CLASIFICACIÓN DE LA INFORMACIÓN

POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

PROTEGE TU EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Clasificación de la información 03

1.1. ANTECEDENTES 03

1.2. OBJETIVOS 04

1.3. CHECKLIST 04

1.4. PUNTOS CLAVE 06

2. REFERENCIAS 08

1. CLASIFICACIÓN DE LA INFORMACIÓN

1.1 ANTECEDENTES

La **información** es uno de los activos principales de cualquier empresa y como tal tenemos que protegerla adecuadamente **[1]**.

Los activos de información pueden estar en formato digital o en otros soportes (papel, película fotográfica, etc.). En formato digital podrán ser desde ficheros de todo tipo (texto, imagen, multimedia, bases de datos...), pasando por los programas y aplicaciones que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.

Para aplicar las medidas de seguridad ajustadas a cada activo de información, debemos realizar un **inventario** y clasificarlos, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, aplicando para ello criterios de confidencialidad, integridad y disponibilidad. Así, sabremos qué información debemos cifrar, quién puede utilizarla, quién es responsable de su seguridad, cada cuánto hacer *backup*, etc.

Estos son algunos ejemplos:

- La aplicación de nóminas es confidencial y sólo tendrán acceso a ella ciertos empleados del departamento de personal para los cuales habilitaremos permisos.
- El acceso al gestor de la página web está restringido al personal de gobernanza web.
- Se han de cifrar los documentos que se envíen a la gestoría por correo electrónico.
- Los servicios que traten datos personales tendrán que cumplir el RGPD **[2]**.
- El ERP (*Enterprise Resource Planning*) es crítico para la empresa y se deben hacer copias de seguridad semanalmente.

Además, al clasificar los activos de información debemos establecer su **ciclo de vida**, que dependerá no solo de la vida útil del soporte, sino también de la vigencia de su contenido. Si el soporte caduca antes que el contenido, tendremos que regenerarlo en otro soporte. El ciclo de vida de la información determinará el momento en el cual dejará de ser útil, y por tanto cuándo tenemos que eliminarla convenientemente **[3]**.

1.2 OBJETIVOS

Clasificar los activos de información para garantizar una eficaz gestión de su seguridad con criterios de **confidencialidad, disponibilidad e integridad.**

1.3 CHECKLIST

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

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.

1.3 CHECKLIST

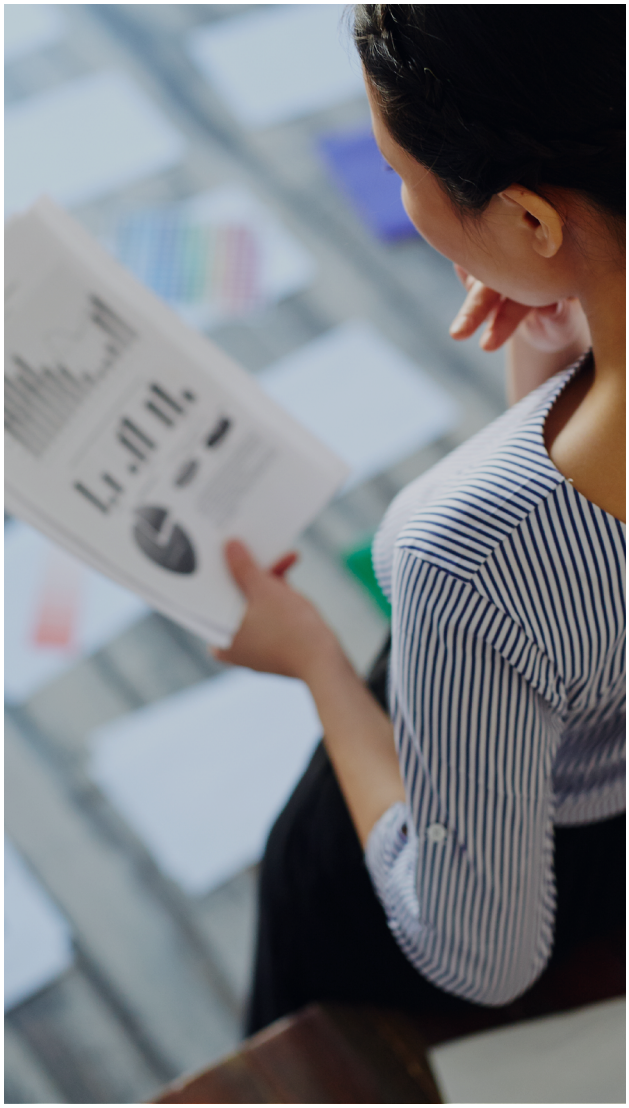
Nivel	Alcance	Control	
B	PRO	**Inventario de la información.** Elaboras un inventario detallado de los activos de información de tu empresa.	☐
B	PRO	**Criterios de clasificación de la información.** Determinas claramente los criterios de seguridad con los que clasificarás los activos de información de tu empresa.	☐
B	PRO	**Clasificación de la información.** Etiquetas los activos de información según los criterios de seguridad establecidos.	☐
B	PRO	**Tratamientos de seguridad disponibles.**Estableces una lista con todos los tratamientos de seguridad de la información disponibles en tu empresa.	☐
A	TEC	**Establecer y aplicar los tratamientos que corresponden a cada tipo de información.** Aplicas correctamente los tratamientos de seguridad que corresponden a cada activo información.	☐
A	TEC	**Auditorías.** Realizas auditorías externas de comprobación de manera periódica. Fecha de última auditoría: dd/mm/aaaa.	☐
A	TEC	**Utilizar modelos de seguridad de la información.** Usas modelos de clasificación de la información para favorecer las fases de implementación, mantenimiento y mejora de la SGSI (ejemplo: ISO 27001).	☐

Revisado por: _____ **Fecha:** _____

1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Inventario de la información.** Es necesario establecer un inventario de los activos de información disponible en la empresa, considerando registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quiénes son sus responsables, etc.
- **Criterios de clasificación de la información.** Debemos establecer claramente los criterios de clasificación que vamos a aplicar a los activos de información. Estos deberán estar relacionados con las medidas de seguridad que plantearemos aplicar a nuestra información. Algunos de estos criterios podrían ser:



- **Por el nivel de accesibilidad o confidencialidad [4]:**
  - Confidencial. Accesible solo por la dirección.
  - Restringida. Accesible solo por el nivel directivo y empleados concretos.
  - Interna. Accesible solo al personal de la empresa.
  - Pública. Accesible públicamente.
- **Por su utilidad o funcionalidad:**
  - Información de clientes y proveedores.
  - Información de compras y ventas.
  - Información de personal y gestión interna.
  - Información sobre pedidos y procesos de almacén.
- **Por su utilidad o funcionalidad:**
  - Daño de imagen.
  - Consecuencias legales.
  - Consecuencias económicas.
  - Paralización de la actividad.

1.4 PUNTOS CLAVE

- **Clasificación de la información.** Asignaremos a cada tipo de información una etiqueta según los criterios de clasificación establecidos.
- **Tratamientos de seguridad disponibles.** Elaboraremos un listado con todos los tratamientos de seguridad de los que dispone la empresa, tales como herramientas de cifrado, sistemas de copias de seguridad **[5]**, sistemas de control de accesos **[6]**, etc.
- **Establecer y aplicar los tratamientos que corresponden a cada tipo de información.** Una vez clasificada la información, debemos asignar y aplicar los tratamientos de seguridad oportunos para cada tipo de información. Entre estos tratamientos, podríamos contemplar los siguientes:
  - Limitar el acceso a las personas o grupos correspondientes.
  - Cifrar la información.
  - Realizar copias de seguridad.
  - Medidas específicas como las reflejadas en el reglamento del RGPD.
  - Información sujeta a acuerdos de confidencialidad concretos **[7]**.
  - Control del acceso y/o modificación de la información.
- **Auditorías.** Conviene realizar periódicamente auditorías de seguridad **[8]** que certifiquen que se aplican los tratamientos estipulados para proteger nuestra información. Las auditorías realizadas por personal externo siempre podrán aportar beneficios como:
  - Garantizar la independencia de las revisiones o auditorias.
  - Contribuir con un punto de vista imparcial.
  - Aportar la experiencia de profesionales de la seguridad de la información que conocen otras organizaciones y pueden ayudar a la compañía a mantener un control adecuado de la clasificación de la información a través de lecciones aprendidas y soluciones implementadas en otras empresas.
- **Utilizar modelos de seguridad de la información.** Emplear referencias como la ISO 27001. Dicha normativa, opcional de clasificación de la información, evalúa los datos que se encuentran almacenados en la empresa y determina un nivel de protección acorde a cada tipo de dato. Estos modelos, de cumplimiento voluntario, de gestión y clasificación de la información pueden servir de referencia para establecer una política interna.

2. REFERENCIAS

[1] INCIBE – Empresas – ¿Qué te interesa? – Protección de la información – https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

[2] Diario Oficial de la Unión Europea – Reglamento general de protección de datos RGPD– https://www.boe.es/doue/2016/119/L00001-00088.pdf

[3] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Borrado seguro y gestión de soportes – https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/borrado-seguro-y-gestion-soportes.pdf

[4] INCIBE – Empresas– ¿Qué te interesa? – Protección de la información – Ejemplo de matriz de clasificación de la información – https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

[5] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Copias de seguridad – https://www.incibe.es/sites/default/files/contenidos/politicas

[6] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Control de acceso – https://www.incibe.es/sites/default/files/contenidos/politicas

[7] INCIBE – Empresas – Blog – Información confidencial, secreto profesional. Acuerdo de confidencialidad – https://www.incibe.es/empresas/blog/informacion-confidencial-secreto-profesional-acuerdos-confidencialidad

[8] INCIBE – Empresas – Herramientas – Políticas de seguridad para la pyme – Auditoria de sistemas – https://www.incibe.es/sites/default/files/contenidos/politicas

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

INSTITUTO NACIONAL DE CIBERSEGURIDAD