Plan de recuperación y continuidad | 4Geeks

Introducción

- 1.1. Objeto del documento: Este informe presenta el plan de recuperación y continuidad del SGSI para la academia 4Geeks, alineado con las normas ISO 27001 y NIST, con el objetivo de proteger la información y asegurar la continuidad de las operaciones críticas.

- 1.2. Ámbito de aplicación: Este plan abarca todos los departamentos y sistemas de la academia 4Geeks, incluyendo la plataforma de aprendizaje en línea, la gestión de datos de estudiantes y docentes, y la infraestructura de red.

- 1.3. Auditoría Interna: Este plan es resultado de una auditoría interna del SGSI, que incluyó pruebas de penetración (pentesting) para identificar vulnerabilidades y fortalecer la seguridad de la información.

- 1.4. Vigencia y derogaciones: Este plan entra en vigor a partir de la fecha de su aprobación y reemplaza cualquier plan anterior de recuperación y continuidad.

- 1.5. Referencias: Este plan se basa en las siguientes normas y estándares:

1. *ISO 27001: Sistemas de gestión de seguridad de la información.*
2. *NIST Cybersecurity Framework: Marco de ciberseguridad del NIST.*

- 1.6. Definiciones: Se incluyen definiciones de términos clave como RTO (Objetivo de Tiempo de Recuperación), RPO (Objetivo de Punto de Recuperación), incidente de seguridad, vulnerabilidad, etc.

Controles de seguridad

2.1. Gestión de los incidentes de seguridad:

- 2.1.1. Ciberincidentes de seguridad: Se gestionarán incidentes como ataques de malware, phishing, denegación de servicio, y explotación de vulnerabilidades (FTP, SSH, wp-config.php).

- 2.1.2. Incidentes de seguridad de la información: Se manejarán casos de pérdida, robo o divulgación no autorizada de datos, incluyendo información personal de estudiantes y docentes.

- 2.1.3. Incidentes de seguridad de las personas: Se atenderán amenazas a la integridad física del personal, como accidentes o situaciones de riesgo.

- 2.1.4. Incidentes de seguridad física: Se responderá a daños a las instalaciones o equipos, como incendios, robos o desastres naturales.

- 2.1.5. Eventos de fraude comercial: Se investigarán y gestionarán intentos de fraude, como suplantación de identidad o facturas falsas.

- 2.2. Gestión de crisis: Se establece un equipo de gestión de crisis para abordar situaciones críticas que escalen más allá de un incidente de seguridad típico, como una interrupción prolongada de servicios o un ataque cibernético masivo.

- 2.3. Aplicación de cambios de emergencia: Se define un procedimiento para implementar cambios urgentes en los sistemas (parches de seguridad, actualizaciones) para mitigar vulnerabilidades como las encontradas en FTP, SSH y wp-config.php.

- 2.4. Recopilación de evidencias: Se detalla cómo se recolectarán y preservarán pruebas digitales y físicas en caso de incidentes o delitos informáticos, incluyendo el análisis forense de las vulnerabilidades explotadas.

- 2.5. Violaciones de seguridad de datos de carácter personal: Se describe cómo se gestionarán las brechas de seguridad que involucren datos personales, incluyendo la notificación a los afectados y a las autoridades competentes, siguiendo la normativa de protección de datos.

Plan de recuperación de datos y Backup.

1 Este plan establece los procedimientos para: la creación, almacenamiento y restauración de copias de seguridad de los sistemas y datos críticos de la academia 4Geeks, asegurando la disponibilidad de la información en caso de incidentes o desastres, y en línea con las normas ISO 27001 y NIST.

1.2 Vigencia y derogaciones: Este plan entra en vigor a partir de la fecha de su aprobación y reemplaza cualquier plan de copias de seguridad anterior.

1.3 Referencias: Este plan se basa en las siguientes normas y estándares:

- ISO 27001: Sistemas de gestión de seguridad de la información.
- NIST Cybersecurity Framework: Marco de ciberseguridad del NIST.

2. Responsabilidades

Responsable de la gestión de copias de seguridad: será el encargado de supervisar y ejecutar el plan de "backup", asegurando el cumplimiento de los procedimientos y la integridad de las copias de seguridad.

Administradores de sistemas: Los administradores de sistemas serán responsables de implementar las herramientas y configuraciones necesarias para la creación de las copias de seguridad, así como de realizar pruebas periódicas de restauración.

Personal de TI: El personal de TI en general deberá seguir los procedimientos establecidos en este plan y reportar cualquier anomalía o incidente relacionado con las copias de seguridad.

3. Desarrollo

3.1 Planificación:

Identificación de datos críticos: Se identificarán los datos y sistemas críticos para la operación de la academia, incluyendo la plataforma de aprendizaje en línea, la base de datos de estudiantes y docentes, y los archivos de configuración de los servidores (wp-config.php).

Frecuencia de las copias de seguridad: Se establecerá la frecuencia de las copias de seguridad, considerando la importancia de los datos y el RPO (Objetivo de Punto de Recuperación) definido. Se recomienda realizar copias de seguridad diarias de los datos críticos y copias de seguridad completas semanales.

Tipos de copias de seguridad: Se utilizarán diferentes tipos de copias de seguridad para optimizar el espacio de almacenamiento y el tiempo de restauración.

Ubicación de las copias de seguridad: Se almacenarán las copias de seguridad en un lugar seguro y separado de los sistemas de producción, preferiblemente en una ubicación remota o en la nube. Se utilizarán medidas de seguridad física y lógica para proteger las copias de seguridad contra accesos no autorizados o daños.

3.2 Protección:
Cifrado: Las copias de seguridad se cifrarán para proteger la confidencialidad de los datos en caso de acceso no autorizado.

Control de acceso: Se implementarán controles de acceso para restringir el acceso a las copias de seguridad solo al personal autorizado.

Integridad: Se utilizarán herramientas de verificación de integridad para asegurar que las copias de seguridad no hayan sido alteradas o dañadas.

Seguridad de la infraestructura: Se protegerá la infraestructura donde se almacenan las copias de seguridad contra amenazas físicas y lógicas, incluyendo firewalls, sistemas de detección de intrusiones y actualizaciones de seguridad.

3.3 Restauración:
Procedimientos de restauración: Se documentarán procedimientos detallados para la restauración de las copias de seguridad, incluyendo los pasos a seguir, los responsables y los tiempos estimados de recuperación.

Pruebas de restauración: Se realizarán pruebas periódicas de restauración para asegurar que las copias de seguridad sean válidas y que los procedimientos de restauración sean efectivos.

Priorización de la restauración: Se establecerán criterios para priorizar la restauración de los sistemas y datos críticos en caso de incidentes o desastres, considerando el impacto en la operación de la academia.

3.4 Eliminación y deshecho:
Política de retención de copias de seguridad: Se definirá una política de retención de copias de seguridad para determinar cuánto tiempo se conservarán las copias de seguridad antes de ser eliminadas.

Eliminación segura: Se implementarán procedimientos seguros para la eliminación de las copias de seguridad, asegurando que los datos sean destruidos de forma irreversible.