CIBERSEGURIDAD PARA DIRECTIVOS NO TÉCNICOS

POLÍTICAS DE SEGURIDAD PARA LA PYME

Colección

PROTEGE TU EMPRESA

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. CIBERSEGURIDAD PARA DIRECTIVOS NO TÉCNICOS

1.1 ANTECEDENTES

Las ciberamenazas y ciberataques pueden afectar gravemente a la continuidad del negocio, dañar la reputación empresarial y provocar grandes pérdidas económicas, así como enfrentarse a graves sanciones. No es preciso ser un experto en ciberseguridad para prevenir estos riesgos, pero sí estar concienciado de su existencia y establecer ciertas reglas básicas de seguridad.

La dirección de una empresa juega un papel fundamental en ciberseguridad de la organización. Aunque no se disponga de conocimientos técnicos, se pueden tomar decisiones estratégicas que reduzcan significativamente los riesgos. En esta política se guiará al empresario no técnico para disponer de las nociones básicas para reducir los riesgos de su empresa en materia de ciberseguridad.

1.2 OBJETIVOS

- **Establecer** unas pautas prácticas de ciberseguridad fácil de seguir por empresarios y responsables de pequeñas y medianas empresas que no dispongan de un perfil técnico.
- **Proteger** la información de las empresas, los datos de los clientes, empleados y proveedores frente a pérdidas, robo o accesos no autorizados.
- **Integrar** la ciberseguridad como un pilar fundamental de la gestión diaria del negocio.

1.3 CHECKLIST

A continuación, se incluye una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al **uso de los dispositivos móviles corporativos.**

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	**Claúsulas contractuales.** Establecer en el contrato compromisos básicos del uso responsable de la información y los dispositivos	
B	PRO	**Acuerdos de confidencialidad.** Disponer de acuerdos de confidencialidad para los empleados y proveedores que tengan acceso a información de la compañía	
B	PRO/PER	**Formación en ciberseguridad.** Estar formado y formar a los trabajadores ayuda a fomentar una cultura de ciberseguridad	
B	PRO/TEC	**Revocación de permisos.** Establecer procedimientos cuando un empleado finaliza la relación laboral con la empresa	
A	PRO/TEC	**Control de accesos.** Mantener un control de los usuarios que acceden a qué tipo de información para evitar fugas de información	
B	PRO/PER	**Seguridad en el teletrabajo.** Medidas de seguridad para trabajar fuera de las instalaciones de la empresa	
B	PRO/PER	**Políticas de seguridad.** Crear y comunicar políticas de seguridad para reducir riesgos	
A	PRO	**Procedimientos de finalización de relación laboral.** A la hora de publicar usas el sentido común, teniendo en cuenta cómo puede afectar a la imagen	
B	PRO	**Políticas de sanciones.** Aplicar sanciones por incumplimiento de normas de seguridad	

Revisado por: _____ **Fecha:** _____

1.4 PUNTOS CLAVE

Los puntos clave de esta política son:

- **Cláusulas contractuales.** Incluir compromisos básicos sobre el uso responsable de la información y los dispositivos empresariales en los contratos laborales, tanto con empleados como con proveedores. Ayuda a dar a conocer a los empleados las políticas de uso del material e información de la organización para proteger los datos, asegurar la confidencialidad y garantizar el uso adecuados de los equipos y sistemas de la organización.

- **Acuerdos de confidencialidad**. Disponer de acuerdos de confidencialidad para los empleados y proveedores que tengan acceso a la información sensible de la compañía. Se debe disponer de un acuerdo de confidencialidad que debe ser firmados por dichos empleados. Es recomendable incluir en dicho documento los datos considerados confidenciales, las acciones permitidas sobre dicha información y las consecuencias de romper dicho acuerdo.

- **Formación básica en ciberseguridad** [1]. Aunque no se disponga de un perfil técnico se recomienda formarse a nivel básico de ciberseguridad para proteger los activos más importantes de la empresa. Para ello, se recomienda estar formado y lo más importante, formar a los empleados de la compañía mediante sesiones o vídeos explicativos que permitan al empleado conocer, por ejemplo, como identificar correos de phishing o generar contraseñas robustas para el acceso a las diferentes herramientas de la organización.

- **Control de accesos**. Mantener un control de las personas que acceden a qué recursos es imprescindible para evitar fugas de información, ya sean intencionadas o involuntarias. Se recomienda crear cuentas personalizadas y definir los niveles de acceso según el rol asignado dentro de la organización.

- **Seguridad en el teletrabajo** [3]. Muchas empresas optan por esta opción para sus trabajadores, por ello es necesario conocer que medidas aplicar para poder trabajar de manera segura fuera de las instalaciones de la empresa. Para ello es necesario contar con políticas y normas que definan al menos:
  - Uso de contraseñas robustas y administrador de contraseñas [4],
  - Uso de redes confiables, evitar uso de redes wifi públicas [5],
  - Mantener los equipos actualizados [6] y con antivirus,
  - No compartir el equipo de trabajo con terceras personas [7].

- **Aceptación de políticas**. Es fundamental disponer de políticas de ciberseguridad que reduzcan los riesgos. No obstante, es imprescindible comunicarlas a los empleados de la manera adecuada para que puedan comprenderlas y ponerlas en uso. Entregar, explicar y

1.4 PUNTOS CLAVE

hacer firmar un documento breve donde se expliquen las principales normas de seguridad de la empresa y ofrecer ayuda para aquellos empleados que tengan dudas sobre su uso es fundamental.

- **Política de sanciones**. Informar a los empleados que el incumplimiento de alguna de las normas de seguridad de la empresa conllevará sanciones. Compartir información sin permiso, instalar software no autorizado o permitir accesos a terceros puede incurrir en sanciones.

- **Finalización de contrato**. Cuando un empleado finaliza la relación contractual con la empresa es necesario:
  - Recoger todos los dispositivos propiedad de la compañía otorgados durante la relación laboral.
  - Eliminar los accesos a cuentas, correos, aplicaciones y archivos compartidos.
  - Reiterar el compromiso de confidencialidad incluso una vez finalizada la relación contractual.

- **Revocación de permisos**. Cuando se finaliza una relación o contrato laboral con un empleado es necesario desactivar sus accesos a los sistemas e información de la organización con la mayor celeridad posible desde su marcha. De esta manera se reduce el riesgo de uso indebido de la información.

2. REFERENCIAS

[1] INCIBE – [1]. – Empresas – Formación
https://www.incibe.es/empresas/formacion

[2] INCIBE – Empresas – Políticas
https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf

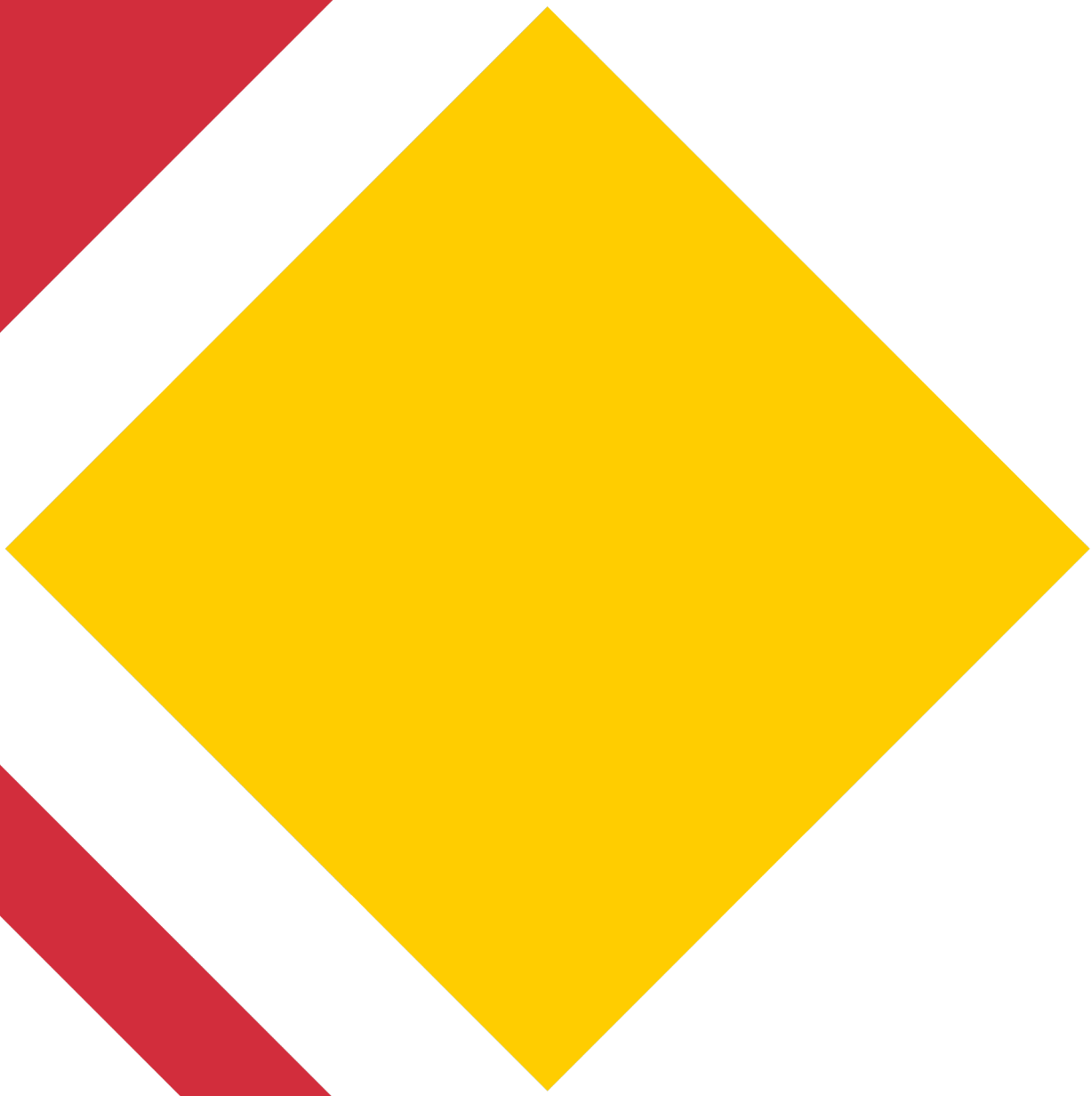
[3] INCIBE – Empresas – Guías
https://www.incibe.es/empresas/guias/ciberseguridad-en-el-teletrabajo-una-guia-de-aproximacion-para-el-empresario

[4] INCIBE – Empresas – Políticas
https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/2024/Contrase%C3%B1as_Pol%C3%ADtica%20de%20seguridad_2024.pdf

[5] INCIBE – Empresas – Políticas
https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/uso-wifis-y-redes-externas.pdf

[6] INCIBE – Empresas – Políticas
https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/actualizaciones-software.pdf

[7] INCIBE – Empresas – Políticas
https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-puesto-trabajo.pdf



Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa