Controles NCH ISO 31000: Relacionados

Control	Nombre
4	Principios
5.7	Mejora
6.2	Comunicación y consulta
6.3	Alcance, contexto y criterios
6.4	Evaluación del riesgo
6.5	Tratamiento del riesgo
6.6	Seguimiento y revisión

Controles NCH ISO 27001: Relacionados

Control	Nombre
A.07.02.02	Concienciación, educación y formación en seguridad de la información
A.06.01.02	Evaluación de riesgos de seguridad de la información
A.06.01.03	Tratamiento de riesgos de seguridad de la información
A.16.01	Gestión de incidentes de seguridad de la información

Controles NCH ISO 27005 Relacionados

Control	Nombre
7	Establecimiento del contexto
8.2.1	Identificación del riesgo
8.2	Análisis del riesgo
8.3	Evaluación del riesgo
9	Tratamiento del riesgo en la seguridad de la información
12	Monitoreo y revisión del riesgo en la seguridad de la información
11	Comunicación de los riesgos para la seguridad de la información

Control de versiones

FECHA	VERSIÓN	RESPONSABLES	DESCRIPCIÓN
22-03-2024	1.0	Jorge Romero	Elaboración del Documento

1. Introducción

El avance tecnológico ha transformado de manera significativa el funcionamiento de todas las áreas operativas actuales, convirtiéndose en un elemento esencial para las instituciones. Esta evolución ha traído consigo un aumento en la dependencia de sistemas digitales, redes y bases de datos, lo que a su vez ha incrementado la vulnerabilidad a una amplia gama de riesgos. Estos riesgos incluyen ciberataques, fallas de sistema, pérdida de datos y obsolescencia tecnológica. Dado este contexto de riesgos en constante cambio, se hace imperativo adoptar un enfoque estratégico y dinámico para su gestión, uno que no solo reconozca los desafíos actuales, sino que también se anticipe y adapte a las futuras tendencias tecnológicas.

El Plan de Gestión de Riesgo Tecnológico de la institución se ha desarrollado con el objetivo de identificar, evaluar y mitigar eficazmente los riesgos tecnológicos que enfrenta nuestra institución. Este documento sirve como una hoja de ruta para la protección de nuestros activos tecnológicos y la garantía de la continuidad operativa y la resiliencia institucional.

Este plan abarca un enfoque integral que incluye la evaluación del entorno tecnológico actual, la identificación y evaluación de riesgos potenciales, el desarrollo de estrategias de mitigación y respuesta, junto con la implementación de programas de formación y concientización para los/las funcionarios/as y colaboradores. Además, establece procedimientos claros para el monitoreo, revisión y comunicación continua, asegurando que la gestión de riesgos tecnológicos se mantenga alineada con los objetivos y estrategias generales de la institución.

La efectividad de este plan depende de su continua revisión y adaptación. Por lo tanto, se compromete a una evaluación y actualización regular para reflejar los cambios en el entorno tecnológico, así como en nuestras operaciones y estrategias institucionales. La implementación y el éxito de este plan requieren la participación y el compromiso de todas las áreas de la institución, fortaleciendo así nuestra postura frente a los desafíos tecnológicos y asegurando nuestro éxito continuo en un mundo digital en constante cambio.

2. Contexto y necesidad

Dada la creciente dependencia de nuestra institución en la tecnología, enfrentamos varios riesgos, incluyendo vulnerabilidades de seguridad cibernética, fallas tecnológicas y pérdida de datos. Este plan es una respuesta estratégica para abordar estos desafíos y proteger nuestros activos.

3. Estructura del Plan

El plan se estructura en base a las siguientes secciones:

Evaluación del entorno tecnológico

Obtener un entendimiento completo del entorno tecnológico de la institución, incluyendo todos los activos tecnológicos y la infraestructura existente. Esta etapa ayuda a identificar los recursos críticos que deben ser protegidos y los posibles vectores de ataque o vulnerabilidades.

Gestión de riesgos

La gestión de riesgos debe ser considerada una prioridad en la protección y el funcionamiento eficiente de cualquier institución, especialmente en lo concerniente a la gestión de la tecnología y la información. Esto se debe a que la identificación y evaluación de riesgos son procesos fundamentales que permiten a una institución prepararse y responder de manera efectiva a posibles amenazas. A continuación, se describen dos componentes esenciales en el proceso de gestión de riesgos que deben ser implementados:

Identificación de riesgos

Es fundamental llevar a cabo un proceso sistemático de reconocimiento y documentación de todos los posibles riesgos y amenazas tecnológicas, tanto internas como externas, que podrían afectar a la institución. Esta identificación constituye el primer paso crítico para poder gestionar los riesgos de manera adecuada. Sin una identificación exhaustiva de los riesgos, las estrategias de mitigación no podrán ser completamente efectivas, ya que los esfuerzos podrían no estar dirigidos a las amenazas reales o más significativas.

Evaluación de riesgos

Tras la identificación de los riesgos, el siguiente paso es evaluarlos cuidadosamente en términos de su probabilidad de ocurrencia y el impacto potencial que podrían tener sobre la institución. Esta evaluación es crucial para la priorización de riesgos, ya que permite a la institución enfocar sus esfuerzos de mitigación y preparación en aquellos riesgos que presentan mayores amenazas en términos de probabilidad y/o impacto. La evaluación de riesgos ayuda a las instituciones a desarrollar una comprensión clara de dónde deben asignar sus recursos limitados para lograr la máxima eficacia en la reducción de vulnerabilidades.

Estrategias de mitigación y planes de respuesta

Desarrollar estrategias específicas y procedimientos de respuesta para mitigar los riesgos identificados. Esto incluye la definición de acciones preventivas y reactivas para minimizar el impacto de los riesgos en la operación de la institución.

Implementación y ejecución

Poner en práctica las estrategias y planes de respuesta diseñados. Esto implica la asignación de responsabilidades y recursos, así como el establecimiento de cronogramas para asegurar que las medidas de mitigación se implementen efectivamente.

Capacitación y concientización

Aumentar la conciencia y preparación del personal respecto a los riesgos tecnológicos y las medidas de seguridad. La capacitación continua asegura que todos los/las funcionarios/as y colaboradores comprendan su papel en la protección de los activos tecnológicos y en la prevención de incidentes.

Monitoreo, revisión y actualización

Establecer procesos continuos para monitorear el entorno tecnológico y los riesgos asociados, revisar regularmente la eficacia del plan de gestión de riesgos y actualizarlo conforme sea necesario para adaptarse a nuevos riesgos o cambios en el entorno tecnológico.

Comunicación y reporte

Mantener líneas claras de comunicación tanto interna como externamente sobre el estado del riesgo tecnológico y las medidas de seguridad implementadas. El reporte regular asegura que las partes interesadas estén informadas y puedan tomar decisiones basadas en la información actualizada sobre riesgos y seguridad.

Reportes de gestión

Elaborar y distribuir reportes de gestión detallados es un componente crucial en la estrategia de gestión de riesgos de cualquier institución. Estos informes proporcionan un análisis comprehensivo y actualizado del estado de los riesgos tecnológicos, las acciones de mitigación implementadas y la eficacia de las estrategias de respuesta frente a los riesgos identificados. La finalidad es asegurar que autoridades y las

partes interesadas clave tengan la información necesaria para comprender el panorama de riesgos tecnológicos y tomar decisiones informadas respecto a la seguridad de la información y la gestión de riesgos.

4. Importancia de la capacitación y concientización

La formación y concientización de los/las funcionarios/as y colaboradores son fundamentales para la prevención y gestión efectiva de los riesgos tecnológicos. Programas de capacitación regulares y campañas de concientización aseguran que el personal esté informado sobre las mejores prácticas y protocolos de seguridad.

5. Monitoreo y actualización continua

El plan enfatiza la importancia del monitoreo continuo de los riesgos tecnológicos y la necesidad de actualizar regularmente el plan para reflejar los cambios en el panorama tecnológico y en las operaciones de la institución.

6. Compromiso institucional

La ejecución exitosa de este plan requiere el compromiso y la colaboración de todas las áreas de la institución. Este enfoque integrado garantiza una gestión de riesgos tecnológicos cohesiva y eficaz, vital para la seguridad y el éxito continuo de nuestra institución.

7. Objetivo

Establecer un enfoque sistemático y estructurado para identificar, evaluar, mitigar y manejar los riesgos asociados con la tecnología en el Ministerio. Este enfoque no solo busca proteger los activos tecnológicos críticos de la institución, sino también asegurar la continuidad y eficiencia de las operaciones frente a posibles amenazas tecnológicas. Los objetivos específicos incluyen:

Protección de activos tecnológicos

Salvaguardar la infraestructura tecnológica, incluyendo hardware, software y datos, contra amenazas internas y externas.

Identificación de riesgos

Identificar y evaluar exhaustivamente los riesgos tecnológicos que podrían amenazar nuestra institución, incluyendo activos críticos, amenazas y vulnerabilidades.

Mitigación efectiva
Implementar medidas de mitigación y protección específicas para reducir la exposición a los riesgos identificados y proteger nuestros activos de tecnología de la información.

Minimización de interrupciones operativas
Implementar estrategias que minimicen las interrupciones de las operaciones del negocio debido a fallos tecnológicos o ciberataques.

Cumplimiento normativo
Asegurar que todas las prácticas tecnológicas y de gestión de riesgos se encuentren en conformidad con las leyes y regulaciones aplicables.

Preparación ante incidentes
Fortalecer nuestra capacidad de respuesta ante incidentes tecnológicos, minimizando el impacto y reduciendo los tiempos de recuperación.

Cultura de concienciación en seguridad
Fomentar una cultura institucional que priorice la seguridad tecnológica y la gestión de riesgos entre todos los/las funcionarios/as y colaboradores.

8. Alcance

El alcance del Plan de Gestión de Riesgo Tecnológico es amplio y abarca todos los aspectos de la tecnología utilizados en la institución. Esto incluye, pero no se limita a:

Tecnologías de información y comunicaciones (TIC)
Todos los sistemas de TIC, aplicaciones, redes y dispositivos utilizados en la institución.

Datos e información
La gestión y protección de datos institucionales, incluyendo datos personales, información confidencial y propiedad intelectual.

Infraestructura tecnológica
Incluye la infraestructura física y virtual, como centros de datos, servidores y sistemas de almacenamiento.

Operaciones y procesos de la institución
Todos los procesos de la institución que dependen de la tecnología, incluyendo operaciones electrónicas, la gestión de la cadena de suministro y las operaciones financieras.

Funcionarios/as, colaboradores y partes interesadas
Involucra a todos los/las funcionarios/as, colaboradores, contratistas y terceros que interactúan con los sistemas y tecnologías de la institución.

Cumplimiento y normativas
Abarca todos los aspectos relacionados con el cumplimiento normativo y legal en relación con la tecnología.

Este plan está diseñado para ser aplicable en todos los niveles de la institución y en todas las áreas que utilicen o se vean afectadas por la tecnología. Su implementación efectiva es fundamental para la resiliencia y seguridad global del Ministerio, permitiéndole enfrentar desafíos tecnológicos actuales y futuros con confianza y preparación.

9. Estructura del plan de gestión de riesgos tecnológicos

9.1. Evaluación del entorno tecnológico

9.1.1. Inventario de activos
El inventario de activos tecnológicos es un proceso exhaustivo y detallado que implica la identificación y documentación de todos los recursos tecnológicos que posee y utiliza la institución. Este proceso debe incluir:

Hardware
Registrar todos los dispositivos físicos como servidores, computadores, dispositivos móviles, impresoras, y equipos de red. Cada ítem debe documentarse con detalles como modelo, ubicación, estado y fecha de adquisición.

Software
Incluir todos los programas de software, sistemas operativos, bases de datos, y aplicaciones, especificando la versión, licencias, fecha de instalación y cualquier personalización realizada.

Datos y almacenamiento
Hacer un inventario de dónde se almacenan los datos (servidores locales, nube, etc.), los tipos de datos (personales, financieros, operativos) y su nivel de sensibilidad y confidencialidad.

Integraciones y dependencias
Mapear las interconexiones entre diferentes activos tecnológicos, identificando dependencias críticas.

Documentación y configuraciones
Recopilar documentación técnica, manuales de usuario y configuraciones de seguridad actuales.

Aspectos de cumplimiento y licencias
Verificar el cumplimiento de licencias de software y estándares de la industria.

9.1.2. Evaluación de la infraestructura actual

La evaluación de la infraestructura tecnológica actual es un análisis profundo que busca identificar fortalezas, debilidades y oportunidades de mejora en el entorno tecnológico de la institución. Este proceso incluye:

Revisión de la arquitectura de red
Evaluar la configuración de la red, incluyendo la topología, el rendimiento, la seguridad y la redundancia.

Análisis de seguridad
Realizar auditorías de seguridad para identificar vulnerabilidades y riesgos en la infraestructura tecnológica.

Evaluación del rendimiento de los sistemas
Medir el rendimiento de los sistemas críticos para identificar cuellos de botella y necesidades de actualización o escalabilidad.

Revisión de procesos de respuesta a incidentes
Evaluar la eficacia de los protocolos actuales de respuesta ante incidentes tecnológicos y recuperación de desastres.

Análisis de costo-eficiencia
Examinar el gasto actual en infraestructura tecnológica en comparación con el rendimiento y los resultados obtenidos.

Consultas con usuarios finales y grupos especiales de interés
Obtener retroalimentación de los usuarios para entender cómo la infraestructura tecnológica afecta su trabajo diario y la eficiencia operativa.

Verificación de actualizaciones y mantenimiento
Comprobar que todos los sistemas estén actualizados y que se cumplan los calendarios de mantenimiento recomendados.

9.2. Gestión de riesgos

9.2.1. Identificación de riesgos

9.2.1.1. Análisis de amenazas y vulnerabilidades

El análisis de amenazas y vulnerabilidades es un componente crítico de la gestión de riesgos tecnológicos, diseñado para identificar los puntos débiles que podrían ser explotados y los posibles agentes de amenaza que podrían explotarlos. Este proceso se compone de varias etapas detalladas:

Evaluación de vulnerabilidades
Se deberán utilizar herramientas automatizadas y auditorías manuales para escanear sistemas, redes y aplicaciones en busca de vulnerabilidades conocidas. Esto incluye, pero no se limita a, configuraciones inseguras, software desactualizado y fallas de seguridad en el código fuente de aplicaciones.

Análisis de amenazas
Estudia las potenciales fuentes de amenaza, tanto internas como externas y evalúa la motivación, capacidad y oportunidad que podrían tener para explotar las vulnerabilidades identificadas. Las fuentes externas incluyen actores de amenazas como hackers o grupos de crimen organizado, mientras que las internas pueden incluir los/las funcionarios/as o colaboradores descontentos o descuidados.

Identificación de escenarios de ataque
Desarrolla escenarios detallados que describen cómo las vulnerabilidades podrían ser explotadas por las amenazas identificadas para comprometer la seguridad, integridad, o disponibilidad de los activos tecnológicos.

Evaluación de la exposición al riesgo
Determina el grado de exposición de la institución a cada amenaza, teniendo en cuenta las medidas de seguridad existentes y la probabilidad de que un atacante tenga éxito.

9.2.1.2. Registro de riesgos

El registro de riesgos es una herramienta esencial para documentar y gestionar los riesgos identificados de manera estructurada. Cada entrada en el registro debe incluir información detallada sobre el riesgo, tales como:

Descripción del riesgo

Una explicación clara y concisa del riesgo, incluyendo la vulnerabilidad que lo permite y la amenaza que lo explota.

Probabilidad de ocurrencia

Una evaluación cuantitativa o cualitativa de la frecuencia con la que se espera que ocurra el evento de riesgo. Esto puede basarse en datos históricos, tendencias del sector y la evaluación experta.

Impacto potencial

Una evaluación del daño que el evento de riesgo podría causar a la institución, que puede incluir pérdidas financieras, daño a la reputación, interrupción de las operaciones, entre otros. El impacto deberá ser clasificado como: Crítico, muy alto, alto, medio, bajo o sin impacto.

Crítico				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Causa una parálisis total o casi total de las operaciones críticas de la institución.	Implica una exposición masiva de datos confidenciales o regulados, poniendo en riesgo la privacidad de los datos personales, secretos o información gubernamental clasificada.	Provoca pérdidas financieras catastróficas que podrían amenazar la viabilidad de la institución.	Tiene el potencial de causar un daño irreparable a la reputación de la institución.	Incumple de manera significativa con las leyes y regulaciones aplicables, resultando en sanciones severas o litigios de gran envergadura.
Recuperación	La recuperación es extremadamente difícil y requiere una cantidad significativa de tiempo y recursos.			
Ejemplo	Ataques que causan interrupciones masivas de servicios críticos, brechas de seguridad que exponen grandes volúmenes de datos sensibles, incluyendo información financiera o de identificación personal.			

Tiempo de solución	Inmediato a 4 horas.

Muy alto				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Interrumpe las operaciones críticas, pero permite cierta capacidad operativa limitada.	Exposición de datos sensibles significativa, pero no a una escala masiva.	Causa pérdidas financieras importantes, pero no catastróficas.	Puede resultar en un daño significativo a la reputación que requerirá esfuerzos considerables para recuperarse.	Resulta en incumplimientos legales o de regulaciones que pueden llevar a sanciones significativas o litigios.
Recuperación	La recuperación es desafiante y requiere recursos considerables y tiempo.			
Ejemplo	Ataques que resultan en una pérdida financiera significativa o robo de propiedad intelectual valiosa para la institución.			
Tiempo de solución	4 a 8 horas.			

Alto				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Afecta las operaciones no críticas o causa interrupciones temporales en las operaciones críticas.	Involucra una pérdida de datos sensibles limitada o controlada.	Provoca un impacto financiero moderado que la organización puede manejar sin riesgo de viabilidad.	Causa preocupación entre clientes o socios, pero es manejable con esfuerzos de comunicación efectivos.	Implica posibles incumplimientos de leyes o regulaciones que pueden ser rectificados sin sanciones severas.
Recuperación	La recuperación es manejable con los recursos existentes, aunque puede requerir esfuerzos significativos.			
Ejemplo	Ataques que interrumpen servicios no críticos o que conducen a la pérdida de datos no esenciales, pero aún sensibles.			
Tiempo de solución	8 a 24 horas.			

Medio				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**

Causa inconvenientes menores en las operaciones, pero no afecta significativamente la continuidad operacional de la institución.	Puede involucrar una exposición mínima de datos sensibles, manejable mediante procedimientos estándar de respuesta.	Tiene un impacto financiero menor, con costos asociados principalmente a la investigación y remedio del incidente.	Puede generar preguntas o preocupaciones menores entre las partes interesadas, pero no afecta significativamente la percepción pública.	Puede requerir revisiones de cumplimiento, pero no se espera que resulte en sanciones o incumplimientos graves.
Recuperación	La recuperación está dentro de las capacidades normales de respuesta y manejo de incidentes.			
Ejemplo	Infecciones por malware que afectan un número limitado de sistemas, incidentes de phishing que no tienen resultados en pérdida de datos sensibles.			
Tiempo de solución	1 a 3 días continuos.			

Bajo				
Impacto	**Datos sensibles**	**Daño financiero**	**Reputación**	**Cumplimiento legal**
Tiene un impacto insignificante en las operaciones diarias.	No hay pérdida de datos sensibles o la pérdida es insignificante y fácilmente contenible.	El impacto financiero es mínimo, con costos limitados a acciones correctivas menores.	Tiene un impacto despreciable o nulo en la reputación de la institución.	No se espera que viole leyes o regulaciones o que cualquier incumplimiento sea de naturaleza menor y fácilmente corregible.
Recuperación	La recuperación es rápida y requiere recursos mínimos.			
Ejemplo	Ataques fallidos o exitosos que no comprometen datos sensibles ni afectan significativamente las operaciones del negocio.			
Tiempo de solución	3 a 7 días continuos.			

Sin impacto
El incidente de seguridad no presenta impacto apreciable dentro de la institución.

Medidas de mitigación existente

Una descripción de los controles o medidas de seguridad implementadas para mitigar el riesgo.

Acciones de mitigación planificadas
Identificación de las acciones adicionales necesarias para tratar el riesgo, incluyendo la asignación de responsabilidades y plazos para su implementación.

Estado del riesgo
Indica si el riesgo está pendiente, ha sido mitigado o ha sido aceptado por la dirección como un riesgo residual.

Revisión y actualizaciones
Fecha de la última revisión del riesgo y cualquier actualización sobre el estado de las acciones de mitigación.

9.2.2. Evaluación de Riesgos

9.2.2.1. Análisis de Impacto

El análisis de impacto es un proceso crítico dentro de la gestión de riesgos tecnológicos que se centra en evaluar el efecto potencial que los riesgos identificados podrían tener sobre las operaciones, la reputación, la viabilidad financiera y otros aspectos clave de una institución. Este proceso involucra una evaluación meticulosa de cómo un incidente de seguridad, falla tecnológica o cualquier otro evento de riesgo podría afectar a la entidad. A continuación, se detallan los componentes principales de un análisis de impacto:

Categorización del impacto
El impacto se evalúa en varias categorías para comprender plenamente su alcance y naturaleza:

Categoría	Descripción
Operativo	Interrupción de procesos críticos de la institución, impacto en la capacidad de entrega de servicios o productos.
Financiero	Pérdidas económicas directas, costos de recuperación, penalizaciones por incumplimiento de acuerdos de nivel de servicio SLA, impacto en el presupuesto institucional.
Reputacional	Daño a la imagen pública de la institución, pérdida de confianza de organismo gubernamentales y ciudadanía.
Legal y cumplimiento	Exposición a litigios, sanciones, y multas por incumplimiento de leyes y regulaciones.

Seguridad de la Información	Compromiso de la confidencialidad, integridad y disponibilidad de datos críticos.
Social y ambiental	Impactos en la comunidad y el medio ambiente.

Escala de gravedad

Para cada categoría de impacto, se establece una escala de gravedad que puede ir desde bajo hasta crítico. Esta escala ayuda a cuantificar y priorizar los riesgos:

Gravedad	Descripción
Crítico	Causa una parálisis total o casi total de las operaciones críticas de la institución.
Muy alto	Interrumpe las operaciones críticas, pero permite cierta capacidad operativa limitada.
Alto	Afecta las operaciones no críticas o causa interrupciones temporales en las operaciones críticas.
Medio	Causa inconvenientes menores en las operaciones, pero no afecta significativamente la continuidad operacional de la institución.
Bajo	Tiene un impacto insignificante en las operaciones diarias.

Metodología de evaluación

Análisis cualitativo	Análisis cuantitativo
Basado en la experiencia, conocimiento de la institución y juicio experto para estimar el impacto	Utiliza datos históricos, modelos financieros, y otras herramientas analíticas para estimar pérdidas potenciales en términos monetarios o métricas operativas

Identificación de activos críticos

Determinar cuáles son los activos más críticos para las operaciones de la institución y cómo su compromiso afectaría al funcionamiento general. Esto incluye sistemas clave, datos esenciales, infraestructura crítica y recursos humanos indispensables.

Desarrollo de escenarios

Crear escenarios de riesgo específicos para entender mejor el impacto potencial. Cada escenario describe cómo un evento de riesgo podría desarrollarse, los activos afectados y las consecuencias resultantes. Esto ayuda a visualizar posibles cadenas de eventos y preparar respuestas más efectivas.

Planes de respuesta y recuperación

Basado en el análisis de impacto, desarrollar o ajustar los planes de respuesta a incidentes y recuperación de desastres para asegurar que la institución pueda responder efectivamente y minimizar el daño.

Revisión continua

El análisis de impacto no es un proceso estático; debe revisarse regularmente para reflejar cambios en el entorno de la institución, la introducción de nuevas tecnologías y la emergencia de nuevas amenazas.

Realizar un análisis de impacto exhaustivo y detallado es fundamental para entender la verdadera magnitud de los riesgos tecnológicos y para preparar a la institución para gestionarlos de manera efectiva.

9.2.2.2. Priorización de riesgos

La priorización de riesgos es un paso crucial en la gestión de riesgos que ayudará a determinar qué riesgos requieren atención inmediata y recursos, basándose en su severidad y probabilidad de ocurrencia. Este proceso implica clasificar los riesgos identificados para enfocar los esfuerzos de mitigación de manera eficiente y efectiva. Aquí se detalla cómo se puede realizar esta priorización:

Establecimiento de criterios de evaluación

Para una clasificación eficaz, es esencial establecer criterios claros para evaluar tanto la severidad (impacto) como la probabilidad de ocurrencia de cada riesgo. Estos criterios deben ser específicos para la institución y pueden incluir aspectos financieros, operativos, legales, de reputación, entre otros.

Matriz de riesgos

Una herramienta comúnmente utilizada para la priorización es la matriz de riesgos, que cruza la probabilidad de ocurrencia del riesgo con su impacto potencial. Cada eje se divide en categorías (bajo, medio, alto), y cada riesgo se coloca en la matriz según su evaluación.

Categorización

Riesgo	Descripción
Alta Prioridad (Rojo)	Riesgos que caen en el cuadrante de alta probabilidad y alto impacto. Estos requieren atención inmediata y planes de mitigación robustos.
Media Prioridad (Amarillo)	Riesgos con una combinación de alta probabilidad y bajo impacto, o baja probabilidad y alto impacto. Requieren acciones de mitigación y monitoreo regulares.

Baja Prioridad (Verde)	Riesgos de baja probabilidad y bajo impacto. Se les puede dar menos atención inmediata, pero deben ser monitoreados en caso de cambios en su evaluación.

Evaluación cuantitativa y cualitativa

Cuantitativa	Cualitativa
Usa datos históricos y análisis estadísticos para asignar valores numéricos a la probabilidad e impacto, permitiendo una comparación objetiva.	Se basa en el juicio de expertos para estimar la severidad y la probabilidad, útil cuando no hay suficientes datos para un análisis cuantitativo.

Revisión de controles existentes

Considerar la efectividad de los controles existentes para reducir la probabilidad o el impacto de los riesgos. Un control efectivo puede disminuir la prioridad de un riesgo.

Factores adicionales

Factor	Descripción
Urgencia	Cuán pronto podría materializarse el riesgo.
Tendencias	Si la probabilidad o impacto del riesgo está aumentando o disminuyendo con el tiempo.
Interdependencias	Cómo la materialización de un riesgo puede afectar o ser afectada por otros riesgos.

Actualización y revisión continua

La priorización de riesgos no es un proceso estático; debe revisarse regularmente para reflejar el cambio en el entorno operativo, la aparición de nuevos riesgos, y la efectividad de los controles de mitigación implementados.

Comunicación y documentación

Los resultados de la priorización deben ser comunicados a todas las partes interesadas relevantes y documentados apropiadamente. Esto asegura que los responsables de la toma de decisiones estén informados sobre los riesgos más críticos y puedan asignar recursos adecuadamente.

La priorización eficaz de los riesgos permite a las instituciones enfocarse en los riesgos más significativos, asegurando que los recursos de mitigación se asignen de manera efectiva para proteger los objetivos organizacionales y minimizar las interrupciones operativas.

9.3. Estrategias de mitigación y planes de respuesta

9.3.1. Desarrollo de estrategias de mitigación

El desarrollo de estrategias de mitigación implica la creación de planes de acción específicos destinados a reducir la probabilidad de ocurrencia de un riesgo identificado, minimizar su impacto o idealmente, eliminarlo por completo. Este proceso detallado requiere un enfoque metódico para asegurar que cada riesgo se aborde de manera efectiva. A continuación, se detallan los pasos y consideraciones clave en el desarrollo de estas estrategias:

Análisis de la raíz del problema

Antes de formular cualquier estrategia, es crucial entender la causa raíz de cada riesgo. Esto puede implicar un análisis más profundo de los sistemas, procesos, o prácticas que contribuyen al riesgo, utilizando herramientas como el análisis de cinco porqués o diagramas de Ishikawa (causa-efecto).

Definición de objetivos de mitigación

Establecer objetivos claros para la mitigación de cada riesgo, que pueden variar desde la reducción del impacto potencial hasta la prevención total de la ocurrencia del riesgo. Estos objetivos deben ser específicos, medibles, alcanzables, relevantes y temporales (Objetivos SMART).

Identificación de opciones de mitigación

Para cada riesgo, se deben explorar múltiples opciones de mitigación, teniendo en cuenta su efectividad, coste y viabilidad. Las opciones incluyen:

Opción de mitigación	Descripción
Prevención	Implementar medidas que eviten que el riesgo se materialice.
Detección y respuesta	Mejorar la capacidad de detectar rápidamente el riesgo y responder de manera efectiva.
Transferencia	Desplazar el riesgo a otra parte, como a través de seguros o contratos con terceros.
Aceptación	En algunos casos, el coste de mitigación puede superar el beneficio, llevando a la decisión de aceptar y monitorear el riesgo.

Evaluación de impacto de la mitigación

Para cada estrategia propuesta, evaluar cómo cambiará la probabilidad y/o el impacto del riesgo. Esto puede requerir análisis cuantitativos o cualitativos y debe considerar cualquier efecto secundario o nuevo riesgo introducido por las medidas de mitigación.

Desarrollo de planes de implementación
Cada estrategia seleccionada debe ser traducida en un plan de implementación detallado, que incluya:

Acciones específicas
Pasos concretos necesarios para implementar la estrategia.

Recursos requeridos
Identificación de los recursos necesarios, incluyendo personal, tecnología y recursos financieros.

Cronograma
Un calendario para la implementación, con hitos claros.

Responsables
Asignación de responsabilidades específicas para cada acción.

Planes de contingencia
Además de las estrategias de mitigación, desarrollar planes de contingencia para cada riesgo, en caso de que las medidas de mitigación no sean efectivas.

Monitoreo y revisión
Incluir mecanismos para el monitoreo continuo del riesgo y la efectividad de las estrategias de mitigación, con revisiones periódicas para ajustar el enfoque según sea necesario.

Comunicación y formación
Asegurar que todos los implicados estén informados sobre las estrategias de mitigación y cualquier cambio en los procedimientos. Esto puede requerir sesiones de formación específicas.

El desarrollo de estrategias de mitigación efectivas es un componente esencial de la gestión de riesgos tecnológicos, asegurando que la institución pueda anticiparse a los riesgos potenciales y responder de manera efectiva para minimizar su impacto.

9.3.2. Planes de respuesta a incidentes

Los planes de respuesta a incidentes son fundamentales para la gestión eficaz de incidentes tecnológicos, proporcionando un marco de acción rápido y organizado para minimizar el impacto y restaurar la operatividad lo antes posible. A continuación, se detalla cómo se pueden desarrollar estos planes:

9.3.2.1. Preparación

Equipo de respuesta a incidentes

Establecer un equipo dedicado con roles y responsabilidades claros, incluyendo expertos en TI, seguridad de la información, legal, comunicaciones y operaciones.

Herramientas y recursos

Asegurar que el equipo tenga acceso a las herramientas de detección, análisis y mitigación necesarias, así como a la información de contacto actualizada y recursos de apoyo.

9.3.2.2. Identificación del incidente

Canales de reporte

Definir métodos claros y accesibles para la notificación de incidentes, tanto internamente entre funcionarios/as y colaboradores como externamente para otros organismos relacionados o ciudadanía.

Procedimientos de detección

Implementar sistemas de monitoreo y detección de intrusiones para identificar actividades sospechosas o anómalas rápidamente.

9.3.2.3. Evaluación del incidente

Clasificación y priorización

Desarrollar criterios para clasificar los incidentes según su severidad y urgencia, lo que ayuda a determinar el nivel de respuesta requerido.

Asignación de recursos

Basado en la clasificación, asignar recursos y personal adecuados para abordar el incidente.

9.3.2.4. Contención

Estrategias de contención inmediata

Implementar medidas para limitar la propagación del incidente y prevenir daños adicionales, lo que puede incluir aislar sistemas afectados o desactivar ciertas funciones.

Análisis forense preliminar

Recopilar información crítica sobre el incidente para la investigación y respuesta subsiguiente, asegurando la preservación de evidencias.

9.3.2.5. Erradicación y recuperación

Eliminación de la causa raíz

Identificar y eliminar las vulnerabilidades o amenazas que permitieron el incidente, incluyendo la aplicación de parches de seguridad o la actualización de políticas.

Restauración de sistemas

Procedimientos para la limpieza y restauración segura de sistemas y servicios afectados a su estado operativo normal.

9.3.2.6. Comunicación

Plan de comunicaciones

Establecer protocolos para la comunicación interna y externa durante y después de un incidente, incluyendo qué información se compartirá, cómo y cuándo.

Notificación a partes afectadas

Incluir procedimientos para notificar a funcionarios/as, colaboradores, autoridades y si es necesario, a autoridades reguladoras u organismos de seguridad.

9.3.2.7. Análisis Post-Incidente

Revisión y análisis

Una vez controlado el incidente, realizar una revisión exhaustiva para identificar las causas, el impacto, la efectividad de la respuesta y las lecciones aprendidas.

Informe Post-Incidente

Documentar el incidente, la respuesta, los resultados del análisis y las recomendaciones para mejorar la respuesta futura y las medidas de prevención.

9.3.2.8. Mejora Continua

Actualización de planes y políticas

Utilizar las lecciones aprendidas para actualizar los planes de respuesta a incidentes, políticas de seguridad y prácticas de formación.

Capacitación y simulacros

Realizar regularmente capacitaciones y simulacros de incidentes para preparar al equipo de respuesta y probar la efectividad de los planes.

El desarrollo de planes de respuesta a incidentes detallados y la preparación continua son esenciales para la resiliencia organizativa frente a incidentes tecnológicos. Al seguir estos pasos, las instituciones pueden asegurar una respuesta coordinada y efectiva que minimice el impacto de los incidentes y acelere la recuperación.

9.4. Implementación y Ejecución

9.4.1. Asignación de roles y responsabilidades

La asignación clara de roles y responsabilidades es fundamental para la implementación y supervisión efectivas de cualquier plan de gestión de riesgos tecnológicos. Garantiza que cada aspecto del plan sea ejecutado por personal calificado y que exista una estructura de rendición de cuentas. A continuación, se detallan cómo asignar, definir estos roles y responsabilidades:

9.4.1.1. Comité de gestión de riesgos

Función	Responsabilidades
Supervisar el desarrollo, implementación y revisión periódica del plan de gestión de riesgos tecnológicos	Definir la política de gestión de riesgos, establecer objetivos y aprobar el plan. Además, revisar y aprobar las modificaciones basadas en el análisis de riesgos y las lecciones aprendidas de incidentes anteriores

9.4.1.2. Oficial de Seguridad de la Información (CISO)

Función	Responsabilidades
Liderar la estrategia de seguridad de la información y la gestión de riesgos tecnológicos	Coordinar la evaluación de riesgos, desarrollar estrategias de mitigación y asegurar la implementación de controles de seguridad adecuados. Actúa como enlace entre el comité de gestión de riesgos y los equipos operativos

9.4.1.3. Gestor de riesgos tecnológicos

Función	Responsabilidades
Administrar el día a día del plan de gestión de riesgos tecnológicos	Identificar y evaluar riesgos, coordinar actividades de mitigación y respuesta y mantener el registro de riesgos. Asegurar la comunicación efectiva de los riesgos y las acciones a todas las partes relevantes

9.4.1.4. Equipo de respuesta a incidentes

Función	Responsabilidades
Responder a incidentes de seguridad de manera eficaz y eficiente	Implementar los procedimientos de respuesta a incidentes, realizar el análisis forense, aplicar medidas de contención y liderar la recuperación tras un incidente. Este equipo también participa en la revisión post-incidente para identificar lecciones aprendidas

9.4.1.5. Área de Gestión de Tecnologías de la Información

Función	Responsabilidades
Apoyar la implementación de las medidas de seguridad tecnológica y las estrategias de mitigación	Mantenimiento de la infraestructura de TI, aplicación de parches de seguridad, gestión de configuraciones, soporte en la recuperación de desastres y continuidad del negocio

9.4.1.6. Área legal y de cumplimiento

Función	Responsabilidades
Asegurar que el plan de gestión de riesgos y las respuestas a incidentes cumplan con las leyes, regulaciones y estándares de la industria	Asesorar sobre temas legales y de cumplimiento, participar en la revisión de contratos y acuerdos con terceros, liderar la comunicación con reguladores y otras partes externas en caso de incidentes

9.4.1.7. Funcionarios, colaboradores y usuarios finales

Función	Responsabilidades
Participar activamente en la seguridad y gestión de riesgos tecnológicos.	Seguir las políticas y procedimientos de seguridad, reportar actividades sospechosas o incidentes,

	participar en programas de formación y concientización.

9.4.1.8. Otros roles específicos

Dependiendo de la estructura y las necesidades de la institución, se pueden designar roles adicionales, como un analista de riesgos, un oficial de protección de datos (DPO) o un coordinador de continuidad del negocio.

9.4.1.9. Establecimiento de procedimientos de comunicación

Es crucial establecer procedimientos de comunicación claros entre estos roles, asegurando que la información sobre riesgos, incidentes y estrategias de mitigación fluya de manera eficiente a través de la institución. Esto incluye comunicaciones regulares, informes de estado, y revisiones de incidentes.

La asignación detallada de roles y responsabilidades, junto con la comunicación efectiva, es clave para asegurar una gestión de riesgos tecnológicos proactiva y resiliente.

9.4.2. Programación e hitos

La definición de una programación y el establecimiento de hitos claros son esenciales para la implementación y supervisión eficaces de cualquier plan de gestión de riesgos tecnológicos. Estos elementos proporcionan un marco temporal que facilita la planificación, el seguimiento del progreso y la evaluación de la eficacia de las acciones emprendidas. A continuación, se detalla cómo desarrollar esta programación y definir los hitos:

9.4.2.1. Desglose del plan en fases

Dividir el plan de gestión de riesgos tecnológicos en fases manejables, cada una con objetivos específicos:

Fase	Actividades
1	Preparación y planificación. Incluye actividades como la formación del equipo de gestión de riesgos, la definición de roles y responsabilidades, y el establecimiento del marco de gestión de riesgos.
2	Identificación y evaluación de riesgos. Implica la realización de un análisis de riesgos y la creación del registro de riesgos.
3	Desarrollo de estrategias de mitigación y respuesta. Se centra en formular y planificar la implementación de medidas de mitigación y planes de respuesta a incidentes.

4	Implementación y ejecución. Involucra la puesta en marcha de controles de seguridad, medidas de mitigación y la realización de simulacros de respuesta a incidentes.
5	Monitoreo, revisión y mejora continua. Dedicada a la supervisión del plan, la evaluación de su efectividad y la realización de ajustes necesarios.

9.4.2.2. Establecimiento de hitos

Para cada fase, definir hitos claros que representen logros clave dentro del plan. Los hitos pueden incluir:

- Compleción de la evaluación de riesgos.
- Finalización del desarrollo de estrategias de mitigación.
- Implementación de un sistema de gestión de incidentes.
- Realización de un simulacro de respuesta a incidentes.
- Revisión anual del plan de gestión de riesgos.

9.4.2.3. Asignación de tiempos y fechas

Asignar una línea de tiempo a cada fase e hito, incluyendo fechas de inicio y finalización esperadas. Esto proporciona una estructura temporal para la implementación del plan y facilita la asignación de recursos.

9.4.2.4. Herramientas de programación

Utilizar herramientas de gestión de proyectos, como diagramas de Gantt o software especializado, para visualizar la programación y realizar un seguimiento del progreso hacia los hitos.

9.4.2.5. Flexibilidad y ajustes

Mantener cierta flexibilidad en la programación para adaptarse a cambios imprevistos o lecciones aprendidas durante la implementación del plan. Establecer procedimientos para revisar y ajustar la programación y los hitos según sea necesario.

9.4.2.6. Revisión de avances

Programar revisiones regulares para evaluar el progreso hacia los hitos y la eficacia general del plan. Estas revisiones deben incluir la actualización del registro de riesgos, la evaluación de la efectividad de las medidas de mitigación y la identificación de nuevas áreas de riesgo.

9.4.2.7. Comunicación de la programación

Compartir la programación y los hitos con todas las partes interesadas relevantes, incluidos miembros del equipo de gestión de riesgos, la dirección ejecutiva y los departamentos afectados, para asegurar la alineación y el compromiso con el plan.

9.4.2.8. Documentación y registro

Documentar detalladamente la programación, los hitos alcanzados y los resultados de las revisiones de avance. Esto no solo proporciona un registro histórico del proceso de gestión de riesgos, sino que también es esencial para las auditorías internas y externas.

La programación cuidadosa y el establecimiento de hitos son componentes críticos para la gestión exitosa de riesgos tecnológicos, proporcionando un camino claro hacia la mitigación efectiva de riesgos y la mejora continua de las prácticas de seguridad de la información.

9.5. Capacitación y concientización

9.5.1. Programas de Capacitación

Los programas de capacitación son esenciales para asegurar que todos los/las funcionarios/as y/o colaboradores entiendan su papel en la protección de los activos tecnológicos de la institución y cómo sus acciones pueden influir en la seguridad general. Una estrategia de capacitación efectiva incluye varias componentes clave para maximizar el aprendizaje y la retención de conocimiento. A continuación, se proporcionan detalles sobre cómo implementar sesiones regulares de capacitación sobre prácticas de seguridad tecnológica:

9.5.1.1. Evaluación de necesidades de capacitación

Identificar brechas de conocimiento

Realizar una evaluación inicial para identificar las brechas de conocimiento específicas entre diferentes grupos de funcionarios/as y colaboradores. Esto puede incluir comprensión de políticas de seguridad, uso seguro de dispositivos, aplicaciones y conciencia de amenazas comunes como el phishing.

Personalización del contenido

Desarrollar contenidos de capacitación que se alineen con las necesidades específicas de la institución y los roles de los/las funcionarios/as y colaboradores.

9.5.1.2. Diseño del programa de capacitación

Contenidos relevantes y actualizados

Asegurar que el material de capacitación cubra las últimas amenazas de seguridad, mejores prácticas y políticas de la institución.

Métodos de enseñanza variados

Incorporar una variedad de métodos de enseñanza, incluidos seminarios web, tutoriales en línea, sesiones presenciales y estudios de caso para adaptarse a diferentes estilos de aprendizaje.

Participación activa

Fomentar la participación activa a través de ejercicios prácticos, juegos de roles y simulaciones de ataques de phishing, entre otros.

9.5.1.3. Programación regular y repetición

Sesiones regulares

Establecer un calendario regular para la capacitación en seguridad tecnológica, asegurando que todos los/las funcionarios/as y colaboradores reciban formación continua y actualizaciones sobre las últimas tendencias y amenazas.

Reciclaje

Incluir sesiones de reciclaje para mantener frescos los conocimientos y habilidades, especialmente en áreas críticas de seguridad.

9.5.1.4. Evaluación y mejora

Evaluaciones previas y posteriores

Realizar evaluaciones antes y después de las sesiones de capacitación para medir el aumento de conocimiento y habilidades.

Feedback de los participantes

Recoger feedback de los/las funcionarios/ar y colaboradores sobre la relevancia, efectividad y áreas de mejora del programa de capacitación.

Ajustes Basados en Resultados

Utilizar los resultados de las evaluaciones y el feedback para hacer ajustes continuos en el programa de capacitación.

9.5.1.5. Certificación y reconocimiento

Certificación

Ofrecer certificaciones o insignias digitales a los/las funcionarios/as y colaboradores que completen satisfactoriamente los programas de capacitación, como un incentivo para su participación.

Reconocimiento

Reconocer y recompensar a los/las funcionarios/as y colaboradores o departamentos que muestren un compromiso excepcional con la seguridad tecnológica.

9.5.1.6. Integración con la inducción de nuevos/as funcionarios/as y colaboradores

Capacitación para nuevos ingresos

Incluir sesiones de seguridad tecnológica como parte del programa de inducción para todos los nuevos/as funcionarios/as y colaboradores, asegurando que comprendan las políticas y expectativas de seguridad desde el primer día.

9.5.1.7. Comunicación continua

Actualizaciones y alertas

Complementar la capacitación formal con comunicaciones regulares, como boletines informativos, alertas de seguridad y actualizaciones rápidas sobre nuevas amenazas o incidentes de seguridad relevantes.

Implementando un programa de capacitación en seguridad tecnológica bien estructurado y regular, la institución puede fortalecer significativamente su postura de seguridad al asegurar que todos los/las funcionarios/as y colaboradores estén informados, capacitados y preparados para actuar de manera segura en el entorno digital.

9.5.2. Iniciativas de Concientización

Las iniciativas de concientización son cruciales para fomentar una cultura de seguridad en toda la institución, haciendo que los/las funcionarios/as y colaboradores no solo estén informados sobre los riesgos y políticas de seguridad, sino también activamente comprometidos en mantener la seguridad tecnológica. Aquí detallamos cómo se pueden desarrollar y ejecutar estas campañas internas:

9.5.2.1. Identificación de temas clave

Evaluación de riesgos

Identificar los principales riesgos de seguridad tecnológica específicos para la institución y los temas que requieren mayor concientización.

Tendencias de seguridad

Incluir información sobre las últimas tendencias en amenazas cibernéticas, ataques recientes relevantes a nivel mundial o del sector y lecciones aprendidas.

9.5.2.2. Diseño de la campaña

Mensajes claros y concisos

Crear mensajes clave que sean fáciles de entender y recordar. Estos deben destacar la importancia de la seguridad tecnológica y el papel de cada funcionario/a o colaborador/a en su mantenimiento.

Variedad de formatos

Utilizar diversos formatos para captar la atención y adaptarse a diferentes preferencias de aprendizaje, incluyendo videos, infografías, carteles y publicaciones en intranet.

9.5.2.3. Programación y difusión

Planificación temporal

Distribuir las iniciativas de concientización a lo largo del año para mantener el tema presente sin saturar a los/las funcionarios/as y colaboradores.

Canales de comunicación

Aprovechar todos los canales de comunicación interna disponibles, como correo electrónico, intranet, reuniones de equipo y redes sociales corporativas, para maximizar el alcance.

9.5.2.4. Interactividad y participación

Actividades participativas

Organizar eventos y actividades que promuevan la participación, como concursos de seguridad, simulacros de phishing y juegos educativos.

Espacios de diálogo

Fomentar la creación de espacios, físicos o virtuales, donde los/las funcionarios/as y colaboradores puedan expresar dudas, compartir experiencias y discutir abiertamente sobre seguridad tecnológica.

9.5.2.5. Integración con otros programas

Capacitación y desarrollo

Vincular las iniciativas de concienciación con los programas de capacitación existentes para reforzar los mensajes de seguridad y fomentar un aprendizaje continuo.

Reconocimiento y recompensas

Implementar un sistema de recompensas para los/las funcionarios/as y colaboradores que demuestren un compromiso excepcional con la seguridad tecnológica, incentivando la participación activa.

9.5.2.6. Evaluación y retroalimentación

Medición del impacto

Utilizar encuestas, evaluaciones de conocimiento y análisis de incidentes para medir el impacto de las campañas de concienciación en el comportamiento y la cultura de seguridad.

Retroalimentación de los/las funcionarios/as y colaboradores

Recoger y analizar la retroalimentación para entender la eficacia de los diferentes componentes de la campaña y áreas de mejora.

9.5.2.7. Actualización y mejora continua

Iteración basada en resultados

Ajustar y mejorar continuamente las iniciativas de concienciación basándose en los resultados de las evaluaciones y la retroalimentación recibida.

Adaptación a nuevos riesgos

Actualizar regularmente los contenidos de las campañas para reflejar los cambios en el panorama de amenazas y las nuevas prioridades de seguridad.

Las iniciativas de concienciación bien diseñadas y ejecutadas pueden transformar significativamente la cultura de seguridad de una institución, creando un entorno donde la seguridad tecnológica es una responsabilidad compartida y una práctica cotidiana entre todos los/las funcionarios/as y colaboradores.

9.6. Monitoreo, revisión y actualización

9.6.1. Monitoreo Continuo

El monitoreo continuo de los riesgos tecnológicos es esencial para detectar y responder a amenazas emergentes en tiempo real, permitiendo a las instituciones adaptarse y mitigar riesgos antes de que se materialicen en incidentes. Aquí se detalla cómo establecer un sistema eficaz de monitoreo constante:

9.6.1.1. Definición de parámetros de monitoreo

Identificar indicadores clave de riesgo (KRI)

Desarrollar un conjunto de indicadores que puedan señalar un aumento en el riesgo o la inminencia de un incidente. Esto puede incluir patrones anómalos de tráfico de red, intentos de acceso no autorizado, y tasas de fallos de sistema.

Establecer límites de tolerancia

Para cada KRI, definir umbrales que, si se superan, indicarán la necesidad de una revisión o acción inmediata.

9.6.1.2. Implementación de herramientas de monitoreo

Software de monitoreo de seguridad

Implementar soluciones avanzadas de software, como sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS) y herramientas de gestión de eventos e información de seguridad (SIEM), para automatizar la recolección y análisis de datos de seguridad.

Auditorías y evaluaciones de vulnerabilidad regulares

Complementar el monitoreo en tiempo real con auditorías de seguridad y evaluaciones de vulnerabilidad periódicas para identificar y remediar proactivamente debilidades en la infraestructura tecnológica.

9.6.1.3. Integración de fuentes de datos

Consolidación de datos

Integrar datos de diversas fuentes, incluidos logs de sistemas, datos de tráfico de red y reportes de seguridad de aplicaciones, para obtener una visión holística del entorno de seguridad.

Análisis de datos en tiempo real

Utilizar técnicas avanzadas de análisis, como el aprendizaje automático y la inteligencia artificial, para analizar datos en tiempo real, detectar patrones anómalos y predecir posibles incidentes.

9.6.1.4. Establecimiento de procedimientos de respuesta

Protocolos de escalamiento

Definir claramente cómo y cuándo los hallazgos del monitoreo deben ser escalados a diferentes niveles dentro de la institución, desde equipos técnicos hasta autoridades.

Planes de respuesta a incidentes

Asegurar que existan planes de respuesta específicos para diferentes tipos de incidentes detectados a través del monitoreo.

9.6.1.5. Capacitación y concientización del equipo

Formación continua

Capacitar regularmente al personal de TI y seguridad en el uso de herramientas de monitoreo y análisis de datos, así como en procedimientos de respuesta a incidentes.

Concienciación sobre la importancia del monitoreo

Fomentar una cultura organizacional que valore el monitoreo continuo como un componente crítico de la gestión de riesgos tecnológicos.

9.6.1.6. Revisión y mejora continua

Evaluación periódica del sistema de monitoreo

Revisar y ajustar regularmente el sistema de monitoreo para garantizar su efectividad y adaptarlo a las cambiantes dinámicas de riesgo y tecnología.

Incorporación de nuevas tecnologías

Estar al tanto de los avances en tecnologías de monitoreo y análisis para mejorar continuamente las capacidades de detección y respuesta.

9.6.1.7. Reporte y análisis de tendencias

Reportes de monitoreo

Generar reportes periódicos que resuman las actividades de monitoreo, incluyendo incidentes detectados, respuestas implementadas y lecciones aprendidas.

Análisis de tendencias

Utilizar los datos recopilados para identificar tendencias emergentes en riesgos tecnológicos y adaptar las estrategias de mitigación según sea necesario.

Estableciendo un sistema de monitoreo continuo robusto y dinámico, las instituciones pueden mantenerse un paso adelante en la identificación y gestión de riesgos tecnológicos, asegurando la protección de sus activos y la continuidad de sus operaciones.

9.6.2. Revisión periódica del plan

La revisión periódica del plan de gestión de riesgo tecnológico es esencial para asegurar su relevancia y efectividad continuas frente a un panorama de amenazas en constante evolución y cambios en el entorno operativo de la institución. A continuación, se detalla cómo realizar estas revisiones de manera sistemática:

9.6.2.1. Establecimiento de un cronograma de revisión

Revisión anual programada

Programar revisiones regulares del plan al menos una vez al año. Este cronograma debe ser documentado y comunicado a todas las partes interesadas relevantes.

Revisiones adicionales desencadenadas por eventos

Establecer criterios claros para revisiones adicionales desencadenadas por eventos específicos, como incidentes de seguridad significativos, cambios importantes en la infraestructura tecnológica, nuevas legislaciones o normativas, o reestructuraciones de la institución.

9.6.2.2. Convocatoria de un equipo de revisión multidisciplinario

Equipo multidisciplinario

Incluir en el equipo de revisión a representantes de varios departamentos, como TI, seguridad de la información, operaciones, legal y recursos humanos, para asegurar una perspectiva integral.

Participación de autoridades

Involucrar a autoridades para reforzar la importancia estratégica de la gestión de riesgos tecnológicos y asegurar el alineamiento con los objetivos de negocio.

9.6.2.3. Evaluación de la efectividad del plan

Análisis de incidentes

Revisar cómo el plan manejó incidentes recientes, evaluando la efectividad de las respuestas y la recuperación.

Comparación con mejores prácticas

Evaluar el plan en comparación con las mejores prácticas y estándares líderes en la industria, considerando las directrices establecidas por entidades reconocidas como el NIST, ISO y CIS Controls, así como los marcos de ITIL y COBIT.

Feedback de las partes interesadas

Recopilar y analizar el feedback de los/las funcionarios/as, colaboradores y otras partes interesadas sobre la claridad, accesibilidad y efectividad del plan.

9.6.2.4. Identificación de áreas de mejora

Brechas y oportunidades

Identificar brechas en la cobertura del plan, así como oportunidades para mejorar la prevención, detección y respuesta a riesgos tecnológicos.

Adaptación a cambios tecnológicos

Considerar los impactos de nuevas tecnologías, tanto en términos de nuevas oportunidades de mitigación como de nuevos riesgos emergentes.

9.6.2.5. Actualización del plan

Incorporación de cambios

Realizar los ajustes necesarios en el plan para abordar las áreas de mejora identificadas, incluyendo la actualización de políticas, procedimientos y estrategias de mitigación.

Documentación de cambios

Registrar todos los cambios realizados en el plan, incluyendo las razones detrás de cada ajuste y la fecha de implementación.

9.6.2.6. Pruebas y validación

Simulacros y pruebas

Llevar a cabo pruebas o simulacros para validar la eficacia de los cambios realizados en el plan.

Evaluación de la capacitación y concientización

Verificar que las iniciativas de capacitación y concientización sean actualizadas para reflejar los cambios en el plan.

9..6.2.7. Comunicación y difusión

Comunicación de cambios

Informar a todas las partes interesadas, internas y externas, sobre los cambios realizados en el plan, asegurando que entienden su papel dentro del marco actualizado.

Capacitación sobre las actualizaciones

Proveer capacitación o sesiones informativas para asegurar que todos los implicados estén al tanto de las nuevas políticas y procedimientos.

9.6.2.8. Documentación y archivo

Archivo de versiones

Mantener un registro de todas las versiones del plan, incluyendo un historial de cambios, para rastrear la evolución del enfoque de gestión de riesgos de la institución.

Revisión de documentación de soporte

Asegurar que toda documentación relacionada, como guías de procedimientos y listas de contacto, sea revisada y actualizada conforme al plan revisado.

La revisión periódica del plan de gestión de riesgos tecnológicos asegura que la institución pueda adaptarse continuamente a nuevos desafíos y mantener una postura

9.7. Comunicación y reporte

9.7.1. Estrategias de comunicación

Las estrategias de comunicación efectivas son cruciales para manejar la respuesta a incidentes de seguridad, minimizando el impacto en la confianza de los stakeholders y en la operatividad de la institución. El desarrollo de un protocolo de comunicación requiere considerar tanto la comunicación interna como externa, asegurando transparencia y eficiencia. A continuación, se detallan aspectos clave para su desarrollo:

9.7.1.1. Definición de roles y responsabilidades

Portavoz oficial

Designar portavoces oficiales tanto para la comunicación interna como externa, generalmente incluyendo al CISO para asuntos técnicos y autoridades para comunicaciones a nivel de institución.

Equipo de comunicación de crisis

Establecer un equipo dedicado que incluya miembros de TI, seguridad, comunicaciones, prensa, legal y recursos humanos, encargados de formular y distribuir mensajes durante un incidente.

Identificación de audiencias clave

Internas	Externas
Funcionarios, colaboradores y autoridades	Organismos gubernamentales, reguladores, medios de comunicación y el público en general

9.7.1.2. Desarrollo de mensajes clave

Adaptados a la audiencia

Crear mensajes específicos para cada audiencia, asegurando que sean relevantes y comprensibles para el grupo destinatario.

Claros y concisos

Los mensajes deben ser claros, evitando jerga técnica innecesaria, proporcionar una visión general del incidente, las acciones tomadas y los pasos siguientes.

Canales de comunicación

Internos	Externos
Utilizar la intranet, correos electrónicos, reuniones informativas y sistemas de mensajería instantánea	Preparar comunicados de prensa, actualizaciones en el sitio web, redes sociales y, si es necesario, conferencias de prensa

9.7.1.3. Protocolo de comunicación

Antes del incidente

Desarrollar plantillas de comunicación y escenarios simulados para agilizar la respuesta en caso de incidente real.

Durante el incidente

Seguir un protocolo establecido para la recopilación y verificación de información antes de la difusión. Mantener una comunicación regular con actualizaciones sobre el progreso de la respuesta al incidente.

Después del incidente

Comunicar la resolución del incidente, las lecciones aprendidas y las medidas tomadas para prevenir futuros incidentes. Asegurar una revisión del manejo de la comunicación durante el incidente para identificar áreas de mejora.

9.7.2. Cumplimiento legal y regulatorio

Revisión legal

Todas las comunicaciones deben ser revisadas por el departamento legal para asegurar el cumplimiento con las obligaciones legales y regulatorias, incluyendo las leyes de notificación de brechas de seguridad.

9.7.3. Entrenamiento y simulacros

Capacitación del portavoz y el equipo de comunicación

Realizar entrenamientos regulares y simulacros de crisis para preparar al equipo de comunicación en el manejo efectivo de la comunicación durante incidentes de seguridad.

Feedback y mejora continua

Recopilar feedback después de cada simulacro o incidente real para mejorar continuamente las estrategias de comunicación.

9.7.4. Monitorización y gestión de la reputación

Monitoreo de medios

Implementar herramientas de monitorización de medios y redes sociales para rastrear la percepción pública y responder adecuadamente a la información errónea o preocupaciones expresadas por las audiencias externas.

Desarrollar e implementar estrategias de comunicación detalladas y efectivas permite a la institución manejar incidentes de seguridad con transparencia y eficacia, manteniendo la confianza de los stakeholders y minimizando el impacto negativo en la reputación de la institución.

9.8. Reportes de gestión

Los reportes de gestión son herramientas clave para comunicar el estado de los riesgos tecnológicos a autoridades, permitiéndoles tomar decisiones informadas basadas en la evaluación actualizada de riesgos y la efectividad de las medidas de mitigación implementadas. Aquí se detalla cómo elaborar y presentar estos informes de manera efectiva:

9.8.1. Periodicidad de los informes

Definir la frecuencia

Establecer un calendario regular para la presentación de informes, que puede variar según el nivel de riesgo, los cambios en el entorno tecnológico y las preferencias de la dirección. Esto puede ser mensual, trimestral o semestral.

9.8.2. Estructura y contenido del informe

Resumen ejecutivo

Incluir un resumen ejecutivo al inicio del informe que destaque los puntos más importantes, incluidas las principales conclusiones y recomendaciones.

Estado actual de riesgos

Describir el panorama actual de riesgos tecnológicos, incluyendo cualquier cambio significativo desde el último informe.

Evaluación de riesgos

Presentar una evaluación detallada de los riesgos identificados, incluyendo su probabilidad, impacto y la clasificación de riesgos (alta, media, baja).

Efectividad de las medidas de mitigación

Analizar la efectividad de las estrategias y medidas de mitigación implementadas, destacando éxitos y áreas de mejora.

Incidentes de seguridad

Reportar cualquier incidente de seguridad ocurrido, las respuestas implementadas y las lecciones aprendidas.

Indicadores clave de rendimiento (KPIs)

Incluir KPIs que midan la efectividad de la gestión de riesgos tecnológicos y la seguridad de la información.

Recomendaciones y acciones futuras

Proporcionar recomendaciones claras para la mejora continua de la gestión de riesgos tecnológicos, incluyendo acciones específicas y plazos.

9.8.3. Visualización de datos

Gráficos y tablas

Utilizar gráficos, tablas y otros elementos visuales para presentar la información de manera clara y concisa, facilitando la comprensión de los datos complejos.

Mapas de calor de riesgos

Incluir mapas de calor para visualizar la clasificación y priorización de los riesgos, mostrando la relación entre la probabilidad y el impacto.

9.8.4. Personalización para la audiencia

Alineación con intereses estratégicos

Asegurar que el informe esté alineado con los intereses estratégicos y preocupaciones de autoridades destacando cómo los riesgos tecnológicos pueden afectar los objetivos globales de la institución.

Lenguaje accesible

Evitar el uso excesivo de jerga técnica, presentando la información en un lenguaje claro y accesible para los no especialistas.

9.8.5. Proceso de revisión

Revisión preliminar

Antes de la presentación, realizar una revisión preliminar del informe con los equipos de TI y seguridad para validar la precisión de la información y las recomendaciones.

Feedback Post-Presentación

Recoger feedback de autoridades tras la presentación para mejorar futuros informes.

9.8.6. Seguimiento de acciones

Registro de acciones

Mantener un registro de las acciones recomendadas y su estado de implementación para seguimiento en futuros informes.

Elaborar reportes de gestión detallados y orientados a la acción es esencial para comunicar eficazmente el estado de los riesgos tecnológicos y facilitar una gestión proactiva de riesgos en la institución. Estos informes no solo informan a autoridades sobre el estado actual, sino que también impulsan la toma de decisiones estratégicas para la mejora continua de la seguridad y la gestión de riesgos.

10. Programación Anual

A continuación, se presenta una programación anual detallada con descripciones de las actividades clave del Plan de Riesgo Tecnológico:

Evaluación de Riesgos		
Enero	Semana 1-2	**Revisión de activos** Identificar y documentar todos los activos de tecnología de la información, incluyendo hardware, software y datos.
	Semana 3-4	**Identificación de amenazas y vulnerabilidades** Realizar análisis de amenazas y vulnerabilidades, consultando fuentes de amenazas y evaluando la exposición.
Febrero	Semana 1-4	**Evaluación de riesgos** Evaluar riesgos en función de la probabilidad e impacto, y asignar prioridades.

Estrategias de mitigación		
Marzo	Semana 1-4	**Planificación de mitigación** Desarrollar planes detallados para abordar los riesgos críticos identificados.

Implementación de controles		
Abril	Semana 1-4	Implementar controles de seguridad, incluyendo cortafuegos, sistemas de detección de intrusiones y actualizaciones de software.

Capacitación y concientización		
Mayo	Semana 1-4	**Campaña de concientización** Iniciar una campaña de concientización en seguridad cibernética para todo el personal.
Junio	Semana 1-4	**Capacitación especializada** Proporcionar capacitación especializada en detección de phishing y buenas prácticas de seguridad.

Plan de respuesta a incidentes		
Julio	Semana 1-4	**Establecimiento del equipo CSIRT** Formalizar el equipo de respuesta a incidentes (CSIRT).
Agosto	Semana 1-4	**Documentación y simulacros** Documentar procedimientos de respuesta a incidentes. Realizar el primer ejercicio de simulacro de respuesta a incidentes.

Monitoreo y detección		
Septiembre	Semana 1-4	**Implementación de herramientas** Implementar herramientas de monitoreo continuo de seguridad.
Octubre	Semana 1-4	**Configuración de alertas** Configurar alertas para detectar actividad sospechosa en la red y sistemas.

Pruebas y evaluaciones		
Noviembre:	Semana 1-4	**Pruebas de penetración** Realizar pruebas de penetración programadas para identificar vulnerabilidades.
Diciembre	Semana 1-4	**Auditorías de seguridad** Llevar a cabo auditorías de seguridad internas y externas.

Anexos

Documentación detallada

Incluir listados de activos, políticas de seguridad, procedimientos de respuesta a incidentes y otros documentos relevantes.

Pasos adicionales

Evaluación de cumplimiento legal

Asegurar que el plan esté en conformidad con las leyes y regulaciones aplicables.

Simulacros de respuesta a incidentes

Organizar simulacros periódicos para probar la eficacia de los planes de respuesta.

Integración con planes generales de la institución

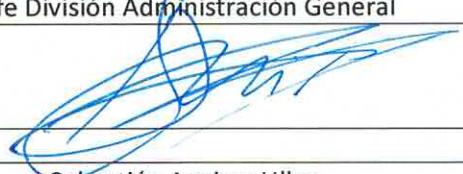
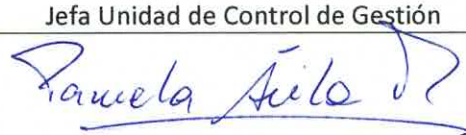
Coordinar con otros planes de gestión de riesgos y continuidad del negocio para asegurar una cobertura integral.

11. Control

Elaborado por: Jorge Romero Vargas

Fecha: 22-03-2024

Comité de Seguridad de la Información, Ministerio Secretaría General de la Presidencia

Samir Toro Garrido Jefe División Administración General	Pamela Ávila Rubio Jefa Unidad de Control de Gestión
	
Sebastián Aguirre Ulloa Asesor División Jurídico-Legislativa	Christian Valenzuela Lorca Jefe Gabinete de la Subsecretaria
	
Fabiola Vidal Oyarzún Asesor Comisión de Integridad y Transparencia	
	

Jorge Romero Vargas Oficial de Seguridad de la Información Encargado de Ciberseguridad

Fecha: 22-03-2024