. (2005-2024). *Centros de análisis e intercambio de información (ISAC)*. Obtenido de https://www-enisa-europa-eu.translate.goog/topics/national-cyber-security-strategies/information-sharing?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

Espinoza Reyes, J. (Febrero de 2024). *Fortaleciendo la ciberseguridad en Costa Rica.* Recuperado el 19 de junio de 2024, de https://repositorio.ucenfotec.ac.cr/bitstream/handle/123456789/497/PIA02-Espinoza%20Reyes%20Jos%c3%a9%20Manuel%20y%20Vargas%20Villalobos%20Roberto_MSEG_mar2024.pdf?sequence=1&isAllowed=y

ETEK. (20 de mayo de 2024). *La importancia de la formación continua en ciberseguridad*. Obtenido de Linkedin: https://www.linkedin.com/pulse/la-importancia-de-formaci%C3%B3n-continua-en-ciberseguridad-kbj7e/

FFIEC. (30 de junio de 2021). *Manual de examen de tecnología de la información de la FFIEC: nueva arquitectura, infraestructura y folleto de operaciones*. Obtenido de Boletín OCC 2021-30: https://www-occ-gov.translate.goog/news-issuances/bulletins/2021/bulletin-2021-30.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

Finance, F. (09 de abril de 2024). *La ciberseguridad en el sistema financiero*. Obtenido de https://www.fedfinance.es/noticias-y-consejos/la-ciberseguridad-en-el-sistema-financiero

García, E. (2 de mayo de 2024). *Fortaleciendo la Ciberseguridad: El Papel Fundamental del Análisis Predictivo*. Obtenido de Linkedin: https://www.linkedin.com/pulse/fortaleciendo-la-ciberseguridad-el-papel-fundamental-del-garcia-tj07e/

Gartner. (2024). *¿Qué es el Magic Quadrant de Gartner?* Obtenido de https://www.gartner.es/es/metodologias/magic-quadrant

Gartner. (2024). *Tendencias en ciberseguridad: optimización para mejorar la resiliencia y el rendimiento*. Obtenido de https://www.gartner.es/es/tecnologia-de-la-informacion/temas/tendencias-ciberseguridad

GeekFlare. (13 de septiembre de 2024). *Las 11 mejores herramientas SIEM para proteger a su organización de los ciberataques*. Obtenido de https://geekflare.com/es/best-siem-tools/

Gómez, J. A. (23 de abril de 2024). *¿Qué es la respuesta a incidentes?* Obtenido de Delta Protect: https://www.deltaprotect.com/blog/plan-respuesta-incidentes

Grupo, S. (01 de agosto de 2023). *¿Qué es la ciberresiliencia y por qué es importante para las empresas?* Obtenido de https://s2grupo.es/que-es-la-ciberresiliencia-y-por-que-es-importante-para-las-empresas/

Grupo, S. (28 de noviembre de 2023). *Continuidad del negocio: qué es y por qué es importante*. Obtenido de https://s2grupo.es/continuidad-del-negocio-que-es-y-por-que-es-importante/

Huerta, J. C. (23 de noviembre de 2023). *Los desafíos de la transformación digital y cómo superarlos*. Obtenido de Linkedin: https://www.linkedin.com/pulse/los-desaf%C3%ADos-de-la-transformaci%C3%B3n-digital-y-c%C3%B3mo-castro-huerta-0lzhe/

IBM. (20 de octubre de 2023). *¿Qué es el marco de ciberseguridad del NIST?* Obtenido de https://www-ibm-com.translate.goog/topics/nist?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

IBM. (27 de octubre de 2023). *¿Qué es el marco regulatorio de ciberseguridad del NIST?* Obtenido de https://www.ibm.com/es-es/topics/nist

IBM. (27 de octubre de 2023). *¿Qué es la ciberseguridad?* Obtenido de https://www.ibm.com/es-es/topics/cybersecurity

IBM. (20 de octubre de 2023). *¿Qué es la resiliencia cibernética?* Obtenido de https://www.ibm.com/es-es/topics/cyber-resilience

IBM. (20 de octubre de 2023). *¿Qué es una infraestructura de TI?* Obtenido de https://www.ibm.com/es-es/topics/infrastructure

IBM. (20 de octubre de 2023). *¿Qué son las pruebas de penetración?* Obtenido de https://www.ibm.com/mx-es/topics/penetration-testing

IBM. (s.f.). *IBM QRadar SIEM*. Obtenido de https://www.ibm.com/es-es/products/qradar-siem

IEBS. (5 de julio de 2024). *Qué es Blockchain y como funciona la tecnología Blockchain*. Obtenido de https://www.iebschool.com/blog/blockchain-cadena-bloques-revoluciona-sector-financiero-finanzas/

INA. (s.f.). *Fórmula para calcular la muestra.*

INCIBE. (s.f.). *Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es/incibe/informacion-corporativa/que-es-incibe

Kaspersky. (s.f.). *¿Qué es la seguridad en la nube?* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-cloud-

security?srsltid=AfmBOoql8HqAFEOh5e0VeUp5pL_zCfnct_VZFsy7UwLI2fmh8vS_Ftzz

KPMG. (2024). *¿Qué constituye un recorrido exitoso por el BCBS 239 para las organizaciones?* Obtenido de https://kpmg-com.translate.goog/be/en/home/insights/2021/11/rc-what-constitutes-a-successful-bcbs-239-journey-for-organizations.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

Labrador, L. A. (1 de octubre de 2023). *Resumen de los cuadrantes mágico de Gartner del SIEM correspondiente del año 2010 hasta el 2024*. Obtenido de https://www.linkedin.com/pulse/resumen-de-los-cuadrantes-m%C3%A1gico-gartner-del-siem-a%C3%B1o-zafra-labrador/

Licencias_OnLine. (s.f.). *FireEye Helix, Recupere el control de sus operaciones de seguridad*. Obtenido de https://www.licenciasonline.com/pe/es/productos/fire-eye/helix

Limones, E. (03 de abril de 2023). *Qué es una vulnerabilidad informática*. Obtenido de OpenWebinars: https://openwebinars.net/blog/analisis-de-vulnerabilidades-informaticas/

Lozano, P. A. (19 de julio de 2024). *Cómo desarrollar una cultura de ciberseguridad en la empresa*. Obtenido de OpenWebinars: https://openwebinars.net/blog/como-desarrollar-cultura-ciberseguridad-empresa/

Mendoza, M. Á. (4 de agosto de 2015). *COBIT para la seguridad en las organizaciones*. Obtenido de https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

México, B. d. (s.f.). *Ciberseguridad Banco de México*. Obtenido de Estrategia de ciberseguridad del Banco de México: https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html

MICITT. (s.f.). *Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones*. Obtenido de https://www.micitt.go.cr/micitt/funciones-micitt

Micrsoft. (s.f.). *Microsfot Sentinel*. Obtenido de https://www.microsoft.com/es-es/security/business/siem-and-xdr/microsoft-sentinel#tabx2569aa1c3ad24c3cb5e92fb60e0d5c4b

Ministerio de Ciencia, I. T. (2023). *Estrategia Nacional de Ciberseguridad de Costa Rica.* Obtenido de https://www.crhoy.com/wp-content/uploads/2023/10/NCS-Costa-Rica-10Oct2023-estrategia-nacional-ciberseguridad.pdf

Moreno García, M. (2022). *Gestión de incidentes de ciberseguridad* (1 ed.). RA-MA Editorial. Obtenido de https://elibro.net/es/lc/ucentral/titulos/222669

Nachas. (s.f.). *Normas de funcionamiento de Nacha - Nuevas normas*. Obtenido de https://www-nacha-org.translate.goog/newrules?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

NIST. (28 de enero de 2021). *Protección de información no clasificada controlada en sistemas y organizaciones no federales*. Obtenido de https://csrc-nist-gov.translate.goog/pubs/sp/800/171/r3/final?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

NIST. (s.f.). *Computer Security Resource Center*. Obtenido de https://csrc.nist.gov/publications/sp800

Nutanix. (8 de mayo de 2024). *Disaster Recovery Plan DRP: Definición y usos*. Obtenido de https://www.nutanix.com/es/info/disaster-recovery

OEA-AWS. (28 de agosto de 2019). *Marco NIST Ciberseguridad.* Obtenido de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Open_Risk_Manual. (26 de marzo de 2021). *BCBS 147*. Obtenido de https://www.openriskmanual.org/wiki/BCBS_147

Paloalto. (4 de mayo de 2020). *Cortex XSOAR*. Obtenido de https://www.paloaltonetworks.lat/resources/datasheets/cortex-xsoar-overview

Rapid7. (s.f.). *InsightIDR, Next-gen SIEM for the cloud-first era*. Obtenido de https://www.rapid7.com/products/insightidr/

Raya, J. (21 de setiembre de 2023). *Los ciberataques en el mundo financiero: amenazas y desafíos*. Obtenido de https://eiposgrados.com/blog-direccion-financiera/ciberataques-mundo-financiero-amenazas-desafios/

Rica, U. C. (20 de octubre de 2022). *Gestión de incidentes de seguridad*. Obtenido de https://ci.ucr.ac.cr/gestion-incidentes-seguridad

Riesgos, A. -A. (2019). *Mapa de Ciberriesgos.* Obtenido de Grupo de trabajo de ciberriesgos de AGERS e ISMS Forum: https://www.ismsforum.es/ficheros/descargas/mapaciberriesgosagersisms2019157303683 6.pdf

Rosencrance, L. (24 de junio de 2024). *Las 15 mejores certificaciones en ciberseguridad para 2024*. Obtenido de Techopedia: https://www.techopedia.com/es/mejores-certificaciones-ciberseguridad

Sampieri, R. H. (2014). *Metodología de la Investigación* (Sexta ed.). México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

Sampieri, R. H. (2018). *Metodología de la Investigación: Las Rutas Cuantitativa, Cualitativa y Mixta.* McGRAW-HILL INTERAMERICANA EDITORES, S.A. de C. V.

Schirn, A. (1 de marzo de 2023). *ISO/IEC 27035-1:2023—Gestión de seguridad de la información*. Obtenido de ANSI: https://blog-ansi-org.translate.goog/iso-iec-27035-1-2023-information-security-management/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

ServiceNow. (2024). *Security Operations (SecOps)*. Obtenido de https://www.servicenow.com/latam/products/security-operations.html

Solís, D. C. (9 de junio de 2023). *Uso de Inteligencia Artificial y Machine Learning en ciberseguridad*. Obtenido de OpenWebinars: https://openwebinars.net/blog/uso-de-inteligencia-artificial-y-machine-learning-en-ciberseguridad/

Solutions, G. (22 de setiembre de 2023). *¿Qué es la norma ISO 27001 y para qué sirve?* Obtenido de GlobalSuite Solutions: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/#:~:text=La%20norma%20ISO%2027001%20es,y%20disponibilidad%20de%20la%20informaci%C3%B3n.

Splunk. (2005-2024). *Hacemos que las organizaciones sean más resilientes*. Obtenido de https://www-splunk-com.translate.goog/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es-419&_x_tr_pto=sc

Tejada, E. C. (2015). *Gestión de incidentes de seguridad informática (MF0488_3).* IC Editorial. Obtenido de https://elibro.net/es/lc/ucentral/titulos/44101

Trellix-McAfee. (s.f.). *Ficha Técnica: McAfee MVISION Endpoint*. Obtenido de https://partners.trellix.com/enterprise/es-mx/assets/data-sheets/ds-mvision-endpoint.pdf

UNIR. (30 de junio de 2020). *Certificación CISA: ¿qué es y como se obtiene?* Obtenido de https://www.unir.net/revista/ingenieria/certificacion-cisa/

Vargas, S. (26 de agosto de 2023). *¡La importancia del monitoreo de ciberseguridad 24x7!* Obtenido de Linkdin: https://www.linkedin.com/pulse/la-importancia-del-monitoreo-de-ciberseguridad-24x7-vargas/

Zendesk. (11 de septiembre de 2024). *Qué es el retorno de inversión (ROI)*. Obtenido de https://www.zendesk.com.mx/blog/que-es-el-roi/

Apéndices

Anexos

Anexo 1. Preguntas de Encuesta

La encuesta aplicada al personal de BN FONDOS se realizó con el objetivo de valorar el conocimiento que pueda tener el personal en aspectos de ciberseguridad, lo cual permitió determinar y establecer acciones de mejora para la prevención de incidentes de ciberseguridad, cumpliendo a cabalidad para la solución del diseño de la propuesta de esta investigación.

1. ¿Qué tan consciente estás de las amenazas cibernéticas que pueden afectar a BN FONDOS?
    1. Nada Consciente
    2. Poco Consciente
    3. Moderadamente consciente
    4. Consciente
    5. Muy Consciente
2. En tu opinión, ¿cuál es la mayor amenaza cibernética que puede enfrentar BN FONDOS?
    1. Correos sospechosos (Phishing & Malware)
    2. Denegación de servicios en IB
    3. Fraude bancario digital
    4. Amenazas internas
3. ¿Has recibido inducción y/o capacitación (ejemplo KnowBe4) en ciberseguridad durante el último año?
    1. Sí
    2. No

4. En caso afirmativo, ¿consideras que dicha capacitación fue suficiente para prepararte frente a posibles ciberataques?
    1. Nada útil
    2. Poco útil
    3. Moderadamente útil
    4. Útil
    5. Muy útil
5. ¿Cómo percibe usted la seguridad de la infraestructura tecnológica (software, redes, hardware) de BN FONDOS?
    1. Muy débiles
    2. Débiles
    3. Moderadamente sólidos
    4. Sólidos
    5. Muy sólidos
6. ¿Consideras que la infraestructura tecnológica actual de BN Fondos es suficiente para garantizar la continuidad del negocio en caso de un ataque cibernético?
    1. Sí
    2. No
7. ¿Qué actividades considera usted puede desarrollar el personal de BN FONDOS en las etapas de prevención de eventos de ciberseguridad?
    1. Adquirir conocimientos de ciberseguridad mediante las actividades de inducción, capacitación y refrescamientos.

2. Mantenerse alertas ante las amenazas cibernéticas como correos sospechosos, nuevos tipos de fraudes, navegación en internet, etc.
3. Reportar eventos sospechosos de ciberseguridad.
4. Atender las instrucciones del personal de TI para investigar, contener o erradicar los incidentes de ciberseguridad.
5. Todas las anteriores.

8. ¿Tienes claro el procedimiento a seguir en caso de un incidente de seguridad de la información en BN Fondos?
    1. Sí
    2. No
9. ¿Tienes conocimiento acerca de las Pruebas de Continuidad de Servicios Tecnológicos que se realizan en BN FONDOS?
    1. Sí
    2. No
10. ¿Sabes que es un evento de ciberseguridad? (correos y llamadas sospechosos, alertas de ransomware, phishing, etc.)?
    1. Sí
    2. No
11. En tu experiencia, ¿los eventos de seguridad en la información en BN FONDOS han sido resueltos de manera eficiente y con el menor impacto posible?
    1. Totalmente en desacuerdo
    2. En desacuerdo
    3. Ni de acuerdo ni en desacuerdo

4. De acuerdo
5. No tengo información al respecto.

12. ¿Consideras que BN FONDOS tiene implementadas las medidas preventivas necesarias para evitar ciberataques?
    1. Sí
    2. No
13. ¿Consideras que en BN FONDOS se ponen en prácticas medidas preventivas en ciberseguridad?
    1. Totalmente en desacuerdo
    2. En desacuerdo
    3. Ni de acuerdo ni en desacuerdo
    4. De acuerdo
    5. Totalmente de acuerdo
14. ¿Qué tan preparado crees que está el personal en general de BN FONDOS para detectar y reportar actividades sospechosas en los sistemas?
    1. Nada preparado
    2. Poco preparado
    3. Moderadamente preparado
    4. Preparado
    5. Muy preparado
15. ¿Tienes conocimientos si BN FONDOS existen planes para recuperarse rápidamente de un ciberataque?
    1. Sí

2. No

16. En caso de un ataque exitoso, ¿crees que la organización tiene un plan adecuado para garantizar la continuidad del negocio?
    1. Sí
    2. No
17. ¿Qué tan seguro te sientes con las medidas que se promueven en BN FONDOS para proteger la reputación de la organización en caso de un ciberataque?
    1. Nada seguro
    2. Poco seguro
    3. Moderadamente seguro
    4. Seguro
    5. Muy Seguro
18. ¿Consideras que BN FONDOS cuenta con los recursos financieros necesarios para implementar un modelo robusto de gestión de incidentes y ciber resiliencia?
    1. Totalmente en desacuerdo
    2. En desacuerdo
    3. Ni de acuerdo ni en desacuerdo
    4. De acuerdo
    5. Totalmente de acuerdo
19. ¿Crees que se debería aumentar la frecuencia de las capacitaciones en ciberseguridad para todo el personal de BN FONDOS?
    1. Sí
    2. No

20. ¿Cómo evaluarías la efectividad de las estrategias de prevención implementadas por BN FONDOS para evitar ciberataques?
    1. Muy inefectivas
    2. Inefectivas
    3. Moderadamente efectivas
    4. Efectivas
    5. Muy Efectivas
21. ¿Tienes conocimiento si existen procedimientos de recuperación en caso de un ciberataque en BN FONDOS?
    1. Sí
    2. No
22. ¿Conoce usted si BN FONDOS cuenta con canales de comunicación alternativos que aseguren una adecuada comunicación entre los responsables de atender un incidente de ciberseguridad?
    1. Sí
    2. No
23. ¿Cómo valorarías el nivel de colaboración entre BN FONDOS y el Banco Nacional para mejorar los servicios de ciberseguridad?
    1. Muy baja
    2. Baja
    3. Moderada
    4. Alta
    5. Muy alta

24. ¿Considera adecuada la periodicidad de revisión y actualización de los planes de gestión de incidentes en BN FONDOS para adaptarse a nuevas amenazas?
    1. Sí
    2. No
25. ¿Qué tan frecuentemente los sistemas de gestión de datos en BN FONDOS se ven afectados por incidentes de seguridad?
    1. Nunca
    2. Raramente
    3. Ocasionalmente
    4. Frecuentemente
    5. Muy frecuentemente
26. ¿Cómo evaluarías el impacto de los incidentes de ciberseguridad en los sistemas de procesamiento de transacciones financieras de BN FONDOS, en caso de que lleguen a materializarse?
    1. Muy baja
    2. Baja
    3. Moderada
    4. Alta
    5. Muy alta
27. ¿Qué tan efectivas son las medidas de seguridad actuales para proteger los sistemas de comunicaciones internas en BN FONDOS?
    1. Muy inefectivas
    2. Inefectivas

3. Moderadamente efectivas
4. Efectivas
5. Muy Efectivas

28. ¿Cómo valoras la capacidad de los sistemas de respaldo y recuperación en BN FONDOS para salvaguardar la información ante un ciberataque que ponga en riesgo a los datos críticos de la sociedad?
    1. Muy débiles
    2. Débiles
    3. Moderadamente sólidos
    4. Sólidos
    5. Muy sólidos
29. ¿Conoce si en BN FONDOS se realizan pruebas de vulnerabilidad en los sistemas más críticos de BN FONDOS para identificar posibles debilidades?
    1. Sí
    2. No
30. ¿Qué mejoras propondrías para mejorar el conocimiento teórico y práctico de ciberataques y ciberseguridad en BN FONDOS?

Anexo 2. Preguntas de Entrevista

Las entrevistas realizadas al personal clase en materia de ciberseguridad de BN FONDOS y del Banco Nacional de Costa Rica se realizó con el objetivo de valorar las proyecciones en las cuales se enfocan ambas instituciones para reforzar y optimizar las gestiones de protección ante incidentes de ciberseguridad, lo cual permitió determinar y establecer acciones de mejora para la prevención de incidentes de ciberseguridad, cumpliendo a cabalidad para la solución del diseño de la propuesta de esta investigación.

1. ¿Como considera hoy en día los ciberataques a nivel mundial?
2. ¿A nivel nacional considera que Costa Rica ha mejorado los procedimientos y planes de continencia contra ciberataques?
3. ¿Qué opina del marco NIST?
4. ¿Considera que se han mejorado en las instituciones públicas las gestiones de respuesta a incidentes y amenazas en ciberseguridad?
5. ¿Qué fuentes referencia emplea el Conglomerado Financiero del Banco Nacional para estar al día con las nuevas técnicas de los ciberdelincuentes?
6. ¿A nivel del CFBCR considera en forma general que se han acatado las mejoras prácticas para evitar en la medida de lo posible ciberataques?
7. ¿Cómo considera el conocimiento en general de los funcionarios del Conglomerado Financiero del Banco Nacional acerca de la ciberseguridad, las consecuencias de los ataques y el impacto que puede traer esto al core de negocio bancario?