TRABAJO DE GRADO
Opción Seminario-Diplomado.

Gestión de Ciberseguridad en Entornos Organizacionales Modernos

Corporación Universitaria Remington.
Faculta de Ingeniería
Programa de Ingeniería de Sistemas

Lorena Gamboa Cardozo

Karol Ximena Vargas Cardenas

Jorge Mauricio Sepúlveda Castaño

Opción de Trabajo de grado Seminario.

2025

Agradecimientos

Con satisfacción y gratitud culminamos este proceso académico, el cual representó un desafío significativo y, al mismo tiempo, una oportunidad de crecimiento personal y profesional. Agradecemos profundamente a la Corporación Universitaria Remington**,** institución que nos acompañó en nuestra formación, brindándonos herramientas conceptuales, orientación constante y un entorno educativo propicio para el desarrollo de competencias tecnológicas y analíticas.

Extendemos un reconocimiento especial a los docentes e ingenieros que hicieron parte de este proceso formativo. Su dedicación, experiencia y acompañamiento fueron fundamentales para fortalecer nuestra comprensión sobre la ingeniería, la gestión tecnológica y la ciberseguridad.

Finalmente, manifestamos nuestra gratitud a nuestras familias, quienes con su apoyo, motivación y confianza nos impulsaron a avanzar incluso en los momentos más exigentes. Gracias a ellos logramos alcanzar esta meta académica que marca el inicio de nuevas oportunidades.

Tabla de Contenidos

1. Introducción

La transformación digital ha impulsado a las organizaciones a la adopción de nuevas tecnologías orientadas a la optimización de procesos, el incremento de la productividad y el apoyo en la toma de decisiones basadas en datos. Al mismo tiempo, el avance de la tecnología también ha generado consigo una mayor complejidad de las amenazas cibernéticas. En este sentido, la ciberseguridad se ha convertido en un elemento estratégico que garantiza la protección de la información, la continuidad operativa y la confianza de los clientes, usuarios y socios. Este documento técnico, del cual se deriva este resumen, se está desarrollando de acuerdo con directrices internacionales, utilizando estándares, marcos de referencia y mejores prácticas que son ampliamente aceptados en el dominio de la Tecnología de la información.

Además, incorpora el conocimiento adquirido del seminario Transformación Digital y Outsourcing Inteligente, el cual se centró en los Desafíos Contemporáneos y las Soluciones Emergentes en la Gestión de Seguridad y Tecnología, a lo largo del documento encontramos el marco teórico que proporciona los conceptos fundamentales de la ciberseguridad y transformación digital. Posteriormente, se presenta un enfoque estructurado orientado a la identificación de riesgos con el objetivo de ayudar a las organizaciones a identificar las amenazas que pueden afectar sus recursos tecnológicos, sus datos y su operación en su conjunto.

Este análisis se completa con el diseño de un modelo integral de gestión de ciberseguridad.

1.1. Palabras clave

Ciberseguridad; Gestión de riesgos; Seguridad de la información; ISO 27001; Amenazas cibernéticas.

2. Marco conceptual y contextual

El marco conceptual proporciona los fundamentos teóricos que permiten comprender el papel de la ciberseguridad dentro de las organizaciones modernas. A medida que los procesos se digitalizan, los sistemas de información se convierten en activos esenciales cuya exposición aumenta ante amenazas internas y externas.

La ciberseguridad es un conjunto de políticas, prácticas y controles enfocados en proteger los sistemas, redes y datos contra accesos no autorizados, fallas operativas o actividades maliciosas. Esta disciplina integra herramientas técnicas, modelos de gestión, normativas internacionales y acciones humanas orientadas a garantizar la disponibilidad, integridad, confidencialidad y trazabilidad de la información.

3. Ciberseguridad

La ciberseguridad es un elemento esencial en las organizaciones modernas, ya que permite proteger los sistemas de información y los activos digitales frente a amenazas que pueden afectar la operación de los datos.

Su objetivo principal es garantizar la continuidad operativa mediante la gestión y reducción de los riesgos tecnológicos que comprometen la confidencialidad, integridad y disponibilidad de la información. Para ello, integra controles técnicos, medidas organizacionales y practicas orientadas al fortalecimiento de la cultura de seguridad.

La ciberseguridad debe entenderse como un proceso continuo, alineado con estándares y marcos de referencia, que exige evaluación permanente de riesgos y mejora constante de los controles implementados

3.1. Estos son los principios fundamentales de la ciberseguridad:

- Confidencialidad: Garantiza la privacidad de la información, accesible solo para usuarios, sistemas o entidades autorizados. Esto se logra mediante la implementación de controles de acceso, mecanismos de autenticación y técnicas de cifrado de la información.
- Integridad: Mantiene los datos precisos, completos e intactos, el hash, el control de versiones y los registros de auditoría ayudan en este aspecto.
- Disponibilidad: Garantiza que los usuarios autorizados puedan acceder a los sistemas y datos cuando lo necesiten. La redundancia, los planes de continuidad y la tolerancia a fallos son clave.
- Trazabilidad: Este principio, aunque frecuentemente subestimado, resulta fundamental para la detección de incidentes y la asignación de responsabilidades, se trata de rastrear y auditar las acciones para detectar incidentes y asignar responsabilidades. En las organizaciones, la ciberseguridad abarca la prevención, la detención y la respuesta.

Incluye seguridad de red, seguridad de aplicaciones, protección de puntos finales, seguridad en la nube, gestión de identidades y respuestas a incidentes.

3.2. Gestión de Riesgos

La gestión de riesgos de ciberseguridad es una forma estructural de detectar, analizar y reducir amenazas que podrían interrumpir las operaciones comerciales. Ayuda a priorizar esfuerzos, asignar recursos sabiamente y configurar protecciones basadas en riesgos reales.

El proceso de gestión de riesgos de ciberseguridad se desarrolla, de manera general, a través de las siguientes etapas:

- Identificar activos críticos: Identificar los datos, sistemas o procesos son decisivos para su organización.
- Encontrar vulnerabilidades: Buscar puntos débiles técnicos, de procedimiento o humanos que podrían explotarse.
- Evaluar amenazas: Considerar actores maliciosos, fallas internas, accidentes o desastres.
- Estimar el riesgo: Medir la probabilidad y el impacto utilizando métodos cualitativos, cuantitativos o híbridos.
- Tratar el riesgo: Decidir si mitigarlo, transferirlo, aceptarlo o evitarlo.
- Monitorear y mejorar: Garantizar la actualización permanente de los controles de seguridad conforme evolucionan las amenazas y el entorno tecnológico.

Las herramientas y métodos comunes incluyen:

- ISO/IEC 27005: Directrices para la gestión de riesgos en sistemas de información, parte del marco ISO/IEC 27001.
- NIST SP 800-30. Un análisis de riesgos estructurado, ideal para organizaciones con madurez técnica.

- Matrices de riesgo: Herramientas visuales que mapean la gravedad del riesgo según la probabilidad y el impacto.
- Evaluaciones de riesgos de amenazas y vulnerabilidades (TVRA): Se utilizan en infraestructura critica.

Este proceso garantiza que sus controles se ajusten al nivel de exposición de su organización.

3.3. Estándares y Marcos de Referencia

Las organizaciones recurren a estándares y marcos de referencia con el fin de estructurar, fortalecer y evaluar sus practicas de seguridad de la información, garantizando un enfoque sistemático y alineado con los objetivos estratégicos del negocio.

El estándar ISO/IEC 27001 constituye una referencia fundamental para la implementación y mantenimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en un enfoque que va orientado al riesgo. Este estándar permite definir políticas formales, establecer controles de seguridad y promover la mejora continua de los procesos de gestión de la seguridad de la información.

El diagnostico de ciberseguridad se estructuró con base en el NIST Cybersecurity Framework (versión 1.1), utilizado sus cinco funciones como eje de análisis para evaluar el nivel de madurez organizacional. Este enfoque permitió identificar brechas especificas en la gestión de activos, protección de la información, capacidades de detección, respuesta a incidentes y procesos de recuperación, facilitando la priorización de riesgos y el diseño del modelo de gestión propuesta. En cuanto a la gobernanza de las tecnologías de la información, se consideraron los siguientes marcos de referencia:

- COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas)

COBIT, desarrollado por ISACA, se emplea como marco de apoyo para la gobernanza y gestión de las tecnologías de la información, permitiendo alinear los controles de ciberseguridad con los objetivos del negocio mediante la definición de principios, objetivos de control, métricas y buenas prácticas.

- ISO 22301

La norma ISO 22301 se oriento a la gestión de la continuidad del negocio, estableciendo los lineamientos necesarios para asegurar la continuidad de las operaciones ante eventos disruptivos. Su integración con los marcos de ciberseguridad resulta fundamental, dado que un incidente de seguridad puede derivar en interrupciones significativas de los procesos críticos de la organización.

4. Contexto del Informe

El presente informe se desarrolla sobre un escenario organizacional representativo de empresas medianas en proceso de transformación digital. Dichas organizaciones suelen contar con infraestructura tecnológica funcionales, aunque fragmentada, y con un bajo nivel de formación en materia de ciberseguridad.

Este modelo corresponde a un modelo conceptual aplicado a un entorno tipo, y no a un estudio de caso real especifico. El objetivo es identificar brechas comunes, priorizar riesgos y proponer un modelo de gestión aplicable a organizaciones con características similares.

En este estudio se observaron en este entorno:

- Sin políticas sólidas de ciberseguridad: Las reglas son vagas o inexistentes, lo que dificulta el establecimiento de estándares.
- Monitoreo limitado de eventos: Ningún sistema rastrea o correlaciona eventos en tiempo real.
- Procesos manuales o no estructurados: Sin automatización, los errores ocurren con mayor frecuencia.
- Cultura de seguridad débil: El factor humano representa uno de los principales vectores de riesgo en materia de ciberseguridad.
- Sin planes de respuesta a incidentes o continuidad: No existen salvaguardas para las interrupciones.

Este tipo de configuración es frecuente en organizaciones en proceso de crecimiento y transformación digital. Este informe ayuda a detectar brechas, establecer prioridades y sugerir pasos para seguir mejorando.

5. Metodología

El informe corresponde a un análisis conceptual aplicado, con enfoque cualitativo y alcance descriptivo – propositivo. La metodología empleada se desarrolla a través de las siguientes etapas:

- Revisión de literatura y estándares internacionales en ciberseguridad y gestión de riesgos.
- Diagnóstico situacional basado en el NIST Cybersecurity Framework (versión 1.1).
- Identificación y análisis de riesgo mediante una matriz cualitativa.

- Diseño de modelo integral de gestión de ciberseguridad alineado con ISO/IEC 27001, NIST CSF, COBIT 2019 e ISO 22301.
- Integración de los aprendizajes adquiridos en el seminario académico.

6. Diagnóstico Situacional

Con el propósito de determinar el nivel de madurez en ciberseguridad de la organización, se realizó una evaluación basada en el **NIST Cybersecurity Framework (NIST CSF 1.1)**, abarcando sus cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.

El diagnóstico permitió evidenciar brechas significativas en procesos, tecnología y gestión, las cuales se describen a continuación.

6.1. Identificar (ID)

- La función identificar evalúa la capacidad de la organización para colocar, gestionar y comprender sus activos, riesgos y entorno operativo. Se identificaron las siguientes brechas:

6.1.1. Gestión de Activos (ID.AM)

- La organización no cuenta con un inventario completo, actualizado ni centralizado de activos tecnológicos (hardware, software, servicios en la nube, dispositivos móviles, sistemas críticos, etc.).
- No existe un proceso definido para el ciclo de vida de los activos, lo que dificulta su control, seguimiento y desincorporación segura.

6.1.2. Protección de Datos (ID.GV)

- No se ha implementado un esquema de clasificación y categorización de la información (pública, interna, confidencial, sensible):
- La falta de clasificación impide aplicar controles diferenciados según criticidad.

6.1.3. Gobernanza (ID.GV)

- Los roles y responsabilidades de ciberseguridad no están completamente formalizados, generando vacíos en la rendición de cuentas y la toma de decisiones.
- No existe un marco normativo interno ni políticas integrales de seguridad de la información.

6.2. Proteger (PR)

- La función Proteger abarcar los controles diseñados para limitar o contener el impacto de un evento de ciberseguridad.
- Estas son las deficiencias que encontramos:

6.2.1. Control de acceso (PR.AC)

- Las contraseñas son demasiado simples. No existe una política de caducidad y se utilizan credenciales compartidas.
- La ausencia de autenticación multifactorial (MFA)
- Protege las aplicaciones criticas o el acceso remoto.
- No se aplica el principio del mínimo privilegio, lo que permite el acceso innecesario a sistemas y datos confidenciales.
- La red no está segmentada, lo que permite que el tráfico fluya libremente entre áreas críticas y zonas de usuario.

6.2.2. Protección contra amenazas (PR.IP/PR.PT)

- Se instala antimalware, pero no hay un sistema de monitorización centralizado para rastrear alertas, actualizaciones o dispositivos desprotegidos.
- Las configuraciones de seguridad de los servidores y equipos no están estandarizadas; el reforzamiento es inconsistente.

6.3. Detectar (DE)

Así es como se evalúa la capacidad de una organización para detectar problemas de seguridad en el momento en que ocurre:

6.3.1. Monitoreo Continuo (DE.CM)

- Sin una plataforma SIEM, no hay correlación de eventos, análisis en tiempo real ni detencción proactiva de amenazas.
- Los registros generados por servidores, firewalls y dispositivos de red no son revisados de manera periódica ni sistemática.
- No se cuenta con mecanismos formales para la identificación y análisis de comportamientos anómalos dentro de los sistemas de información.

6.3.2. Auditorias y Evaluaciones (DE.AE)

- No se realizan auditorias de seguridad internas ni externas de forma regular.
- La ausencia de privas de penetración y análisis periódicos de vulnerabilidades incrementa significativamente el nivel de exposición a riesgos de seguridad.

6.4. Responder (RS)

La función de Respuesta verifica la eficacia de la organización de la gestión de incidentes de seguridad.

- Encontramos lo siguiente:

6.4.1. Planificación y Operaciones (RS.RP/RS.CO)

- No existe un Plan de Respuesta a incidentes (PRI)
- No está documentada, validado ni aprobado por la dirección
- No existen protocolos de escalamiento, matrices de comunicación ni roles claros para cada etapa de un incidente
- El personal no ha recibido formación formal en gestión de incidentes

6.4.2. Mejora Continua (RS.IM)

- No se realizan ejercicios prácticos ni simulaciones de escenarios para probar las respuestas.
- No se realizan revisiones de lecciones aprendidas ni actualizaciones de los procedimientos tras los incidentes.
- Esta situación limita la capacidad de preparación y reduce la efectividad de la respuesta ante incidentes.

6.5. Recuperar (RC)

- La función de recuperación se orienta al restablecimiento oportuno de los servicios críticos tras la ocurrencia de un incidente de seguridad.

6.5.1. Planificación de Recuperación (RC.RP)

- Las copias de seguridad se realizan manualmente y sin ningún proceso estándar, lo que significa que los datos importantes podrían pasar desapercibidos.
- No hay registro de comprobaciones regulares en estas copias de seguridad, por lo que no puede estar seguro de que funcionarán cuando las necesite.

6.5.2. Restauración y Continuidad (RC.IM/RC.CO)

- No hay pasos escritos para volver a poner los servicios en línea durante las interrupciones.
- No existe un Plan de Continuidad de Negocio (BCP) o Plan de Recuperación ante Desastres (DRP), por lo que si ocurre un desastre, no hay una hoja de ruta a seguir.

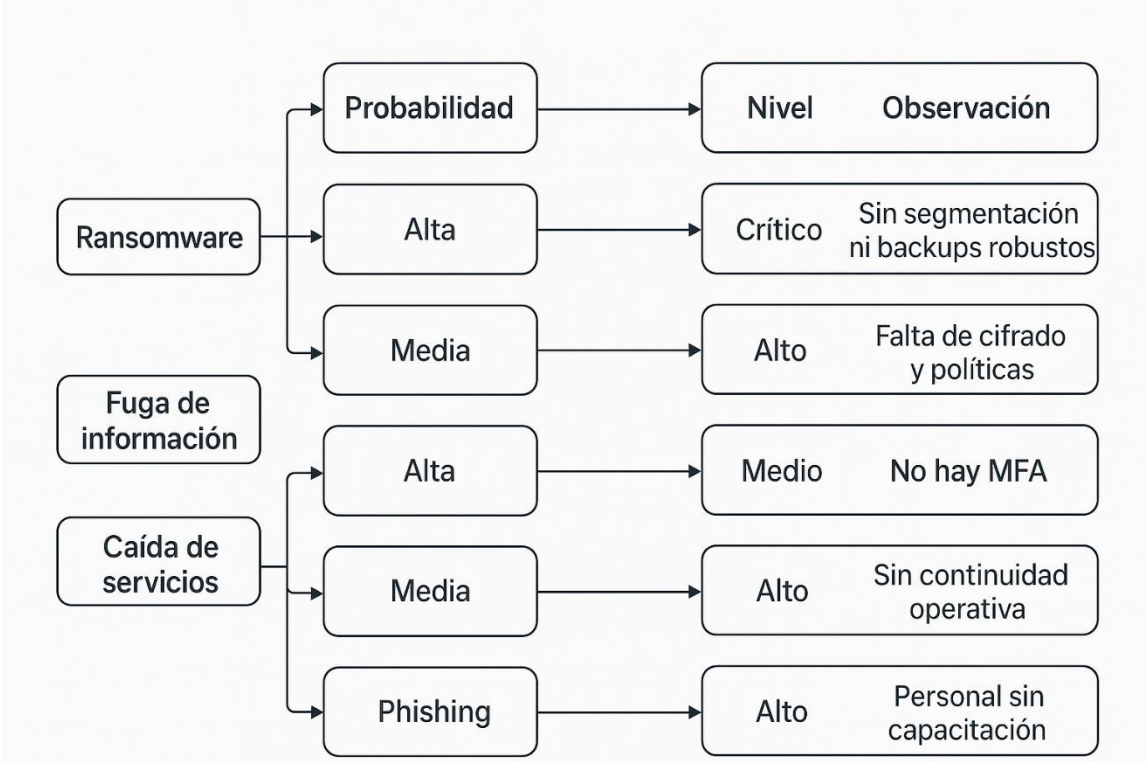
7. Análisis de riesgos

Tabla 1. Matriz de Riesgos

RIESGO	PROBABILIDAD	IMPACTO	NIVEL	OBSERVACIÓN
Ransomware	Alta	Alta	Crítico	Sin segmentación ni Backups robustos
Fuga de información	Media	Alta	Alto	Falta de cifrado y políticas
Robo de credenciales	Alta	Media	Alto	No hay MFA
Caída de servicios	Media	Media	Medio	Sin continuidad operativa
Phishing	Alta	Media	Alto	Personal sin capacitación

MATRIZ FODA

Fortalezas	Oportunidades
Evaluación clara de riesgos, identificación de prioridades	Implementar MFA, cifrado, segmentación, backups; capacitaciones; adoptar estándares
Debilidades	**Amenazas**
Falta de segmentación, backups, MFA, cifrado, politicas y capacitación	Ransomware, fuga de información, robo de credenciales, caidas de servicios, phishing



8. Modelo de Gestión de Ciberseguridad Propuesto

Este es un modelo para la gestión de la ciberseguridad que integra gobernanza, controles técnicos y organizativos, y monitoreo y respuesta en tiempo real. Está diseñado para ayudar a las organizaciones a fortalecer su seguridad, mantener el buen funcionamiento de sus operaciones y abordar eficazmente las ciber-amenazas emergentes. Este enfoque se alinea con los principales estándares internacionales, como la ISO/IEC 27001, el Marco de Ciberseguridad del NIST y las directrices de gestión de riesgos corporativos.

8.1. Gobernanza

La gobernanza es la columna vertebral de cualquier sistema de ciberseguridad. Garantiza que las decisiones, políticas y responsabilidades se alineen con los objetivos estratégicos de una organización.

8.1.1. Creación y adopción de políticas obligatorias de seguridad:

Se propone la creación de políticas formales que cubran el uso aceptable, la clasificación de la información, el control de acceso, la continuidad del negocio, la seguridad en el lugar de trabajo, el trabajo remoto y la retención de datos. Cada política tendrá una revisión anual y la aprobación del liderazgo para mantenerla relevante y efectiva.

8.1.2. Roles y responsabilidades de seguridad claros:

Se definen roles específicos dentro del ecosistema de seguridad:

- Un director de seguridad de la información (CISO) o equivalente.
- Un comité de seguridad de la información.
- Propietarios de activos y procesos.
- Usuarios administradores y custodios de datos.

También trazaremos una matriz RACI para realizar un seguimiento de las responsabilidades de la gestión de incidentes, la gestión de riesgos y las operaciones de control.

8.1.3. Implementación de un sistema de gestión de seguridad ISO 27001:

Esto sucede en tres fases:

1. Comenzaremos con un análisis de brechas contra los requisitos de ISO/IEC 27001:2022.
2. Luego, priorizaremos e implementaremos los controles del Anexo A en función del riesgo.
3. Finalmente, iniciaremos un ciclo de mejora continua (PDCA), realizaremos un seguimiento de las métricas, realizaremos auditorías internas y nos prepararemos para la certificación.
4. Esto mantiene el entorno de seguridad de la organización documentado, controlado y medible.

8.2. Controles Técnicos

Estos controles buscan reducir las vulnerabilidades y fortalecer la protección contra amenazas automatizadas y dirigidas.

8.2.1. Autenticación Multifactor (MFA)

Implementaremos MFA para puntos de acceso críticos, incluyendo:

- Servicios en la nube.
- VPN corporativas.
- Consolas de administración.
- Sistemas financieros y de misión crítica.
- Esto ayuda a prevenir el robo de credenciales, el phishing y el acceso no autorizado.

8.2.2. Plataforma de Protección Centralizada: EDR, Antivirus o XDR

Se propone la adopción de una solución avanzada:

- Prevención de malware y ransomware.
- Aislamiento automático de dispositivos comprometidos.
- Alertas correlacionadas e informes integrados.
- Esta configuración ayuda a detectar actividad inusual de forma temprana y agiliza la respuesta ante incidentes.

8.2.3. Segmentación de Red

Dividiremos la red en segmentos lógicos para aislar áreas críticas mediante VLAN, firewalls internos y políticas de confianza cero (Acceso a la Red de Confianza Cero — ZTNA). Esto limita la propagación de amenazas y mejora la gestión del acceso.

8.2.4. Actualizaciones automatizadas y gestión de parches

Estableceremos:

- Un inventario de activos actualizado.
- Aplicación automatizada de parches para sistemas operativos y aplicaciones.
- Pruebas previas a la implementación en entornos de prueba para sistemas críticos.

8.2.5. Políticas de cifrado y copias de seguridad.

- Cifrado de disco para portátiles y servidores.
- Cifrado TLS para datos en tránsito.
- Copias de seguridad automatizadas según la regla 3-2-1 con comprobaciones de integridad.
- Controles antiransomware para el almacenamiento.

8.3. Controles Organizacionales

La tecnología por sí sola no lo soluciona todo. Aquí es donde entran en juego los controles organizacionales: procesos, una sólida cultura de seguridad y una gestión rigurosa de terceros.

8.3.1. Capacitación Continua en Ciberseguridad

Implementaremos un plan de capacitación anual que abarca:

- Detección de intentos de phishing y prácticas seguras.
- Talleres prácticos para la protección de datos.
- Simulacros periódicos de ingeniería social.
- Capacitación avanzada para administradores sobre las mejores prácticas.

Esto se justifica debido a que el error humano representa una de las principales causas de incidentes de seguridad a nivel organizacional.

8.3.2. Simulacros periódicos de Respuesta a Incidentes

Realizaremos ejercicios prácticos, simulacros técnicos y pruebas de recuperación ante desastres para comprobar:

- Nuestra rapidez de respuesta.
- La eficacia del trabajo en equipo.
- Si nuestros procedimientos realmente funcionan.
- Si documentamos todo correctamente.

Estas actividades permiten evaluar la efectividad de los procedimientos establecidos y fortalecer la capacidad de respuesta ante incidentes reales.

8.3.3. Gestión de Proveedores y Terceros

Reforzaremos nuestra cadena de suministro con:

- Contratos que incluyan cláusulas de seguridad.
- Evaluaciones de riesgos para proveedores críticos.
- Controles regulares para garantizar que cumplan con nuestros estándares de seguridad.
- Revisiones periódicas de cómo manejan nuestros datos los terceros.

La gestión de la ciberseguridad requiere la participación coordinada de todos los actores organizacionales, incluyendo usuarios áreas técnicas y de alta dirección

8.4. Vigilancia y respuesta rápida

La detención temprana y la respuesta oportuna son elementos críticos para minimizar el impacto de los incidentes de seguridad. Por eso, la monitorización constante y las respuestas rápidas son su mejor defensa contra incidentes que podrían interrumpir el negocio.

8.4.1. Configuración de un sistema de monitorización centralizado

Un sistema SIEM (Gestión de información y eventos de seguridad) es una decisión inteligente. Debe gestionar:

- Recopilar y correlacionar registros de servidores, firewalls, herramientas EDR y aplicaciones.
- Activar alertas automáticas para patrones inusuales.
- Detectar amenazas avanzadas de forma temprana.
- Analizar los incidentes una vez que ocurren.

En organizaciones con menor nivel de madurez, la monitorización puede iniciarse mediante herramientas básicas, las cuales deben evolucionar progresivamente conforme aumentan las capacidades de seguridad.

8.4.2. Manual de respuesta a incidentes.

Necesitará un manual de respuesta a incidentes (IRM) formal que incluya:

- Cómo clasificar los incidentes.
- A quién involucrar y cuándo.
- Qué hace cada persona durante un incidente.
- Pasos para contener, eliminar y recuperarse de las amenazas.
- Qué informar interna y externamente.
- Lecciones aprendidas tras cada incidente.

8.4.3. Informes trimestrales de seguridad para el liderazgo.

Los ejecutivos deben recibir informes trimestrales con:

- Indicadores clave de rendimiento y riesgo (KPI/KRI).
- El funcionamiento de los controles.
- Riesgos detectados y abordados.
- Incidentes detectados y gestionados.
- Acciones pendientes o planificadas.

Esto mantiene a todos informados y ayuda al liderazgo a tomar decisiones estratégicas e inteligentes.

9. Desarrollo e Implementación del Aprendizaje

Las lecciones del seminario no se quedaron en el olvido. Tomamos lo aprendido y construimos un enfoque integral de gestión de ciberseguridad para entornos corporativos. ¿Cómo? Combinando teoría, mejores prácticas globales y técnicas de análisis basadas en estándares reconocidos. Como resultado, se obtiene un modelo de gestión sólido y escalable que se adapta a las necesidades de las organizaciones modernas.

Primero, mapeamos los activos críticos, sopesando la exposición, el valor estratégico y la dependencia operativa. Este paso nos proporcionó una visión clara del panorama de la organización, las superficies de ataque y las posibles vulnerabilidades según su configuración tecnológica.

A continuación, realizamos un diagnóstico utilizando marcos como ISO/IEC 27001, NIST CSF y las mejores prácticas de gestión de riesgos. El cruce de estas normas nos ayudó a identificar brechas de cumplimiento y puntos débiles en la arquitectura de seguridad, lo que nos permitió saber exactamente qué era necesario reforzar. Con esta información, construimos un modelo de solución estructurado: políticas, controles, diagramas de referencia y un plan de acción priorizado.

Abarca desde la gestión de identidades y la protección perimetral hasta la monitorización continua, la respuesta a incidentes y la capacitación del personal. El modelo abarca de manera integral los principales componentes de la gestión de la ciberseguridad. Para probar nuestro trabajo, creamos escenarios y simulaciones reales. Incorporamos evaluaciones de riesgos, modelado de amenazas, categorización de activos y definiciones de control de seguridad, todo

diseñado para reflejar los desafíos organizacionales reales. Esto nos permitió verificar la eficacia de nuestras estrategias. Finalmente, incorporamos la mejora continua.

Los indicadores de rendimiento, las métricas de madurez y los ciclos de retroalimentación garantizan la evolución constante de la gestión de la ciberseguridad. ¿El objetivo? Convertir la teoría en procesos prácticos y sostenibles que se alineen con los objetivos del negocio

10. Conclusiones

La gestión de la ciberseguridad se ha convertido en un pilar fundamental para mantener las operaciones en marcha, desarrollar resiliencia digital y proteger los activos críticos en cualquier organización moderna. Nuestro análisis reveló algunas deficiencias evidentes en la gobernanza, las políticas, los controles técnicos y los procesos de respuesta a incidentes.

La solución se fundamenta en la adopción de un enfoque integral y sistemático.

La ausencia de un modelo sólido de ciberseguridad expone a las organizaciones a ataques, fugas de información y afectaciones a la continuidad operativa, impactando negativamente la confianza de clientes y partes interesadas. Nuestro modelo propuesto ofrece una hoja de ruta para reforzar la seguridad. Se basa en marcos reconocidos como la ISO/IEC 27001 y el Marco de Ciberseguridad del NIST, junto con políticas de gestión de riesgos.

También promueve controles preventivos, de detección y correctivos, además de métricas para monitorizar el correcto funcionamiento de todo. La cultura también importa. Necesitamos organizaciones donde todos practiquen un buen manejo de la información, utilicen la tecnología de forma responsable y reporten los incidentes lo antes posible. La ciberseguridad no es algo que se soluciona una sola vez. Es un proceso continuo que exige monitoreo constante, actualizaciones y la capacidad de adaptarse a la evolución de las amenazas.

En síntesis, este modelo de gestión puede ayudar a las organizaciones a fortalecer su resiliencia tecnológica, reducir drásticamente las vulnerabilidades, optimizar los recursos de seguridad y perfeccionar su capacidad para anticipar, detectar y responder a los ciberataques. Es una base sólida para alcanzar mayores niveles de madurez y cumplimiento normativo.

11. Referencias

International Organization for Standardization. (2019). *ISO 22301:2019 — Security and resilience — Business continuity management systems — Requirements*. ISO. https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

International Organization for Standardization. (2019). *Guía de implantación ISO 22301*. NQA. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-22301-Guia-de-implantacion.pdf

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO. https://www.iso.org/standard/27001

ANSI National Accreditation Board. (2022). *ISO/IEC 27001:2022 information security management systems*. ANSI Blog. https://blog.ansi.org/anab/iso-iec-27001-2022-information-security-systems/

Almeida, R. (2022). *ISO 27001 Information Security Management Systems*. ResearchGate. https://www.researchgate.net/publication/367166657_ISO_27001_Information_Security_Management_Systems

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments (NIST SP 800-30 Rev. 1)*. U.S. Department of Commerce. http://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5)*. U.S. Department of Commerce. http://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

ISACA. (2018). *COBIT 2019 design guide: Designing an information and technology governance solution*. ISACA. http://www.isaca.org/resources/cobit

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA. http://www.isaca.org/resources/cobi

European Union Agency for Cybersecurity. (2016). *ENISA threat landscape report*. ENISA. http://www.enisa.europa.eu/publications

SANS Institute. (2020). *Incident handler's handbook*. SANS Institute. http://www.sans.org/white-papers

Broadcom Inc. (2022). *Internet security threat report*. Symantec. http://www.broadcom.com/support/security-center

Microsoft Corporation. (2021). *Zero Trust architecture*. Microsoft. https://www.microsoft.com/security/business/zero-trust

Cisco Systems, Inc. (2020). *Cisco Zero Trust: Security for the modern workforce*. Cisco Press. http://www.cisco.com/go/zerotrust

Cybersecurity and Infrastructure Security Agency. (2021). *Ransomware guide*. U.S. Department of Homeland Security. http://www.cisa.gov/ransomware

Up Klatam. (s. f.). *Seguridad en la nube y física*. https://www.upklatam.com/ciberseguridad-y-cloud/seguridad-en-la-nube-y-fisica/