

RI 812

**CONFIDENTIAL**

# Clasificación de la información

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE  
CIBERSEGURIDAD  
SPANISH NATIONAL  
CYBERSECURITY INSTITUTE

 **incibe**  
INSTITUTO NACIONAL DE CIBERSEGURIDAD



## ÍNDICE

---

<b>1. Clasificación de la información.....</b>	<b>3</b>
1.1. Antecedentes .....	3
1.2. Objetivos .....	3
1.3. Checklist .....	4
1.4. Puntos clave.....	5
<b>2. Referencias .....</b>	<b>6</b>

# 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 aplicativos 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 [8] 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 cuanto hacer *backup*, etc.

Estos son algunos ejemplos:

- el aplicativo de nóminas es confidencial y sólo tendrán acceso a él ciertos empleados del departamento de personal para los cuales habilitaremos permisos;
- el acceso al gestor de la página web está restringido al personal de marketing;
- se han de cifrar los documentos que se envíen a la gestoría por correo electrónico;
- los servicios que traten datos personales tendrán que cumplir la LOPD;
- el ERP es crítico para la empresa y se debe hacer *backup* semanalmente.

Además, al clasificar los activos de información debemos establecer su **ciclo de vida**, que dependerá no sólo 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 [2].

## 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.

NIVEL	ALCANCE	CONTROL	
B	PRO	<b>Inventario de la información</b> Elaboras un inventario detallado de los activos de información de tu empresa.	<input type="checkbox"/>
B	PRO	<b>Criterios de clasificación de la información</b> Determinas claramente los criterios de seguridad con los que clasificarás los activos de información de tu empresa.	<input type="checkbox"/>
B	PRO	<b>Clasificación de la información</b> Etiquetas los activos de información según los criterios de seguridad establecidos.	<input type="checkbox"/>
B	PRO	<b>Tratamientos de seguridad disponibles</b> Estableces una lista con todos los tratamientos de seguridad de la información disponibles en tu empresa.	<input type="checkbox"/>
A	TEC	<b>Establecer y aplicar los tratamientos que corresponden a cada tipo de información</b> Aplicas correctamente los tratamientos de seguridad que corresponden a cada activo información.	<input type="checkbox"/>
A	TEC	<b>Auditorías</b> Realizas auditorías de comprobación cada _____.	<input type="checkbox"/>

Revisado por: \_\_\_\_\_

Fecha: \_\_\_\_\_

## 1.4. Puntos clave

Los puntos clave de esta política son:

- **Inventario de la información.** Es necesario establecer un inventario [8] de los activos de información disponible en la empresa, considerando registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quienes 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 [3]:
    - Confidencial. Accesible solo por la dirección o personal concreto
    - 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 el impacto por robo, borrado o pérdida:
    - daño de imagen
    - consecuencias legales
    - consecuencias económicas
    - paralización de la actividad
- **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 [4], sistemas de control de accesos [5], 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 de la LOPD
  - información sujeta a acuerdos de confidencialidad concretos [6]
  - control del acceso y/o modificación de la información
- **Auditorías.** Conviene realizar periódicamente auditorías de seguridad [7] que certifiquen que se aplican los tratamientos estipulados para proteger nuestra información.

## 2. REFERENCIAS

---

- [1]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protección de la información <https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion>
- [2]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Borrado seguro y gestión de soportes <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
- [3]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protección de la información – Ejemplo de matriz de clasificación de la información. <https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion#descargas>
- [4]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Copias de seguridad <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
- [5]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Control de accesos <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
- [6]. Incibe – Protege tu empresa – Blog – Ingredientes para un acuerdo de confidencialidad «exquisito». <https://www.incibe.es/protege-tu-empresa/blog/ingredientes-acuerdo-confidencialidad>
- [7]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Auditoria de sistemas <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
- [8]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plan director de Seguridad – Plantilla ejemplo para inventario de activos <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad>



INSTITUTO NACIONAL DE CIBERSEGURIDAD