Auditoría de sistemas

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Auditoria de sistemas 3

1.1. Antecedentes 3
1.2. Objetivos 3
1.3. Checklist 4
1.4. Puntos clave 5

2. Referencias 6

1. AUDITORIA DE SISTEMAS

1.1. Antecedentes

Ante el incesante aumento de los **ataques** de ciberseguridad, la empresa debe determinar su **nivel de seguridad** actual y establecer el nivel que ha de conseguir [1] para proteger los sistemas y la información corporativos. Por este motivo es necesario realizar auditorías que permitan la **evaluación y análisis** de la seguridad de los sistemas [2]. Dichas auditorias se realizarán normalmente por personal externo especializado, y ayudarán a mejorar la seguridad, eficacia y eficiencia de nuestros procesos.

Por otro lado, en ciertos casos es necesario solicitar auditorías especializadas, como por ejemplo auditorias de revisión de **cumplimientos legales** (auditoría RGPD y LSSI-CE), o auditorías **forenses** para investigar lo ocurrido tras un incidente grave (brecha de datos, botnet, ransomware, DDoS, etc.).

1.2. Objetivos

Obtener **evidencias** de que cómo nuestros sistemas de información cumplen con los **requisitos de seguridad** deseados. Utilizar estas evidencias para llevar a cabo un proceso de mejora continua de la ciberseguridad.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **auditoria de sistemas**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
A	PRO	**Detallar los elementos clave que queremos que sean auditados** Tienes identificados los activos más relevantes que deben ser auditados.	☐
B	PRO	**Mejora continua y modelos de madurez** Enfocas el proceso de auditoría desde un punto de vista de mejora continua o de consecución de niveles de madurez.	☐
A	PRO/TEC	**Auditorías legales** Realizas auditorías específicas para verificar el cumplimiento de los requerimientos legales del RGPD.	☐
A	PRO/TEC	**Auditorías forenses** Realizas auditorías forenses para determinar lo ocurrido tras un incidente de seguridad.	☐
A	TEC	**Procedimientos** Has definido/revisado procedimientos detallados para auditar la seguridad de cada activo clave de tus sistemas de información.	☐
A	TEC	**Realización de auditorías periódicas** Realizas auditorías de tus sistemas de información cada _____.	☐
A	PRO/TEC	**Análisis del resultado de la auditoría** Analizas los resultados de la auditoría en busca de debilidades a corregir.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Detallar los elementos clave que queremos que sean auditados.** Para llevar a cabo con éxito el proceso de auditoría, es necesario identificar los activos de información [3] más importantes (críticos) de la empresa cuya seguridad queremos que sean revisada. Estos activos pueden ser desde ficheros, bases de datos, páginas web, equipos o programas hasta servicios completos. Para estos activos revisaremos los aspectos de ciberseguridad, entre otros [4]:
  - sistemas antimalware
  - procesos de gestión de permisos
  - procesos para el cumplimiento legal
  - políticas de prevención de fraude y de fuga de datos
  - sistema de actualizaciones
  - sistemas de monitorización de recursos
- **Mejora continua y modelos de madurez.** Para garantizar que los resultados de las auditorias conllevan la implantación de mejoras permanentes en ciberseguridad, es necesario enfocar el proceso de auditoría desde un punto de vista de mejora continua o de consecución de niveles de madurez [5].
- **Auditorías legales.** Para garantizar el cumplimiento de ciertos requisitos legales puede ser conveniente u obligatorio, realizar auditorías específicas, por ejemplo, el cumplimiento por parte de nuestra empresa del RGPD [6].
- **Auditorías forenses.** Para identificar las causas que han producido un incidente y recabar evidencias para su análisis posterior, para depurar responsabilidades o para iniciar una denuncia.
- **Procedimientos.** Seleccionaremos el tipo de auditoría más conveniente [4]:
  - test de penetración
  - auditoría de red
  - auditoría de seguridad perimetral
  - auditoría web
  - auditoría forense
  - auditoria legal

  Definiremos con detalle los procedimientos y *logs* [7] necesarios para realizar cada tipo de auditoría. Asimismo, concretaremos cómo registrar los resultados de estas revisiones.
- **Realización de auditorías periódicas.** Debemos realizar auditorías periódicas independientes con la finalidad de revisar y evaluar todos los aspectos relacionados con la seguridad de la información de nuestra empresa. Fijaremos esta periodicidad al menos con carácter bianual. Evaluaremos si debemos repetir estas auditorías tras la implantación de algún cambio significativo en nuestros sistemas.
- **Análisis del resultado de la auditoría.** Se analizan los resultados de la auditoría en busca de errores o debilidades. Se llevan a cabo acciones para corregir las vulnerabilidades detectadas:
  - identificación de las causas y motivos del resultado desfavorable
  - evaluación de las medidas correctoras
  - implantación y revisión de dichas medidas

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plan Director de Seguridad https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

[2]. Incibe – Protege tu empresa – Blog – Analizando la seguridad de nuestra empresa https://www.incibe.es/protege-tu-empresa/blog/analizando-seguridad-empresa

[3]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plantilla ejemplo para el inventario de activos https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad#descargas

[4]. Incibe – Protege tu empresa – Blog – A tu empresa también le toca hacerse una revisión... de ciberseguridad https://www.incibe.es/protege-tu-empresa/blog/tu-empresa-tambien-le-toca-hacerse-revision-ciberseguridad

[5]. ISO2700.es ¿Cómo puede medirse la seguridad? http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf

[6]. Incibe – Protege tu empresa – Blog – Para cumplir correctamente el RGPD, sigue estas siete recomendaciones https://www.incibe.es/protege-tu-empresa/blog/cumplir-correctamente-el-rgpd-sigue-estas-siete-recomendaciones

[7]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Gestión de *logs* https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INSTITUTO NACIONAL DE CIBERSEGURIDAD