Control de acceso

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. CONTROL DE ACCESO

1.1. Antecedentes

Controlar quien **accede** a la información de nuestra empresa es un primer paso para protegerla. Es esencial que podamos decidir **quién** tiene permisos para acceder a nuestra información, **como**, **cuando** y **con qué finalidad** [1] [2].

A la hora de gestionar el control de acceso a nuestros datos debemos tener en cuenta que la información, los servicios y las aplicaciones utilizadas no tienen por qué ubicarse de manera centralizada en nuestras instalaciones, sino que pueden estar **diseminadas** en equipos y redes remotas propias o de terceros. También tenemos que considerar que cada vez es más habitual el uso de **dispositivos móviles** en los centros de trabajo. En ocasiones estos dispositivos son propiedad del propio empleado [3] lo que dificulta esta tarea.

Por otra parte el registro de los accesos en *logs* de los sistemas va a ser determinante para analizar los **incidentes de seguridad**.

1.2. Objetivos

Establecer **quien**, **como** y **cuando** puede acceder a los activos de información de la empresa y **registrar** convenientemente dichos accesos.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al **control de acceso**.

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	**Política de usuarios y grupos** Defines los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.	☐
B	PRO	**Asignación de permisos** Asignas los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso.	☐
B	TEC	**Creación/modificación/borrado de cuentas de usuario con permisos** Defines y aplicas un **procedimiento** para dar de alta/baja o modificar las cuentas de usuario.	☐
B	TEC	**Cuentas de administración** Gestionas las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.	☐
A	TEC	**Mecanismos de autenticación** Determinas e implantas las técnicas de autenticación más apropiados para permitir el acceso a la información de tu empresa.	☐
A	TEC	**Registro de eventos** Estableces los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de tu empresa.	☐
B	TEC	**Revisión de permisos** Revisas cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados.	☐
B	TEC	**Revocación de permisos y eliminación de cuentas** Desactivas los permisos de acceso y eliminas las cuentas de usuario una vez finalizada la relación contractual.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Política de usuarios y grupos.** Definiremos una serie de grupos que tendrán determinados accesos para cada tipo de información establecido. Esta clasificación se puede hacer teniendo en cuenta los siguientes aspectos:
  - en función del área o departamento al que pertenezca el empleado;
  - en función del tipo de información a la qué accederá;
  - en función de las operaciones permitidas sobre la información a la que se tiene acceso.

  En función de los criterios anteriores podemos establecer diversos perfiles de usuarios.
- **Asignación de permisos.** Una vez establecidos los tipos de información, los perfiles de usuarios y los grupos existentes, podremos concretar los tipos de acceso a la información a los que tienen derecho. Los permisos concretarán que acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el **mínimo privilegio** en el establecimiento de los permisos.
- **Creación/modificación/borrado de cuentas de usuario.** Para permitir el acceso real a los sistemas de información de la empresa debemos tener un **procedimiento** que permita gestionar la creación/modificación/borrado de las cuentas de acceso de los usuarios (por ejemplo: cuenta de correo, acceso al CRM, etc.) indicando quién debe autorizarlo. Detallaremos los datos identificativos de las mismas, las acciones que se permiten y las dotaremos de las credenciales de acceso correspondientes que deberán ser entregadas de forma confidencial a sus dueños. Se incluirán asimismo parámetros tales como la caducidad de las contraseñas y los procedimientos de bloqueo oportunos. Se debe informar al usuario de estos requisitos al entregarle las credenciales así como de la Política de contraseñas [4].
- **Cuentas de administración.** Las cuentas de administración permiten realizar cualquier acción sobre los sistemas que administran, por lo que deben ser gestionadas con la máxima precaución. Tendremos en cuenta los siguientes aspectos:
  - utilizar este tipo de cuentas únicamente para realizar labores que requieran permisos de administración;
  - implantar un control de acceso basado en un doble factor de autenticación;
  - registrar convenientemente todas sus acciones (registro de *logs*);
  - cuando accedemos a un sistema en modo administrador, este debe indicarnos claramente tal situación a través de su contexto;
  - el acceso como administrador debería ser notificado convenientemente;
  - evitar que los privilegios de las cuentas de administrador puedan ser heredados;
  - las claves de acceso deben ser lo más robustas posibles y ser cambiadas con frecuencia;
  - pueden ser sometidas a auditorías periódicas;
- **Mecanismos de autenticación** [4]**.** Definiremos e implantaremos los mecanismos de autenticación más adecuados para permitir el acceso a la información de nuestra empresa. Tendremos en cuenta aspectos tales como:

- utilizar mecanismos de autenticación internos o basados en servicios de autenticación de terceros (como la federación de identidades o el *social-login)*
- las tecnologías que utilizaremos:
  - autenticación vía web
  - servicios de directorio
  - LDAP
- factores de los mecanismos de autenticación (uno o varios):
  - algo que somos (a través de técnicas biométricas)
  - algo que sabemos (a través de contraseñas)
  - algo que tenemos (a través de dispositivos personales, *tokens* criptográficos)

- **Registro de eventos** [5]**.** Estableceremos los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa. Registraremos convenientemente quién accede a nuestra información, cuando, cómo y con qué finalidad.
- **Revisión de permisos.** Revisaremos periódicamente que los permisos concedidos a los usuarios son los adecuados.
- **Revocación de permisos y eliminación de cuentas.** Al finalizar la relación contractual con el empleado [6] es necesario revocar sus permisos de accesos a nuestros sistemas e instalaciones. Eliminaremos sus cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones. Además, exigiremos la devolución de cualquier activo de información que se le hubiese asignado (tarjetas de acceso o de crédito, equipos, dispositivos de almacenamiento, *tokens* criptográficos, etc.).

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog – «Como Pedro por su casa»: ¿a quién dejas acceder a tus sistemas? (1/2) https://www.incibe.es/protege-tu-empresa/blog/como-pedro-por-su-casa-01

[2]. Incibe – Protege tu empresa – Blog – «Como Pedro por su casa»: ¿a quién dejas acceder a tus sistemas? (2/2) https://www.incibe.es/protege-tu-empresa/blog/como-pedro-por-su-casa-02

[3]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de dispositivos móviles no corporativos https://www.incibe.es/protege-tu-empresa/herramientas/politicas

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

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

[6]. 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

INSTITUTO NACIONAL DE CIBERSEGURIDAD