Almacenamiento en la nube

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. ALMACENAMIENTO EN LA NUBE

1.1. Antecedentes

Son muchas las razones para almacenar información corporativa en la nube:

- acceder a la información desde cualquier dispositivo y lugar;
- ahorro de recursos y ahorro económico;
- proporciona directorios compartidos con distintos permisos de acceso;
- y permite el trabajo colaborativo sobre un documento.

Pero antes de su implantación en la empresa también deben valorarse sus aspectos negativos como la dependencia de terceros o la necesidad de conexión a internet para tener acceso a la información.

Para que los empleados hagan un buen uso de los recursos de almacenamiento, la empresa dispondrá de una Política de clasificación de la información [1] donde se debe indicar qué tipo de información puede subirse a la nube. Además se informará al personal sobre el contenido de la misma.

Junto a esta clasificación se elaborará una normativa interna para el tratamiento de la información crítica y sensible, que indicará cuándo debe ir cifrada y otras medidas de seguridad que le aplicarán como *backups* o borrado seguro de la información.

1.2. Objetivos

Establecer en qué casos se permite utilizar el almacenamiento en la nube y mantener de modo seguro la información almacenada en la nube, especificando reglas, criterios y procedimientos que deben seguir todos los empleados que usen estos servicios.

1.3. Checklist

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

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	**Uso de servicios de almacenamiento en *cloud* públicas.** Informas a los empleados sobre si se permite o se prohíbe el uso de servicios de almacenamiento en *cloud* públicas.	☐
B	PRO	**Lista de servicios *cloud* permitidos.** Elaboras una lista donde los empleados pueden consultar qué servicios de almacenamiento en *cloud* están permitidos y cuáles no.	☐
B	PRO	**Proceso de borrado de la información en la nube.** Informas al personal sobre el procedimiento de borrado adecuado para los repositorios de información en la nube.	☐
B	PRO	**Tipo de información almacenada y tratamiento.** Informas a los empleados del tipo de información que pueden almacenar en la nube y si necesita ser cifrada.	☐
B	PRO	**Copias de seguridad en la nube.** Valoras las ventajas e inconvenientes antes de almacenar tus copias de seguridad en la nube.	☐
A	PRO/TEC	**Contratación de servicios de almacenamiento en la nube.** Contratas un servicio de almacenamiento en *cloud* que cumple con los criterios organizativos y obligaciones legales de tu empresa.	☐
B	PRO/TEC	**Política de seguridad del proveedor.** Conoces la política de seguridad del proveedor de servicios de almacenamiento en la nube.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Uso de servicios de almacenamiento en *cloud* públicas** [2]**.** El empresario debe decidir si está permitido el uso de servicios de almacenamiento nube pública. El empleado no podrá utilizar este tipo de repositorios si así lo contempla la normativa de la empresa.
- **Lista de servicios de almacenamiento en *cloud* permitidos.** Es práctico elaborar y difundir una lista de los servicios de almacenamiento en *cloud* permitidos y prohibidos. De esta forma evitaremos el uso de servicios de almacenamiento que no consideremos seguros.
- **Proceso de borrado de la información.** Tendremos una Política de borrado de la información [3] que también debemos aplicar cuando se elimina información almacenada en la información en la nube.
- **Tipo de información almacenada** [4]**.** El empleado debe conocer qué tipo de información puede almacenarse en la nube (y cual no) y en qué casos tendrá que almacenarse cifrada. La política de clasificación de la información incluirá este dato.
- **Copias de seguridad en la nube.** Se han de valorar las ventajas e inconvenientes de realizar copias de seguridad [7] en la nube antes de realizarlas.
    - Ventajas:
        - Disponer de más espacio para realizar la copia de seguridad a medida que lo necesitemos.
        - La mayoría de los servicios en la nube realiza copias de seguridad como garantía de disponibilidad.
        - Disponer de una copia fuera de las dependencias de la empresa. En caso de que se produjera un incidente, nuestra información no se vería afectada y podríamos recuperarla.
    - Inconvenientes:
        - Depender de terceros que tendrán sus riesgos propios que pueden quedar fuera de nuestro control.
- **Contratación de servicios de almacenamiento en *cloud*.** A la hora de contratar un servicio de almacenamiento en *cloud* [5], tenemos que asegurarnos que cumple con los criterios de seguridad específicos que precisa la información que vamos a almacenar en la nube (garantía de confidencialidad, disponibilidad de la información, copias de seguridad, etc.), así como con las necesidades legales si se trataran de datos personales.
- **Política de seguridad del proveedor.** Antes de contratar servicios en la nube que traten información de la empresa debemos leer y comprender la política de seguridad del proveedor de servicios para asegurar que cumple todas nuestras necesidades [6].

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 – Razones para almacenar información corporativa en la nube https://www.incibe.es/protege-tu-empresa/blog/razones-almacenar-informacion-corporativa-nube
[3]. Incibe – Protege tu empresa – ¿Qué te interesa? – Políticas de seguridad para la pyme – Borrado seguro y gestión de soportes https://www.incibe.es/protege-tu-empresa/herramientas/politicas
[4]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protección de la información https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion
[5]. Incibe – Protege tu empresa – Blog – 12 preguntas de ciberseguridad que has de hacer antes de contratar servicios en la nube · https://www.incibe.es/protege-tu-empresa/blog/12-preguntas-seguridad-antes-contratar-cloud
[6]. 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
[7]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Copias de seguridad https://www.incibe.es/protege-tu-empresa/herramientas/politicas

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD