Pentesting Technical Report

4Geeks
Ph: +1 786 345 5555

0. Índice

1. Introducción

El principal objetivo de esta práctica sería elegir una organización de las que se nos propone, en este caso la elegida es el Sistema de la universidad de California debido a que maneja mucho tipo de datos, lo que implica tener una buena seguridad para la protección de los mismos.

2. Definición del alcance

2.1 Propósito y objetivos del SGSI

El principal objetivo del SGSI sería establecer un marco para proteger la información,gestionando su prioridad según sea el tipo de activo(crítico,alto,medio,bajo),para garantizar la confidencialidad, integridad y disponibilidad de la información crítica, cumpliendo con normativas legales y buenas prácticas internacionales (como ISO/IEC 27001).

2.2 Inventario y clasificación de activos

Tipo de Activo	Ejemplos	Clasificación
Hardware	Servidores,ordenadores,router …	Crítico/Alto
Software	Sistemas de gestión,ERP…	Crítico
Datos	Expedientes de estudiantes,nóminas,registros médicos	Crítico/Alto
Recursos Humanos	Personal administrativo,alumnos,profesores	Alto
Red	VLAN internas,Wifi,VPN	Crítico
Plataformas en la nube	Google Workspace,AWS	Medio

2.3 Límites físicos del SGSI

En cuanto a límites físicos, el SGSI se aplicará en el campus de la Universidad de California:

- Oficinas de administración
- Salas de servidores y centro de datos
- Aulas digitalizadas
- Laboratorios de investigación

2.4 Áreas de acceso restringido

Una vez quedan definidos los límites físicos, tenemos que delimitar el acceso restringido para evitar que personas no deseadas entren como por ejemplo a una sala de servidores;

- Centro de procesamiento de datos: el SGSI establece solo personas que estén autorizadas.
- Laboratorios donde se manejan datos sensibles
- Oficina de recursos humanos: la política define los datos que manejan,como nóminas etc…
- Salas donde se guarda equipo informático: ya que alguien podría entrar y manipular los equipos

2.5 Redes, entornos virtuales y sistemas en la nube

Otra forma de alcance en SGSI sería indicando que equipos(IP) pueden acceder a que cosas en la red:

- Acceso por VPN: lo hará todo más seguro
- Usar plataformas Cloud
- Usar sistemas virtuales con IP aisladas del dominio principal para evitar incidentes y limitar propagaciones.

2.6 Partes interesadas y responsabilidades

A su vez, se implementa gestionar personas o grupo de personas y el rol que cumple en SGSI:

-Dirección de la Universidad: aprobar políticas.
-Departamento IT: implementar controles técnicos.
-Estudiantes: Cumplimiento de políticas de la Universidad.

2.7 Limitaciones o exclusiones

El SGSI no cubre los campus externos a la universidad fuera de alcance geográfico ni dispositivos personales del alumnado de la universidad.

3. Evaluar riesgos

Para la evaluación de riesgos se seguirá la metodología basada en directrices de la norma ISO/IEC 27005.

1. Identificación de activos: como podría ser,los servidores que se alojan en sistemas académicos y administrativos,sistemas de autenticación de usuarios,red interna del campus,sistemas en la nube.
2. Identificación de amenazas y vulnerabilidades:

Amenaza	Descripción
Acceso no autorizado	Acceso de usuarios no autorizados a datos personales o sistemas sensibles
Malware y ransomware	Software malicioso
Phishing	Correos fraudulentos
Fallos hardware	Averías en servidores u ordenadores

3. Valoración del impacto y probabilidad.

Riesgo	Impacto	Probabilidad	Nivel de riesgo
Acceso no autorizado	Alto	Media	Alto
Malware,ransomware	Crítico	Media	Crítico
Fallo hardware	Alto	Media	Medio
Phishing	Alto	Media	Alto
Fuga de datos	Alto	Alta	Crítico

Una vez se implementen VPN,backups etc, se volverán a evaluar los riesgos para estimar los riesgos residuales que queden.

4. Estimación del riesgo: siempre hay que estimar un riesgo aproximado para en caso de incidente hagan el menor daño posible y estemos lo más preparados que podamos.
5. Aceptación y mitigación del riesgo: una vez hemos aceptado los riesgos que existen en la universidad,se busca una forma de mitigar cada uno de ellos de la manera más rápida y eficaz.

Aunque algunos riesgos presentan la misma combinación de impacto y probabilidad que sostiene la ISO 27001 su nivel final de riesgo puede no ser el mismo debido a que unos datos llegan a ser más sensibles que otros,es el ejemplo de datos de cuentas bancarias en las nóminas tiene un mayor grado de importancia que por ejemplo que un listado de los horarios de clase. En este caso, aunque ambos activos puedan estar expuestos a una misma amenaza (como un acceso no autorizado) y con la misma probabilidad, el impacto real sobre la organización sería mucho mayor en el caso de las nóminas, ya que podría suponer una violación grave de la privacidad, consecuencias legales y una pérdida significativa de confianza.Por tanto, se han considerado factores adicionales como:

- El valor del activo dentro de la organización.
- La naturaleza sensible de la información.
- Las posibles repercusiones legales y reputacionales.

4. Selección de controles

Deberemos de seleccionar controles de seguridad apropiados para cada uno de los posibles riesgos encontrados en la empresa:

1. Gestionar acceso de los usuarios,gestionar privilegios:con esto solucionamos que cualquier estudiante o persona ajena pueda llegar a acceder a contenido que es privado y sensible.
2. Uso de firewall o WAF: con el uso de estas herramientas podemos llegar a controlar que nos descarguemos un ransomware o cualquier otro tipo de virus por error.
3. Gestionar correo y uso de filtros: gracias a una buena gestión del correo, e incluso de aplicar una serie de filtros en nuestro correo podemos hacer que el phishing pase a bandeja de spam y pase a un plano secundario
4. Aplicar reglas de entrada y salida: al aplicar una serie de reglas en la red con iptable podemos gestionar que equipos son capaces de entrar y salir además de poder aplicar un monitoreo de red con otras aplicaciones para saber qué hace cada equipo.

5. Controlar los dispositivos extraíbles: a menos que un supervisor lo asigne,no podrán añadir un dispositivo extraíble para así evitar una fuga de datos.
6. Realizar copias de seguridad con continuidad: al realizar copias seguridad de nuestros datos y servidores haremos que en caso de un incidente y pérdida de datos o incluso una caída del servidor no perdamos datos.
7. Formar a los empleados: con una formación básica previa podemos prevenir muchos incidentes como podría ser phishing,descargas de virus de servicios de terceros,etc…

Control	Código ISO 27001	Prioridad
Gestionar acceso de los usuarios	A.5.15, A.5.16, A.5.17	Alta
Uso de firewall o WAF	A.8.22	Alta
Gestionar correo y uso de filtros	A.8.23, A.8.9	Media
Aplicar reglas de entrada y salida	A.8.7, A.8.8	Media/Alta
Controlar los dispositivos extraíbles	A.8.10	Alta
Realizar copias de seguridad con continuidad	A.8.13	Alta
Formar a los empleados	A.6.3	Alta

Para el orden implementación primero deberemos de pensar que opción puede llegar a abarcar más campos más rápidamente y de una manera más cómoda,en este caso al tratarse de una universidad podemos pensar:

1. Dar una breve formación a los empleados: es la vía más rápida,fácil y la que más campos abarca ya que con una formación serán capaces de distinguir que correos pueden llegar a ser no deseados,además de dejar de realizar una descargas inapropiadas por falta de conocimiento.
2. A su vez algo que es muy importante sería el gestionar los privilegios de los usuarios ya que así podemos asignar que usuario puede hacer una tarea específica en el equipo del dominio y cuales no pueden hacerla sin orden de un supervisor.
3. Aplicar reglas en red sería muy importante también casi al mismo nivel que gestionar los privilegios de los usuarios ya que si gestionamos qué equipos pueden entrar a que parte de la red lo que nos resulta muy útil además usar aplicaciones para monitorear la red.
4. Realizar copias de seguridad, es muy buena práctica para prevenir posibles pérdidas de datos en caso de ataque.
5. Usar un firewall o waf, también es muy importante y también se le debería de dar mucha prioridad ya que con un buen uso de waf o firewall podemos monitorear la red y ver que está ocurriendo en todo momento, así como prevenir posibles acceso o descargas maliciosas.

5. Políticas y procedimientos de seguridad

5.1 Política general de seguridad

La Universidad de California establece como principio fundamental la protección de la información y sus activos,garantizando así los 3 pilares fundamentales de la ciberseguridad(confidencialidad,integridad y disponibilidad).Todo el alumnado o persona colaboradora con el centro deberá de cumplir dichas políticas.

5.2 Procedimientos implementados

Los procedimientos son:

- Gestión de accesos: el acceso a sistemas y datos se concede con mínimo privilegio, los usuarios deben autenticarse mediante unas credenciales seguras,las cuentas inactivas se desactivan.

- Gestión de contraseñas: cada X días se cambiará,requisitos mínimos de 12 caracteres, uso de símbolos etc… Prohibido reutilizar contraseñas ya usadas previamente.

- Uso aceptable de los recursos TIC: prohibido instalar software no autorizado,no se permite el uso de dispositivos sin cifrado,se vigilará el uso de red.

- Copia de seguridad: se realizan backups automáticos programados diariamente,se almacenan en un lugar seguro y se prueban las restauraciones para comprobar que se está realizando correctamente

- Solo se permite el uso de dispositivos externos: autorizados y siempre con un previo escaneo del dispositivo a introducir.

- Protección de la red: siempre usando un firewall o una segmentación de red por áreas(alumnos,profesorado).

- Usar plataformas cloud: solo se permite el uso de plataformas aprobadas(Google),los datos son confidenciales y se deben cifrar.

En caso de incidente(pérdida de datos, accesos no autorizados, malware, etc.) debe reportarse inmediatamente al equipo de seguridad IT.
Ellos disponen del procedimiento de respuesta a incidentes con niveles de severidad y tiempos de reacción correctos y previamente definidos.

Todos los empleados deberán de recibir una formación anual sobre prácticas básicas de ciberseguridad(phishing,gestión de contraseñas…)

6. Conclusiones

El Sistema de Gestión de Seguridad de la Información para el entorno de la Universidad de California sienta las bases para una gestión eficaz y proactiva de la seguridad de la información en el entorno universitario.
Con este SGSI se ha definido un alcance claro, identificando qué activos son más críticos y qué espacios físicos y tecnológicos forman parte del sistema.

A través del análisis de riesgos se han podido detectar las principales amenazas y vulnerabilidades,que han permitido priorizar acciones de seguridad y diseñar un plan de actuación eficiente.

Además, se han creado políticas y procedimientos que no sólo ordenan la gestión de la seguridad, sino que también ayudan a que cada persona dentro de la universidad sepa qué papel tiene en este proceso: desde el equipo técnico hasta el alumnado de la Universidad.

Este trabajo deja claro que la seguridad no es algo que se implemente una sola vez y ya está. Es un proceso continuo y que tiene que ir mejorando a medida que va pasando el tiempo,además que necesita revisión constante, adaptación a los cambios tecnológicos y compromiso por parte de todos.
Gracias a este sistema, la universidad no solo protege sus datos, sino que también da un paso firme hacia una cultura de seguridad real, adaptada a su entorno y alineada con las mejores prácticas. Esto también transmite confianza a toda la comunidad universitaria.