Gestión de recursos humanos

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. GESTIÓN DE RECURSOS HUMANOS

1.1. Antecedentes

Es frecuente escuchar que «el eslabón más importante de la seguridad es el empleado», ya que evitar el error humano es clave para proteger nuestros sistemas y nuestra información. Por ello es importante, además de realizar la oportuna concienciación y formación [3] para fortalecer este eslabón, tomar medidas de seguridad en la gestión de los llamados «recursos humanos».

Una buena manera de garantizar que vamos a contar con una plantilla responsable en materia de ciberseguridad es establecer los oportunos **filtros, pruebas y controles** en la relación con nuestros colaboradores y empleados, especialmente en las **fases de firma** y **finalización del contrato**. En ambas fases se tendrán en cuenta aspectos tales como:

- qué requisitos y acuerdos relativos a la seguridad deben conocer, aceptar y cumplir;
- qué políticas internas deben aplicar: uso del correo corporativo, clasificación de la información, aplicaciones permitidas, uso del puesto de trabajo, etc.;
- qué formación que les vamos a proporcionar;
- cuáles son los procesos para darles de alta/baja en nuestros sistemas, etc.

1.2. Objetivos

Asegurar que todo el personal tiene conocimiento sobre los **derechos, deberes y responsabilidades** en relación a la seguridad de la información, haciendo hincapié en las posibles **sanciones** ante un acto negligente que ponga en riesgo los activos de información de la organización.

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 **gestión de recursos humanos**.

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	**Cláusulas contractuales** Reflejas en los contratos laborales de tus empleados los aspectos más importantes en materia de ciberseguridad.	☐
B	PRO	**Acuerdos de confidencialidad** Concretas en acuerdos de confidencialidad la manera de gestionar el acceso a la información más sensible.	☐
B	PRO	**Revisar las referencias de los candidatos** Revisas las referencias de los candidatos antes de su contratación en aquellos puestos que requieren acceso a información muy confidencial.	☐
B	PRO	**Plan de formación y concienciación en ciberseguridad** Mantienes concienciada y formada a tu plantilla en aspectos relacionados con la ciberseguridad.	☐
B	PRO	**Política de sanciones y expedientes** Informas a tus empleados de las sanciones que conlleva el uso negligente de la información de tu empresa.	☐
B	PRO	**Finalización del contrato** Comunicas a tus empleados las obligaciones que deben cumplir con la información de tu empresa al finalizar su contrato.	☐
B	TEC	**Concesión autorizada de los permisos de acceso** Concedes los permisos oportunos para garantizar que cada empleado solo accede a la información conveniente.	☐
B	TEC	**Revocación de permisos de acceso** Eliminas los permisos y cuentas de usuario de los empleados que finalizan su contrato.	☐

NIVEL	ALCANCE	CONTROL	
B	PER	**Aceptación de las clausulas y políticas de seguridad de la información** Lees, entiendes y firmas los acuerdos, clausulas y políticas relacionados con la seguridad de la información.	☐
B	PER	**Aprovechamiento de las sesiones formativas y de concienciación** Participas de manera activa en las sesiones formativas de la empresa en materia de ciberseguridad.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Cláusulas contractuales.** El empresario, con el departamento de recursos humanos, establecerán qué aspectos relevantes en relación a la seguridad de la información deben ser reflejados en el contrato de trabajo. Se considerarán todas las responsabilidades y derechos legales en lo relacionado con la propiedad intelectual [1] o con datos de carácter personal [2].
- **Acuerdos de confidencialidad.** Los empleados y colaboradores firmarán acuerdos relativos a la confidencialidad de la información de la empresa, que contendrán la siguiente información:
    - partes intervinientes;
    - qué información tendrá carácter confidencial;
    - compromisos por ambas partes;
    - posibles sanciones y legislación aplicable.
- **Revisar las referencias de los candidatos.** En ciertas ocasiones (sobre todo para puestos de especial criticidad o con acceso a información muy confidencial) detallaremos las comprobaciones a realizar antes de incorporar a algún candidato a la plantilla. Será necesario determinar las referencias que han de ser revisadas y qué datos del currículum tienen que verificarse. Además, indicaremos qué puestos concretos necesitarán una acreditación especial de estar libre de antecedentes penales.
- **Plan de formación y concienciación en ciberseguridad** [3]**.** Estableceremos las actividades oportunas para mantener a tu plantilla concienciada y formada en todo momento en aspectos relativos a la seguridad de la información.
- **Política de sanciones y expedientes.** Elaboraremos un procedimiento disciplinario formal que recoja las sanciones a aplicar en aquellos casos en los que se haya producido una negligencia en relación con la seguridad de la información (fuga o pérdida de datos confidenciales o sensibles, actuaciones intencionadas, ataques a la reputación en redes sociales, permitir ataques de terceros como infecciones por malware, etc.). Este procedimiento debe ser notificado a los empleados y estar accesible en todo momento.
- **Finalización del contrato.** Para evitar fugas de información es importante comunicar a los empleados las responsabilidades y obligaciones de seguridad y confidencialidad que deberán cumplir una vez finalizada la relación contractual [4].
- **Concesión autorizada de los permisos de acceso.** Si queremos garantizar que cada empleado solo acceda a la información oportuna, deberemos darle de alta en los sistemas de acuerdo con las políticas de control de acceso (físico y lógico) correspondientes [5]. En este punto, entre otras, realizaremos las siguientes acciones:
    - entregar las tarjetas de acceso físico;
    - asignar las cuentas de correo electrónico;
    - conceder los permisos de acceso a servicios, aplicativos y recursos compartidos;
    - asignar el puesto de trabajo, los dispositivos y equipos.
- **Revocación de permisos de acceso**. Del mismo modo que en su incorporación damos los accesos y permisos oportunos a los nuevos empleados para que puedan realizar su trabajo, al finalizar la relación contractual los revocaremos:

  - recogiendo las tarjetas de acceso y los dispositivos entregados;
  - eliminando sus cuentas de correo;
  - eliminando sus permisos de acceso a sistemas y aplicativos.

- **Aceptación de las clausulas y políticas de seguridad de la información.** Cada empleado de la empresa debe asegurarse de leer, comprender y firmar cada uno de los acuerdos, contratos, cláusulas y documentos de políticas relacionados con la seguridad de la información.
- **Aprovechamiento de las sesiones formativas y de concienciación.** Debemos aprovechar al máximo las posibles sesiones formativas y de concienciación [6] que la empresa ponga a disposición de los empleados. De esta forma nos aseguraremos de comprender los riesgos a los que se enfrenta la empresa en materia de ciberseguridad.

2. REFERENCIAS

[1]. BOE – Texto refundido de la Ley de Propiedad Intelectual https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

[2]. BOE – Ley Orgánica de Protección de Datos de Carácter Personal http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

[3]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Concienciación y formación https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[4]. Incibe – Protege tu empresa – Blog – La seguridad ante la rotación de personal en la empresa https://www.incibe.es/protege-tu-empresa/blog/seguridad-rotacion-personal-empresa

[5]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Clasificación de la información https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[6]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Cumplimiento legal https://www.incibe.es/protege-tu-empresa/herramientas/politicas