

ÍNDICE

[1. Concienciación y formación 3](#_Toc480468901)

[1.1. Antecedentes 3](#_Toc480468902)

[1.2. Objetivos 3](#_Toc480468903)

[1.3. Checklist 4](#_Toc480468904)

[1.4. Puntos clave 5](#_Toc480468905)

[2. Referencias 6](#_Toc480468906)

# Concienciación y formación

## Antecedentes

El creciente uso de las nuevas tecnologías en las empresas hace indispensable la **concienciación** [[1]](#referencias) sobre los riesgos asociados a las mismas. Es necesario que los empleados conozcan y apliquen buenas prácticas en el uso de todo tipo de dispositivos (de escritorio, portátiles, móviles, pendrives,…) y soluciones tecnológicas (página web, servicios en la nube, redes sociales, correo electrónico,…) para lo cual debemos proporcionarles **formación** [[2]](#referencias) en ciberseguridad adecuada a su puesto ya que de este modo se pueden **prevenir** la mayoría de los incidentes.

Para alcanzar los objetivos fijados con esta política, será necesario el **compromiso** **total** por parte de la dirección, que ha de ser consciente que la formación debe ser una actividad continua que ha de repetirse y revisarse periódicamente, para que surta su efecto preventivo de incidentes y esté adaptada a las nuevas tecnologías que inevitablemente iremos utilizando.

## Objetivos

Asegurar que, en todo momento, los empleados **conocen, entienden y cumplen** las normas y las medidas de protección en materia de ciberseguridad adoptadas, advirtiéndoles de los **riesgos** que puede suponer un mal uso de los dispositivos y soluciones tecnológicas a su alcance.

## Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **concienciación y formación** en ciberseguridad.

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 | **Difusión de la política de seguridad**  Documentas y difundes las normas de ciberseguridad de tu empresa para que estén siempre accesibles. |  |
| B | PRO | **Concretar el plan de formación**  Elaboras o revisas el plan de formación para elevar el nivel de seguridad de tu plantilla. |  |
| B | PRO | **Programas de formación específicos**  Desarrollas y aplicas programas de formación en ciberseguridad adecuados a los distintos puestos de trabajo. |  |
| B | PRO | **Periodicidad de la formación**  Tus empleados realizan cursos o van a charlas de concienciación, cada \_\_\_\_\_\_\_\_\_\_. |  |
| B | PRO | **Evaluar el aprendizaje obtenido**  Compruebas la asimilación del conocimiento adquirido por tus empleados. |  |
| B | PRO | **Promover una cultura de seguridad de la información**  Promueves una cultura de seguridad de la información que abarca a toda la cadena de suministro de la empresa y a tus clientes. |  |

**Revisado por**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Fecha:** \_\_\_\_\_\_\_\_\_\_

## Puntos clave

Los puntos clave de esta política son:

* **Difusión de la política de seguridad.** Las normas de seguridad de la información de la organización deben estar correctamente documentadas y al alcance de todo el personal en todo momento.
* **Concretar el plan de formación.** Para garantizar el éxito de nuestro programa formativo, debemos seleccionar los aspectos que queremos que sean cubiertos:
  + procedimientos y controles de seguridad básicos;
  + necesidad de conocer y cumplir normas, leyes, contratos y acuerdos;
  + seguridad en el puesto de trabajo, aplicaciones permitidas, uso correcto de los recursos, propiedad intelectual, protección datos personales, etc.;
  + conciencias a los empleados sobre la existencia y peligros de la ingeniería social;
  + responsabilidad personal por acción u omisión y posibles sanciones.
* **Programas de formación específicos.** Es conveniente analizar si se deben desarrollar programas de formación y concienciación especializados [[4]](#referencias) para ciertos perfiles de empleados, tales como técnicos de soporte, administradores de sistemas, etc. Además, sería de gran utilidad elaborar una actividad formativa introductoria para los nuevos empleados.
* **Periodicidad de la formación.** Se debe establecer una periodicidad en las actividades formativas y de concienciación. De esta manera conseguiremos tener unos contenidos actualizados en materia de ciberseguridad y reforzaremos las debilidades detectadas o los mensajes de mayor importancia.
* **Promover una cultura de seguridad de la información.** Además de concienciar y formar a nuestros empleados en ciberseguridad, es conveniente exigir a las entidades externas [[3]](#referencias) que interactúan con nuestros sistemas de información que sus políticas de ciberseguridad estén alineadas con la nuestra. Intentaremos extender el plan de concienciación a la mayoría de nuestros proveedores y clientes.
* **Evaluar el aprendizaje obtenido.** Consideraremos la necesidad de realizar evaluaciones entre los empleados para determinar el grado de concienciación y formación que han alcanzado.

# Referencias

1. Incibe – Protege tu empresa – Kit de concienciación <https://www.incibe.es/protege-tu-empresa/kit-concienciacion>
2. Incibe – Protege tu empresa – Formación <https://www.incibe.es/protege-tu-empresa/formacion>
3. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Relación con proveedores <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
4. Incibe – Otras actividades – Formación especializada <https://www.incibe.es/formacion>

