Copias de seguridad

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. COPIAS DE SEGURIDAD

1.1. Antecedentes

Los medios de almacenamiento contienen uno de nuestros **activos** más preciados: **la información**. Estos dispositivos pueden verse involucrados en situaciones como robos, incendios, inundaciones, fallos eléctricos, rotura o fallo del dispositivo, virus, borrados accidentales, etc. En estos casos nos sería imposible acceder a nuestra información, llegando a ponerse en peligro la **continuidad de nuestro negocio** [2].

La empresa debe realizar un **inventario de activos de información** y una **clasificación** [12] de los mismos en base a su criticidad para el negocio. El objetivo de esta clasificación es tener un registro de todo el software y los datos imprescindibles para la empresa de manera que sirva para determinar la periodicidad de los *backups* y su contenido.

La empresa identificará a los **responsables** de realizar los *backups* y de definir el **procedimiento para hacer las copias de seguridad y restaurarlas** [1] que incluirá:

- de qué hacer copia,
- el tipo de copia,
- el programa necesario,
- los soportes,
- la periodicidad,
- la vigencia,
- su ubicación,
- y las pruebas de restauración.

Así mismo se llevará un **control de los soportes** utilizados, se vigilará que sólo tiene **acceso personal autorizado** y que se destruyen los soportes de forma segura, en caso de tener que desecharlos. Los mismos criterios de seguridad serán aplicables en caso de hacer copias en la nube o en proveedores externos.

1.2. Objetivos

Verificar que se realizan copias de seguridad que **garantizan la continuidad de negocio**.

1.3. Checklist

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

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 activos de información** Mantienes un inventario de activos de información (software, datos, soportes, responsables, ubicación…) y los clasificas para identificar los necesarios (críticos) para reanudar el negocio en caso de desastre o incidente grave.	☐
B	PRO	**Control de acceso** Controlas el acceso a las copias de seguridad (sólo personal autorizado).	☐
B	PRO/TEC	**Copias de seguridad de la información crítica** Haces copias de seguridad de la información crítica corporativa, la exigida por la ley y la establecida en los contratos.	☐
B	PRO/TEC	**Periodicidad de las copias de seguridad** Las copias de seguridad se realizan cada _____.	☐
B	PRO/TEC	**Tipo de copia apropiada** Haces copias de seguridad completa, incremental o diferencial (elegir la adecuada para tu empresa).	☐
B	PRO/TEC	**Caducidad de las copias de seguridad** Conservas las copias de seguridad durante _____.	☐
A	PRO/TEC	**Ubicación de las copias de seguridad** Guardas al menos una copia completa fuera de la organización. Guardas las copias de seguridad en una caja ignífuga y bajo llave.	☐

NIVEL	ALCANCE	CONTROL	
A	PRO/TEC	**Copias en la nube** Tomas las medidas de seguridad (firmar ANS con el proveedor, cifrar las copias, comprobar la confidencialidad de los canales de transmisión) necesarias si almacenas tus copias en la nube.	☐
B	PRO/TEC	**Procedimientos de copia y restauración** Elaboras y aplicas los procedimientos de copia y restauración, revisándolos anualmente y con cada cambio importante en los activos de información.	☐
B	TEC	**Comprobar que las copias están bien realizadas y que pueden restaurarse** Compruebas cada _____ la fiabilidad de las copias verificando que pueden restaurarse.	☐
A	TEC	**Soporte de las copias de seguridad** Antes de hacer la copia revisas que el soporte es el adecuado (tasa de transferencia, capacidad,…) y que está en buen estado.	☐
B	TEC	**Control de los soportes de copia** Etiquetas los soportes para realizar las copias de seguridad y llevas un registro de los soportes sobre los que se ha realizado alguna copia.	☐
B	TEC	**Destrucción de soportes de copia** Cuando se desechan los soportes utilizados para copias de seguridad, los destruyes de forma segura.	☐
B	PER/TEC	**Cifrado de las copias de seguridad** Cifras las copias de seguridad que contienen información confidencial y la que subes a la nube.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Inventario de activos de información** [2]. El empresario, junto con los técnicos, han de identificar toda la información necesaria para reanudar el negocio en caso de desastre o de incidente grave. Se incluirá el software necesario y los datos críticos, los dispositivos que lo albergan, los responsables, la ubicación, etc.
- **Control de acceso.** Las copias de seguridad han de estar sometidas a un control de acceso restringido al personal autorizado.
- **Copias de seguridad de la información crítica.** Tendremos que verificar que hacemos copia de seguridad de la información crítica corporativa, de la exigida por la ley (por ejemplo por el RGPD) y de la establecida en los contratos con terceros.
- **Periodicidad de las copias de seguridad.** Fijaremos con cuanta frecuencia hacer las copias de seguridad teniendo en cuenta:
  - la variación de los datos generados;
  - el coste de almacenamiento [3];
  - y las obligaciones legales, por ejemplo el Reglamento General de Protección de datos [4] obliga a cualquier empresa que trate datos de carácter personal, a establecer procedimientos de actuación para la realización de copias de respaldo.
- **Tipo de copia apropiada** [5]**.** Decidiremos qué tipo de copia de seguridad es la idónea estimando los recursos y tiempo necesarios para llevarlas a cabo:
  - completa: se copian todos los datos a un soporte;
  - incremental: sólo se graban los datos que han cambiado desde la última copia;
  - diferencial: se copian los datos que han cambiado desde la última copia completa.
- **Caducidad de las copias de seguridad.** También debemos decidir cuánto tiempo conservar las copias en función de:
  - si la información almacenada sigue vigente;
  - la duración del soporte en el que realizan las copias;
  - la necesidad de conservar varias copias anteriores a la última realizada.
- **Ubicación de las copias de seguridad.** Es necesario buscar un lugar adecuado para guardar las copias, con los siguiente criterios:
  - cuenta con al menos una copia fuera de la organización;
  - no guardes *backups* con datos de carácter personal (datos de clientes o de empleados, por ejemplo) en casa;
  - valora contratar servicios de guarda y custodia según los datos que contienen.
- **Copias en la nube.** Si decides realizar tu copia en la nube [7] toma las siguientes precauciones para garantizar la seguridad de la información:
  - cifra la información confidencial antes de realizar la copia;
  - firma Acuerdos de Nivel de Servicios (ANS) con el proveedor, que garanticen la disponibilidad, integridad, confidencialidad y control de acceso a las copias;
  - considera el ancho de banda que necesitas para subir y bajar las copias.

- **Procedimientos de copia y restauración.** Se han de elaborar y aplicar procedimientos que describan cómo hacer las copias y cómo restaurarlas. De esta forma se minimiza el tiempo necesario de recuperación de los datos en caso de necesitar una restauración. Se han de revisar anualmente y con cada cambio importante del inventario de activos de información.
- **Comprobar que las copias están bien realizadas y que pueden restaurarse.** Fijaremos una periodicidad para realizar pruebas de restauración para garantizar que la información necesaria para la continuidad de negocio puede ser recuperada en caso de desastre.
- **Soporte de las copias de seguridad.** Decidiremos dónde hacer las copias teniendo en cuenta los siguientes aspectos:
    - coste, fiabilidad, tasa de transferencia y capacidad de los distintos soportes: discos duros externos, USB, cintas, DVD y la nube;
    - utiliza soportes que no estén obsoletos o en mal estado.
- **Control de los soportes de copia.** Tendremos que etiquetar e identificar los soportes dónde se realizan las copias de seguridad de manera que se pueda llevar un registro de los soportes sobre los que se ha realizado alguna copia. Así en el caso de tener que recuperar una información concreta, agilizaremos el proceso al poder consultar fácilmente en qué soporte se ha almacenado.
- **Destrucción de soportes de copia.** Cuando se desechan los soportes [9] utilizados para copias de seguridad debemos destruirlos de forma segura. Es muy importante asegurar que esta información nunca volverá a ser accesible para evitar posibles accesos malintencionados.
- **Cifrado de la información** Cifraremos la información [8] confidencial y la que requiera de almacenamiento en la nube. De esta manera protegemos los datos en caso de robo de información o accesos no autorizados.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog – Las 10 preguntas antes de hacer backup · https://www.incibe.es/protege-tu-empresa/blog/las-10-preguntas-clave-hacer-backup

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

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

[4]. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo · https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=es

[5]. Incibe – Protege tu empresa – Guía – Borrado seguro de la información: una guía de aproximación para el empresario inalámbricas · https://www.incibe.es/protege-tu-empresa/guias/almacenamiento-seguro-informacion-guia-aproximacion-el-empresario

[6]. Incibe – Protege tu empresa – Blog – Insistimos: ¡Haz copias de seguridad! (1/2) · https://www.incibe.es/protege-tu-empresa/blog/copias-seguridad-01

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

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

[9]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Borrado seguro y gestión de soportes https://www.incibe.es/protege-tu-empresa/herramientas/politicas

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

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

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD