

Bachillerato en ingeniería en Sistemas

Administración y Control de Proyectos de Sistemas

Caso Hipotético De Riesgos En El Proyecto

Estudiantes:

Oscar Mauricio Delgado Guadamuz

Sergio Gamboa Gamboa

Leyner Fabián Mora Mora

Francela Ortiz Vargas

Harold Castillo Delgado

Profesor:

Fauricio Conejo Navarro

San José

Primer Cuatrimestre

2023

**Caso De Riesgo 1:**

**Riesgo:** Caída de los enlaces de comunicación

**Impacto:** Alto.

* |22

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  |  | **34** |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Mantener enlaces con otros proveedores.
* Implementar métodos de contingencia en caso de fallo

**Plan Remedial Hipotético:**

* Comunicarse con la compañía para el apoyo necesario
* Realizar una revisión y verificación de los enlaces segundarios.

**Posibles Gastos para la Remediación:**

* Normalmente las caídas de enlaces están cubiertas por el proveedor que nos brinda estos servicios.

**Tiempo y Recursos necesarios para la Remediación:**

* Acompañamiento a los proveedores durante la revisión: 8 horas, 1 administrador de redes
* Pruebas adicionales: 3 días, 1 técnico de soporte de TI.

**Caso De Riesgo 2:**

**Riesgo:** La falta de disponibilidad del servidor puede causar una interrupción en el servicio y la pérdida de datos críticos.

**Impacto:** Alto.

* Pérdida de datos críticos del usuario y del sistema.
* Interrupción del servicio y la satisfacción del cliente.
* Aumento de los costos debido a la necesidad de recuperar datos y restaurar el servicio.

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  |  | **34** |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Realizar copias de seguridad periódicas de los datos del servidor.
* Implementar redundancia de hardware y software para garantizar la disponibilidad del servidor.
* Establecer políticas de seguridad de la información para proteger los datos críticos del usuario y del sistema.
* Realizar pruebas de contingencia para garantizar la capacidad de recuperación del sistema.

**Plan Remedial Hipotético:**

* Restaurar los datos del servidor a partir de la copia de seguridad más reciente.
* Reemplazar cualquier hardware defectuoso y realizar reparaciones para garantizar la disponibilidad del servidor.
* Realizar una revisión de la política de seguridad de la información y mejorar la seguridad del sistema según sea necesario.
* Realizar pruebas adicionales para asegurarse de que el sistema esté completamente recuperado y sea capaz de proporcionar un servicio estable.

**Posibles Gastos para la Remediación:**

* Costo de reemplazar hardware defectuoso y realizar reparaciones: $5,000
* Costo de restaurar datos a partir de la copia de seguridad más reciente: $2,500
* Costo de realizar una revisión de la política de seguridad de la información y mejorar la seguridad del sistema: $3,000
* Costo de realizar pruebas adicionales para asegurarse de que el sistema esté completamente recuperado: $1,500

**Tiempo y Recursos necesarios para la Remediación:**

* Reemplazo de hardware y reparaciones: 1 semana, 2 técnicos de soporte de TI
* Restauración de datos: 2 días, 1 técnico de soporte de TI
* Revisión de la política de seguridad de la información y mejoras: 2 semanas, 1 consultor de seguridad de TI
* Pruebas adicionales: 3 días, 1 técnico de soporte de TI.

**Caso De Riesgo 3:**

**Riesgo:** Riesgo de Calidad de software

El software no puede producir resultados que no cumplan con los estándares de calidad esperados.

**Impacto:** Medio

* Falta de usabilidad.
* Satisfacción del cliente.

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  | 33 |  |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Realizar pruebas de unidad, carga, de integración y entre otras para detectar y corregir los errores
* Analizar fallas e incomodidades por parte del software para buscar soluciones y corregirlas con parches de actualización y mantenimientos

**Plan Remedial Hipotético:**

* En caso de fallas hacer rolle back a la versión más estable del software
* Evaluar fallas y analizarlas para la pronta reparación de los mismos

**Posibles Gastos para la Remediación:**

* Gastos en personal y técnicas de revisión para la mejora del software.

**Tiempo y Recursos necesarios para la Remediación:**

* Recursos lógicos y humanos para las revisiones y reparaciones
* Pruebas necesarias para asegurar un correcto funcionamiento

**Caso De Riesgo 4:**

**Riesgo:** Fallas en la parte física (Hardware) de servidores, data-center o servicio de hosting

**Impacto:** Alto.

* Pérdida de la continuidad del negocio.
* Interrupción del servicio y la satisfacción del cliente.

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  |  | **34** |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Tener planes de contingencia para la migración de los servicios en el tiempo más corto posible, llámense configuraciones y scripts de automatización como ejemplo.
* Contar con Alta disponibilidad en servicios, servidore y dispositivos primarios de red en caso de ser necesario
* Contar con sistemas de redundancia, como discos duros duplicados, puede minimizar el impacto de una falla de hardware en el negocio.

**Plan Remedial Hipotético:**

* Migraciones de servicios a ubicaciones de infraestructura diferentes.
* Generar el reporte y hacer la solicitud de soporte necesaria para la asistencia física en caso de ser un servicio de nube
* Si el equipo es irreparable, se debe sustituir lo antes posible. Si no se cuenta

con un equipo de reemplazo, se podría alquilar uno temporalmente.

**Posibles Gastos para la Remediación:**

* Si el servicio de nube, los gastos por fallas se verían cubiertos por el proveedor de servicios
* Si el hardware es físico luego de haber solucionado temporalmente con el plan de contingencia, se debe hace una evaluación para medir el impacto y los gastos que van a conllevar las respectivas reparaciones

**Tiempo y Recursos necesarios para la Remediación:**

* Una vez que se ha solucionado la falla de hardware, es importante realizar pruebas para asegurarse de que el equipo y los datos funcionan correctamente.
* Monitorización y pruebas de failover para cada uno de los sistemas más críticos para la organización

**Caso De Riesgo 5:**

**Riesgo:** Riesgo de Seguridad (USB habilitado)

**Impacto:** Alto.

* Pérdida de la información por ransomware.
* Encriptación de la información y hacer pública información sensible

**Probabilidad:** Alta.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  | **55** |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  |  |  |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Deshabilitar la lectura de Unidades de almacenamiento externas
* Asegurar configuración de arranque (Bios) con contraseña

**Plan Remedial Hipotético:**

* Restaurar los datos del servidor a partir de la copia de seguridad más reciente.

**Posibles Gastos para la Remediación:**

* No incurre en gastos adicionales, la tarea la completa el equipo de soporte de la empresa.

**Tiempo y Recursos necesarios para la Remediación:**

* El restore de la información tomará alrededor de 8 horas, 1 administrador de servidores
* Pruebas adicionales: 3 días, 1 técnico de soporte de TI.

**Caso De Riesgo 6:**

**Riesgo:** Filtraciones y violaciones de datos

**Impacto:** Alto.

* Pérdida de la continuidad del negocio.
* Interrupción del servicio y la satisfacción del cliente.

**Probabilidad:** Alta.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  | 24 |  |
| 3.  Media |  |  |  |  |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Aplique un cifrado potente: Utiliza algoritmos de cifrado potentes para proteger los datos sensibles, tanto en tránsito como en reposo.
* Actualice regularmente el software y los sistemas: Mantenga al día el software, los sistemas operativos y las herramientas de seguridad con los últimos parches y actualizaciones.
* Controles de acceso y autenticación: Limite el acceso a los datos confidenciales utilizando un control de acceso basado en funciones y métodos de autenticación sólidos, como la autenticación de dos factores.
* Formación y concienciación de los empleados: Eduque a los empleados sobre los riesgos de las brechas y filtraciones de datos y capacítelos para que sigan las mejores prácticas de seguridad.
* Auditorías de seguridad periódicas: Realice auditorías de seguridad periódicas para identificar vulnerabilidades y evaluar la eficacia de las medidas de seguridad actuales.
* Sistemas de detección y prevención de intrusiones: Utilice sistemas de detección y prevención de intrusiones para supervisar el tráfico de la red en busca de posibles amenazas a la seguridad.
* Plan de respuesta a incidentes: Desarrolla y mantén un plan de respuesta a incidentes para gestionar posibles violaciones y fugas de datos de forma eficaz y minimizar los daños.
* Eliminación segura de los datos: Elimine adecuadamente los datos sensibles utilizando métodos de borrado seguro o la destrucción física de los dispositivos de almacenamiento.
* Evaluaciones de riesgos de terceros: Evalúe las prácticas de seguridad de terceros proveedores y socios y asegúrese de que siguen las mejores prácticas del sector.
* Seguro de ciberseguridad: Considere la posibilidad de contratar un seguro de ciberseguridad para cubrir los costes asociados a las violaciones y filtraciones de datos, como honorarios legales, gastos de notificación y esfuerzos de relaciones públicas.

**Plan Remedial Hipotético:**

* Identificación de incidentes: Establecer un sistema de supervisión y detección de posibles violaciones y fugas de datos, utilizando herramientas como sistemas de detección de intrusiones, análisis de registros y análisis del comportamiento de los usuarios.
* Contención: Una vez identificada una filtración o violación de datos, tome medidas inmediatas para contener el incidente y limitar los daños. Esto puede implicar el aislamiento de los sistemas afectados, la revocación de las credenciales de acceso o el cierre temporal de servicios específicos.
* Investigación y evaluación: Lleve a cabo una investigación exhaustiva para determinar la causa y el alcance de la violación o fuga de datos. Identifique el tipo de datos comprometidos, el número de personas afectadas y las posibles implicaciones legales o reglamentarias.
* Notificación y comunicación: Notifíquelo a las personas afectadas, a los socios y a las autoridades reguladoras, tal y como exige la ley o las mejores prácticas del sector. Sea transparente sobre la situación, las medidas adoptadas para resolverla y los riesgos existentes.
* Remediación y recuperación: Aplique medidas para abordar la causa raíz de la violación o fuga de datos y evitar incidentes similares en el futuro. Esto puede implicar parchear vulnerabilidades, reforzar los controles de acceso o mejorar la formación de los empleados.
* Supervisar y evaluar: Supervise y evalúe continuamente la eficacia de las medidas correctoras para garantizar que se minimiza el riesgo de fugas y filtraciones de datos. Ajuste sus estrategias según sea necesario en función de las amenazas emergentes o las circunstancias cambiantes.
* Actualice las políticas y los procedimientos: Revise las políticas y procedimientos de ciberseguridad de su organización basándose en las lecciones aprendidas del incidente. Esto puede implicar la actualización de los controles de acceso, las prácticas de cifrado o los planes de respuesta a incidentes.
* Formación y concienciación de los empleados: Proporcione formación continua a los empleados para asegurarse de que entienden su papel en la prevención de fugas y filtraciones de datos, y son conscientes de las últimas amenazas y las mejores prácticas.
* Auditorías y evaluaciones de seguridad periódicas: Realice auditorías y evaluaciones de seguridad periódicas para identificar posibles vulnerabilidades y áreas de mejora en la postura de ciberseguridad de su organización.
* Mejora continua: Comprométase con un proceso de mejora continua en las prácticas de ciberseguridad de su organización, manteniéndose informado sobre las amenazas emergentes y ajustando sus estrategias según sea necesario para minimizar el riesgo de filtraciones y violaciones de datos.

**Posibles Gastos para la Remediación:**

* **I**nvestigación y evaluación del incidente: Contratación de expertos externos o asignación de recursos internos para investigar la filtración y evaluar su impacto.
* Contención y recuperación: Costes asociados con la contención de la brecha y la recuperación del incidente, incluida la restauración del sistema, la recuperación de datos y la posible sustitución de hardware o software.
* Notificación y comunicación: Gastos relacionados con la notificación a las partes afectadas, las autoridades reguladoras y la posible contratación de expertos en relaciones públicas o gestión de crisis para gestionar los esfuerzos de comunicación.
* Costes legales y reglamentarios: Posibles multas o sanciones impuestas por las autoridades reguladoras, honorarios legales asociados con el tratamiento de demandas o investigaciones reguladoras, y costes relacionados con la aplicación de las medidas de cumplimiento exigidas.
* Medidas correctoras: Inversión en nuevas herramientas, sistemas o infraestructuras de seguridad para abordar las causas profundas de la brecha y prevenir futuros incidentes.
* Formación y concienciación de los empleados: Costes asociados al desarrollo e impartición de programas de formación para empleados con el fin de mejorar la concienciación y las prácticas de seguridad.
* Auditorías y evaluaciones de seguridad: Contratación de auditores de seguridad externos o asignación de recursos internos para realizar auditorías y evaluaciones de seguridad periódicas.
* Actualización de políticas y procedimientos: Asignación de recursos para actualizar y mantener las políticas y procedimientos de ciberseguridad en respuesta al incidente y al cambiante panorama de amenazas.
* Seguimiento y evaluación continuos: Inversión en herramientas de supervisión y evaluación, así como la asignación de recursos para gestionar y analizar los datos resultantes.
* Primas de seguro de ciberseguridad: Si la organización decide contratar un seguro de ciberseguridad, habrá costes de primas asociados.

**Tiempo y Recursos necesarios para la Remediación:**

* Identificación del incidente: La acción inmediata (en cuestión de horas) es crucial. Los recursos necesarios incluyen herramientas de supervisión y detección, personal de seguridad y miembros del equipo de respuesta a incidentes.
* Contención: Es necesaria una actuación inmediata (entre horas y días). Los recursos necesarios incluyen personal de seguridad, personal de TI, administradores de redes y sistemas y, potencialmente, expertos externos.
* Investigación y evaluación: Este paso puede llevar de días a semanas, dependiendo de la complejidad del incidente. Los recursos necesarios incluyen expertos en ciberseguridad internos o externos, analistas forenses y, potencialmente, asesoramiento jurídico.
* Notificación y comunicación: La notificación debe producirse lo antes posible (entre días y semanas) después de que se hayan determinado el descubrimiento y el alcance del incidente. Los recursos necesarios incluyen asesoramiento jurídico, profesionales de las relaciones públicas y personal dedicado a gestionar las comunicaciones con las partes afectadas y las autoridades.
* Reparación y recuperación: Este paso puede llevar de semanas a meses, dependiendo de la gravedad del incidente y de las medidas necesarias. Los recursos necesarios incluyen personal de seguridad y TI, consultores externos y, potencialmente, proveedores de hardware o software.
* Supervisar y evaluar: La supervisión y evaluación continuas (de días a meses) son esenciales. Los recursos necesarios incluyen personal de seguridad, herramientas de supervisión y capacidades de análisis de datos.
* Actualizar políticas y procedimientos: Este paso puede llevar de semanas a meses, dependiendo de los cambios necesarios. Los recursos necesarios incluyen expertos en ciberseguridad internos o externos, asesores jurídicos y personal dedicado a revisar y actualizar la documentación.
* Formación y concienciación de los empleados: Este paso puede llevar de semanas a meses, dependiendo del alcance y la escala del programa de formación. Los recursos necesarios incluyen formadores o materiales de formación, asignación de tiempo para la participación de los empleados y, potencialmente, consultores externos.
* Auditorías y evaluaciones de seguridad periódicas: La frecuencia de las auditorías y evaluaciones puede variar en función del perfil de riesgo de la organización, pero por lo general, deben producirse al menos una vez al año. Los recursos necesarios incluyen auditores de seguridad internos o externos y personal dedicado a revisar y aplicar las conclusiones de las auditorías.
* Mejora continua: Este paso es un esfuerzo continuo, con recursos asignados para mantenerse informado sobre las amenazas emergentes y las mejores prácticas, así como para ajustar la postura de ciberseguridad de la organización en consecuencia.

**Caso De Riesgo 7:**

**Riesgo:** Phishing y ataques de ingeniería social

**Impacto:** Alto.

* Pérdida de la continuidad del negocio.
* Interrupción del servicio y la satisfacción del cliente.

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  | 24 |  |
| 3.  Media |  |  |  |  |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Desarrollar una política de ciberseguridad: Cree una política de ciberseguridad exhaustiva que describa el enfoque de la organización para gestionar los riesgos de seguridad, incluidas directrices específicas para gestionar las amenazas de phishing e ingeniería social.
* Formación y concienciación de los empleados: Organice sesiones de formación periódicas para los empleados con el fin de informarles sobre las tácticas de phishing e ingeniería social, cómo reconocer y notificar correos electrónicos o mensajes sospechosos y la importancia de respetar las mejores prácticas de seguridad.
* Aplique medidas de seguridad en el correo electrónico: Despliegue herramientas de seguridad del correo electrónico, como filtros de spam, detección de phishing y protocolos de autenticación del correo electrónico (por ejemplo, DMARC, DKIM y SPF), para reducir la probabilidad de que los empleados reciban correos electrónicos de phishing.
* Autenticación multifactor (MFA): Implemente la MFA en todas las cuentas y sistemas para reducir el riesgo de acceso no autorizado debido a credenciales robadas o comprometidas.
* Controles de acceso: Aplique el control de acceso basado en funciones y el principio del mínimo privilegio para limitar el acceso a información y sistemas sensibles, reduciendo el daño potencial causado por un ataque de phishing o ingeniería social con éxito.
* Actualice periódicamente el software y los sistemas: Asegúrese de que todo el software, los sistemas operativos y las herramientas de seguridad están actualizados con los últimos parches y actualizaciones para proteger contra vulnerabilidades conocidas que podrían ser explotadas por atacantes.
* Plan de respuesta a incidentes: Desarrolle y mantenga un plan de respuesta a incidentes que aborde específicamente los ataques de phishing y de ingeniería social, describiendo los pasos a seguir para identificar, contener y remediar los incidentes.
* Supervisar y evaluar: Supervisar y evaluar continuamente la eficacia del plan de mitigación, ajustando las estrategias según sea necesario en función de las amenazas emergentes, los avances tecnológicos o los cambios en el perfil de riesgo de la organización.
* Fomente la presentación de informes: Cree un sistema de notificación fácil de usar para que los empleados informen de correos electrónicos, mensajes u otros posibles intentos de phishing o ingeniería social sospechosos, y fomente una cultura de comunicación y notificación abierta.
* Realice auditorías y evaluaciones de seguridad periódicas: Realice auditorías y evaluaciones de seguridad periódicas para identificar posibles vulnerabilidades y áreas de mejora en la postura de ciberseguridad de la organización, incluida su capacidad para defenderse contra ataques de phishing e ingeniería social.

**Plan Remedial Hipotético:**

* Identificación de incidentes: Establecer un sistema de supervisión y detección de posibles ataques de phishing e ingeniería social, utilizando herramientas como filtros de correo electrónico, análisis del comportamiento de los usuarios e informes de los empleados.
* Activación de la respuesta a incidentes: Una vez identificado el ataque, active el plan de respuesta a incidentes de la organización y reúna al equipo de respuesta a incidentes para abordar la situación.
* Contención y aislamiento: Tomar medidas inmediatas para contener el incidente y limitar los daños. Esto puede implicar el aislamiento de los sistemas afectados, la revocación de las credenciales de acceso o el cierre temporal de servicios específicos.
* Investigación y evaluación: Llevar a cabo una investigación exhaustiva para determinar la causa y el alcance del ataque de phishing o de ingeniería social. Identifique el tipo de datos comprometidos, el número de personas afectadas y las posibles implicaciones legales o normativas.
* Notificación y comunicación: Notifíquelo a las personas afectadas, a los socios y a las autoridades reguladoras tal y como exige la ley o las mejores prácticas del sector. Sea transparente sobre la situación, las medidas adoptadas para resolverla y los riesgos existentes.
* Remediación y recuperación: Aplique medidas para abordar la causa raíz del ataque de phishing o ingeniería social y evitar incidentes similares en el futuro. Esto puede implicar reforzar la seguridad del correo electrónico, aumentar la formación de los empleados o mejorar los controles de acceso.
* Supervisar y evaluar: Supervise y evalúe continuamente la eficacia de las medidas correctoras para garantizar que se minimiza el riesgo de ataques de phishing e ingeniería social. Ajuste sus estrategias según sea necesario en función de las amenazas emergentes o las circunstancias cambiantes.
* Actualice las políticas y los procedimientos: Revise las políticas y procedimientos de ciberseguridad de su organización basándose en las lecciones aprendidas del incidente. Esto puede implicar la actualización de las directrices para la gestión de correos electrónicos sospechosos, la mejora de los planes de respuesta a incidentes o la mejora de los programas de formación de los empleados.
* Formación y concienciación de los empleados: Proporcione formación continua a los empleados para asegurarse de que comprenden su papel en la prevención de ataques de phishing y de ingeniería social, y de que conocen las últimas amenazas y las mejores prácticas.
* Auditorías y evaluaciones de seguridad periódicas: Realice auditorías y evaluaciones de seguridad periódicas para identificar posibles vulnerabilidades y áreas de mejora en la postura de ciberseguridad de su organización.

**Posibles Gastos para la Remediación:**

* Investigación y evaluación del incidente: Contratación de expertos externos o asignación de recursos internos para investigar el ataque y evaluar su impacto.
* Contención y recuperación: Costes asociados a la contención del ataque y a la recuperación del incidente, incluida la restauración del sistema, la recuperación de datos y la posible sustitución de hardware o software.
* Notificación y comunicación: Gastos relacionados con la notificación a las partes afectadas, las autoridades reguladoras y la posible contratación de expertos en relaciones públicas o gestión de crisis para gestionar los esfuerzos de comunicación.
* Costes legales y reglamentarios: Posibles multas o sanciones impuestas por las autoridades reguladoras, honorarios legales asociados con el tratamiento de demandas o investigaciones reguladoras, y costes relacionados con la aplicación de las medidas de cumplimiento exigidas.
* Medidas correctoras: Inversión en nuevas herramientas, sistemas o infraestructuras de seguridad para abordar las causas profundas del ataque y prevenir futuros incidentes.
* Formación y concienciación de los empleados: Costes asociados al desarrollo e impartición de programas de formación para empleados con el fin de mejorar la concienciación y las prácticas de seguridad.
* Auditorías y evaluaciones de seguridad: Contratación de auditores de seguridad externos o asignación de recursos internos para realizar auditorías y evaluaciones de seguridad periódicas.
* Actualización de políticas y procedimientos: Asignación de recursos para actualizar y mantener las políticas y procedimientos de ciberseguridad en respuesta al incidente y al cambiante panorama de amenazas.
* Seguimiento y evaluación continuos: Inversión en herramientas de supervisión y evaluación, así como la asignación de recursos para gestionar y analizar los datos resultantes.
* Primas de seguro de ciberseguridad: Si la organización decide contratar un seguro de ciberseguridad, habrá costes de primas asociados.

**Tiempo y Recursos necesarios para la Remediación:**

* Identificación del incidente: La acción inmediata (en cuestión de horas) es crucial. Los recursos necesarios incluyen herramientas de supervisión y detección, personal de seguridad y miembros del equipo de respuesta a incidentes.
* Activación de la respuesta al incidente: Es necesaria una actuación inmediata (en un plazo de horas a días). Los recursos necesarios incluyen personal de seguridad, personal de TI y miembros del equipo de respuesta a incidentes.
* Contención y aislamiento: Se requiere una acción inmediata (en un plazo de horas a días). Los recursos necesarios incluyen personal de seguridad, personal de TI, administradores de redes y sistemas y, potencialmente, expertos externos.
* Investigación y evaluación: Este paso puede llevar de días a semanas, dependiendo de la complejidad del incidente. Los recursos necesarios incluyen expertos en ciberseguridad internos o externos, analistas forenses y, potencialmente, asesoramiento jurídico.
* Notificación y comunicación: La notificación debe producirse lo antes posible (entre días y semanas) después de que se hayan determinado el descubrimiento y el alcance del incidente. Los recursos necesarios incluyen asesoramiento jurídico, profesionales de relaciones públicas y personal dedicado a gestionar las comunicaciones con las partes afectadas y las autoridades.
* Reparación y recuperación: Este paso puede llevar de semanas a meses, dependiendo de la gravedad del incidente y de las medidas necesarias. Los recursos necesarios incluyen personal de seguridad y TI, consultores externos y, potencialmente, proveedores de hardware o software.
* Supervisar y evaluar: La supervisión y evaluación continuas (de días a meses) son esenciales. Los recursos necesarios incluyen personal de seguridad, herramientas de supervisión y capacidades de análisis de datos.
* Actualizar políticas y procedimientos: Este paso puede llevar de semanas a meses, dependiendo de los cambios necesarios. Los recursos necesarios incluyen expertos en ciberseguridad internos o externos, asesores jurídicos y personal dedicado a revisar y actualizar la documentación.
* Formación y concienciación de los empleados: Este paso puede llevar de semanas a meses, dependiendo del alcance y la escala del programa de formación. Los recursos necesarios incluyen formadores o materiales de formación, asignación de tiempo para la participación de los empleados y, potencialmente, consultores externos.
* Auditorías y evaluaciones de seguridad periódicas: La frecuencia de las auditorías y evaluaciones puede variar en función del perfil de riesgo de la organización, pero por lo general, deben producirse al menos una vez al año. Los recursos necesarios incluyen auditores de seguridad internos o externos y personal dedicado a revisar y aplicar las conclusiones de las auditorías.

**Caso De Riesgo 8:**

**Riesgo:** Ataques DDoS (Denegación de servicio distribuido)

**Impacto:** Alto.

* Pérdida de datos críticos del usuario y del sistema.
* Interrupción de la actividad y del servicio.
* Exposición de data crítica

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  |  | **34** |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Realizar pruebas de intrusión de forma periódica.
* Mantener los diferentes softwares de defensa del sistema actualizados.
* Realizar campañas de concientización de brindar datos.

**Plan Remedial Hipotético:**

* Bloquear e hibernar las cuentas afectadas.
* Realizar bloqueos o bajas, para evitar mayor afectación.

**Posibles Gastos para la Remediación:**

* Costo de contraataque: $8,000

**Tiempo y Recursos necesarios para la Remediación:**

* Supervisión y pruebas: 1 semana, administrador del datacenter.

**Caso De Riesgo 9:**

**Riesgo:** Errores Humanos

**Impacto:** Alto.

* Exposición de data
* Interrupción del servicio.

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  |  | **34** |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Capacitaciones constantes al personal.
* Evitar tener expuestas cosas que puedan ser “fáciles” de dañar o de alta importancia, como switches, tomas, etc

**Plan Remedial Hipotético:**

* Restaurar lo dañado o obstruido lo más pronto posible.
* En caso de ser una exposición de data, intervenir.
* Realizar una revisión y verificación de todo lo que esté relacionado

**Posibles Gastos para la Remediación:**

* Los errores humanos pueden ser diversos, por lo que se tiene un backup de $15000

**Tiempo y Recursos necesarios para la Remediación:**

* Revisión mínima de 2 días por algún técnico

**Caso De Riesgo 10:**

**Riesgo:** Amenazas internas

**Impacto:** Alto.

* Exposición de data
* Interrupción del servicio.

**Probabilidad:** Media.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **RIESGO** | | **- < Impacto > +** | | | | |
| 1.  Muy bajo | 2.  Bajo | 3.  Medio | 4.  Alto | 5.  Muy Alto |
| **- < Probabilidad > +** | 1, Muy Alta |  |  |  |  |  |
| 2.  Alta |  |  |  |  |  |
| 3.  Media |  |  |  | **34** |  |
| 4.  Baja |  |  |  |  |  |
| 5.  Muy baja |  |  |  |  |  |

**Plan de Mitigación:**

* Capacitaciones constantes al personal.
* Evitar tener expuestas cosas que puedan ser “fáciles” de dañar o de alta importancia, como switches, tomas, etc

**Plan Remedial Hipotético:**

* Restaurar lo dañado u obstruido lo más pronto posible.
* En caso de ser una exposición de data, intervenir.
* Realizar una revisión y verificación de todo lo que esté relacionado

**Posibles Gastos para la Remediación:**

* Los errores humanos pueden ser diversos, por lo que se tiene un backup de $15000

**Tiempo y Recursos necesarios para la Remediación:**

* Revisión mínima de 2 días por algún técnico