4Geeks Academy

Manual del Sistema de Gestión de Seguridad de la Información

Por: Juan Cervantes Simón

Manual del Sistema de Gestión de Seguridad de la Información

- **Introducción**
  En este manual se recogen todas las especificaciones, normativas, grupos de interés, controles y políticas que conforman la normativa general para la gestión de la información institucional, estudiantil y de personal, protegiendo activamente esta de las filtraciones y robos de datos, al tiempo que se asegura su confidencialidad y disponibilidad, levantando medidas de protección activas y pasivas que también ayudan a identificar y prevenir el impacto de las mismas sobre el SGSI académico.

- **Alcance del Sistema**
  El SGSI pretende cubrir la administrativa, así como las plataformas académicas del estudiantado, protegiendo con ello los datos personales de todos los usuarios.
  De la misma forma, quedan fuera de la protección las plataformas que prestan servicios de forma remota, sin embargo sí que se protege la conexión que la academia guarda con estas.

- **Normativas utilizadas**
  Para el desarrollo de este manual se ha seguido la normativa de la **ISO 27001**, que provee de estándares internacionales en la creación de un SGSI, así como la **normativa vigente** en materia de controles mínimos y procedimiento de respuesta a incidentes.

- **Equipos implicados**
  - Equipo ejecutivo: Sus funciones principales son la toma de decisiones sobre las normativas, aprobando o denegando las medidas propuestas al tiempo que gestiona los recursos financieros de los que dispone el centro.

  - Equipo de Seguridad: Es un grupo destinado a supervisar las funciones, verificando que se cumpla con las normativas y políticas descritas en el SGSI.

  - Equipo Técnico: Departamento encargado de aplicar configuraciones necesarias para dar cumplimiento a la normativa, así como la realización de las labores de mantenimiento de la infraestructura.

  - CSIRT: Es el equipo de respuesta a incidentes en el apartado de ciberseguridad.

  - CISO: Coordinador de las operaciones asociadas a la seguridad además de emitir las notificaciones a la dirección en caso de incidentes.

  - Responsable de Datos: Es el responsable de los datos, clasificando su nivel de criticidad y definiendo qué roles acceden y como a los datos requeridos.

❖ Clasificación de los datos

La clasificación estipulada según la normativa vigente organiza la criticidad de los datos de la siguiente forma:

- ➢ Riesgo Alto
  Datos personales de grán sensibilidad, como registros médicos del personal, documentos de identidad así como las investigaciones en curso y las patentes.

- ➢ Riesgo Medio
  Datos de carácter administrativo de sensibilidad moderada, cuya filtración y/o revelación al público puede traer consecuencias legales moderadas, como sanciones monetarias o avisos formales, como puede ser el caso de los datos financieros o académicos personales de los alumnos.

- ➢ Riesgo Bajo
  Esta categoría se refiere a la información pensada para uso del personal administrativo y/o docente, en la que se detallan procesos operativos así como información laboral que no ha sido pensada para presentar al público.

- ➢ Datos Públicos
  Datos pensados y aprobados por el grupo responsable para ser difundidos al público, como puede ser el caso de los boletines de jornadas de puertas abiertas o ferias de investigación.

❖ Evaluación de Riesgos

Para la evaluación de riesgos del sistema, se ha tomado como referencia el plan de cuatro etapas que presenta el NIST:

- ➢ Preparación de la revisión, definir qué áreas y datos se van a evaluar y qué métodos de evaluación van a ser usados.

- ➢ Realización de la evaluación, se listan las amenazas percibidas para los activos a examinar así como las vulnerabilidades encontradas, con ello se estima la probabilidad e impacto de los mismos para denotar el nivel del riesgo.

- ➢ Comunicación de los resultados obtenidos al equipo directivo con la correspondiente documentación de la evaluación.

- ➢ Planificar y ejecutar revisiones anuales de la infraestructura, o ante cambios de normativa importantes si estos se producen antes del año.

- **Controles del Sistema**

  Los controles de seguridad implementados en el sistema han sido los siguientes:

  - Inventariado de Equipos.
  - Autenticación Multi-Factor.
  - Cifrado de Equipos.
  - Segmentación en la Infraestructura.
  - Políticas de acceso basadas en roles.
  - Políticas de creación de copias de seguridad.
  - Control de versiones y actualizaciones.
  - Planificación de formación del personal.
  - Planificación de logs y monitorización.
  - Planificación de auditorías.
  - Plan de respuesta a incidencias.

- **Políticas y Procedimientos**

  En el desarrollo de estos documentos que definen el sistema de gestión de seguridad de la información se han definido las siguientes políticas principales:

  - Política de gestión de incidentes:
    En esta política se detalla el proceso a seguir en el ejercicio de detección y mitigación de incidencias, así como el apartado de mejora del proceso.

  - Política de copias de seguridad:
    En esta política se determinan la cantidad de copias de seguridad, la frecuencia y puntos de almacenamiento de las copias.

  - Política de acceso a datos:
    En ella indican los requisitos para que los usuarios accedan a los datos, así como los deberes en el manejo de datos que los usuarios y empleados deben de cumplir.

  - Política de Formación del personal y concienciación al estudiante:
    Plantea el programa de concienciación y capacitación del estudiantado y plantel de empleados con objetivo de reducir el fallo humano en la aparición de riesgos.

  - Políticas de Auditaje y revisión:
    Define la parte del SGSI que describe la planificación de revisiones para la elaboración de informes de mejora constante que presentar para la actualización del SGSI.

- **Línea de tiempo para la implantación**

  - Durante los 3 primeros meses se crearía el grupo ejecutivo, se crearía el informe de inventario y se definirían las políticas básicas para las siguientes etapas.

  - En los siguientes 8 meses vista (entre los meses 4 y 12) se implementarán las medidas de seguridad de acceso a datos que los usuarios deberán cumplir, así como también se creará el grupo de ciberseguridad para la respuesta a incidencias, además, se comenzará con la instrucción y concienciación del plantel y el estudiantado mediante las medidas especificadas.

  - Durante el siguiente año se tratarán de optimizar los procesos operativos y automatizar la creación y actualización de los registros, con objetivo de hacer lo menos tediosos posibles los ejercicios de monitorización de datos.

  - A partir de los dos años de administración del proceso anteriormente descrito, se realizarán las revisiones periódicas estipuladas y se mejorará el sistema en función de los resultados obtenidos en las auditorías.

- **Indicadores de interés**
  Las principales señales de que el sistema está rindiendo adecuadamente son principalmente el tiempo de respuesta ante incidencias de seguridad de datos y disponibilidad de datos y servicios docentes, siendo que lo que se trata de conseguir es la mayor cobertura posible y el tiempo mínimo de respuesta.

- **Revisión del SGSI y Mejora contínua**
  Para lograr un refinamiento constante de este SGSI, así como de sus procesos y controles, se revisarán todos ellos anualmente, tanto las políticas como los controles, con objeto de adaptar los controles a las necesidades de la institución a medida que estas surjan, asimismo también se busca adaptarse ante cambios o nuevas normativas emergentes por parte del gobierno, realizando una revisión tan pronto como estos cambios o nuevas normativas salgan aprobadas.

- **Compromiso de cumplimiento**
  Para que todas las medidas descritas en este manual sean realmente efectivas se necesita del cumplimiento de cada política de seguridad por parte del usuario al que afecte, así como siempre tratar de aplicar las mejores prácticas posibles en el manejo de datos.

❖ **Plantillas Adjuntas**

➢ *Notificación de Incidencia*

- Nombre del usuario que reporta
- Descripción de los hechos
- Dispositivos/Áreas afectadas por la incidencia:
    - <Plataforma X>
    - <Servidor X>
    - etc...
- Acciones tomadas:
    - <Medida 1>
    - <Medida 2>
    - etc…
- Fecha de apertura de incidencia y de cierre en caso de solución.