Almacenamiento en la red corporativa

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. ALMACENAMIENTO EN LA RED CORPORATIVA

1.1. Antecedentes

Para poder disponer de un lugar común de trabajo donde almacenar el resultado de los trabajos individuales y poder compartir información entre los diferentes usuarios de la empresa se dispone de servidores de almacenamiento en red.

En la red corporativa es necesario distinguir entre información general de la empresa que deben utilizar todos los usuarios, e información de trabajo de los empleados almacenada en esta red corporativa. Los controles de acceso a esta información son definidos por la dirección y el responsable de sistemas, con el objetivo de limitar quién puede acceder y a dónde.

El contenido de la información almacenada se determina a través de una Política de clasificación de la información [1] que debe cubrir al menos los siguientes aspectos: tipo de información almacenada, momento de su almacenamiento y ubicación dentro de los directorios del sistema, además de las personas encargadas de la actualización de dicha información en caso de modificación. Se prestará una especial atención cuando la información haya sido catalogada como confidencial o crítica o si está sujeta a algún requisito legal.

Las empresas que necesitan almacenar gran cantidad de información utilizarán los sistemas de almacenamiento en redes del tipo *NAS* (*Network Attached Storage*), para archivos compartidos, o *SAN* (*Storage Area Network*) de alta velocidad para bases de datos de aplicaciones. Estos sistemas presentan un volumen de almacenamiento grande, ya que unen la capacidad de múltiples discos duros en la red local como un volumen único de almacenamiento.

1.2. Objetivos

Conseguir que los trabajadores hagan un buen uso de los servidores de almacenamiento disponibles para un óptimo tratamiento de la información.

Concienciar a los empleados de la relevancia de la información corporativa para un buen desempeño de su trabajo y de la necesidad de almacenarla en un sitio centralizado para evitar duplicidades y problemas de versiones, evitar pérdidas de documentos, centralizar las copias de seguridad, compartir información para la elaboración de proyectos y documentos, etc.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **almacenamiento en la red corporativa**.

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	**Inventario de los servidores de almacenamiento.** Informas a los empleados sobre los servidores de almacenamiento disponibles, la información que se comparte, qué datos deben almacenarse en ellos y las responsabilidades que conlleva.	☐
B	PRO	**Criterios de almacenamiento.** Informas a los empleados sobre los criterios de almacenamiento corporativos (qué se puede almacenar, quién tiene acceso y cuándo se elimina la información).	☐
B	PRO	**Clasificación de la información.** Informas al empleado sobre la necesidad de cumplir la política de clasificación de la información a la hora de almacenar y eliminar información en la red corporativa.	☐
A	PRO/TEC	**Control de acceso.** Estableces e implementas reglas de acceso que permiten llevar un control de quién tiene acceso y a qué discos/directorios.	☐
A	PRO/TEC	**Copias de seguridad.** Defines un plan de copias de seguridad en el que se detalla la información a guardar, cada cuanto tiempo se va a realizar, donde se va a almacenar y el tiempo de conservación de la copia.	☐

NIVEL	ALCANCE	CONTROL	
A	TEC	**Acceso limitado.** Permites el acceso a los empleados solo a los repositorios necesarios para el desempeño de su trabajo.	☐
A	TEC	**Almacenamiento clasificado.** Creas carpetas organizadas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Asignas los permisos de acceso pertinentes según el perfil del empleado.	☐
A	TEC	**Auditoría de servidores.** Revisas periódicamente el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.	☐
A	TEC/PER	**Cifrado de la información.** Cifras la información crítica almacenada en los servidores.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Inventario de los servidores de almacenamiento.** El empresario debe poner en conocimiento de los empleados cuáles son los servidores de almacenamiento disponibles en la red corporativa, la información que se comparte, qué datos deben ser almacenados en los mismos y las responsabilidades que conlleva. Esto se deberá reflejar en la formación de los nuevos empleados y refrescarse cada cierto tiempo.
- **Criterios de almacenamiento.** Tendremos que elaborar una normativa que establezca que la información debe almacenarse en la red corporativa teniendo en cuenta los siguientes aspectos:
  - qué información debe o no debe almacenarse en estos directorios;
  - las personas que tienen acceso a la información y si son encargadas su actualización en caso de necesidad de modificación;
  - cuándo es necesario eliminar la información por quedarse obsoleta.
- **Clasificación de la información.** El empleado debe conocer y cumplir la Política de clasificación de la información [1] a la hora de almacenar y eliminar información en la red corporativa. De esta forma se almacenará en la forma y lugar correctos.
- **Control de acceso.** Es esencial establecer implementar reglas de acceso que permitan llevar un control de quién tiene acceso y a qué directorios o sistemas de almacenamiento.
- **Copias de seguridad.** Ejecutaremos el plan de copias de seguridad [4] en el que se detalla la información a guardar, cada cuánto tiempo se va a realizar, dónde se va a almacenar y el tiempo de conservación de cada copia.
- **Acceso limitado.** Según lo establecido en la política de clasificación de la información [1] se definen perfiles de acceso (y se asignan a los usuarios) que limitan el uso de la información, de manera que cada usuario acceda solo a los directorios necesarios para el desempeño de su actividad laboral.
- **Almacenamiento clasificado.** Crearemos carpetas según la política de clasificación de la información para que el personal almacene la documentación donde corresponde. Se asignarán los permisos de acceso pertinentes según el perfil del empleado.
- **Cifrado de la información** [3]**.** Según la política de clasificación de la información, cifraremos la información crítica que se almacene en la red corporativa.
- **Auditoría de servidores.** Cada cierto tiempo, que especificaremos, tendremos que revisar el estado de los servidores: uso actual, capacidad, registros, estadísticas de uso, etc.

2. REFERENCIAS

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

[2]. Incibe – Protege tu empresa – Guías – Almacenamiento seguro de la información: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/almacenamiento-seguro-informacion-guia-aproximacion-el-empresario

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

[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 – Guías – Borrado seguro de la información: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/borrado-seguro-informacion-aproximacion-el-empresario

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

[7]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en dispositivos personales https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[8]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en dispositivos extraíbles https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INSTITUTO NACIONAL DE CIBERSEGURIDAD