Respuesta a incidentes

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. RESPUESTA A INCIDENTES

1.1. Antecedentes

Es un hecho que a pesar de las medidas que implantemos, siempre existe el riesgo de que ocurra un **incidente de ciberseguridad**. Por ello, debemos preparar un **plan de acción** [1 y 2] que nos indique cómo actuar de la manera más eficaz posible en estos casos.

Existen muchos tipos de incidentes de ciberseguridad [4], algunos son más habituales que otros que podrían encajar en una de las siguientes tipologías:

- incidentes no intencionados o involuntarios;
- daños físicos;
- incumplimiento o violación de requisitos y regulaciones legales;
- fallos en las configuraciones;
- denegación de servicio;
- acceso no autorizado, espionaje y robo de información;
- borrado o pérdida de información;
- infección por código malicioso.

Para ejecutar correctamente el plan y evitar que el daño se extienda se deben detallar las acciones a realizar en cada momento, la lista de las personas involucradas y sus responsabilidades, los canales de comunicación oportunos, etc.

Tras un incidente, si hemos aplicado el plan, tendremos una valiosa información para conocer y valorar los riesgos existentes, y así evitar incidentes similares en el futuro.

En caso de que ocurran incidentes graves o desastres que paralicen nuestra actividad principal, aplicaremos el **plan de contingencia y continuidad del negocio** [3].

1.2. Objetivos

Asegurarnos de que todos los miembros de la organización conocen y aplican un **procedimiento** rápido y eficaz para **actuar ante cualquier incidente** en materia de seguridad de la información. Este procedimiento incluirá medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa. También incluirá los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su **origen** y **evitar** que ocurran en un futuro.

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 **respuesta a incidentes** de ciberseguridad.

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	**Equipo responsable** Seleccionas el equipo que se encargará de gestionar los incidentes de ciberseguridad.	☐
B	PRO	**Mejora continua** Usas la información recogida en la gestión de los incidentes para adoptar mejoras en tus sistemas.	☐
B	PRO	**Caducidad del plan de gestión** Revisas cada _____ el plan de gestión y respuesta ante incidentes de ciberseguridad.	☐
B	TEC	**Detección del incidente** Concretas las situaciones que deben ser catalogadas como incidentes de ciberseguridad.	☐
B	TEC	**Evaluación del incidente** Categorizas convenientemente el incidente y le otorgas la criticidad correspondiente.	☐
B	TEC	**Notificación del incidente** Estableces correctamente la manera de notificar un incidente.	☐
A	TEC	**Resolución de incidentes** Desarrollas procedimientos detallados de actuación para dar respuesta a cada tipología de incidente de ciberseguridad.	☐
B	TEC	**Tratamiento del registro del incidente** Registras de forma conveniente toda la información relativa a la gestión del incidente.	☐
B	PRO	**Cumplimiento del RGPD** Tienes prevista la notificación de incidentes según el RGPD en caso de brechas de seguridad que afecten a datos de carácter personal.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Equipo responsable.** Para garantizar una respuesta eficaz durante el tratamiento de incidentes de ciberseguridad, nombraremos un equipo responsable de su gestión. Tendremos que considerar no solo al personal técnico encargado de su resolución (interno o externo), sino también personal de la dirección que debiera estar informado en todo momento del estado del incidente.
- **Mejora continua.** Es conveniente analizar la utilidad de usar la información recogida en la gestión de los incidentes para medir y evaluar la posibilidad de modificar procedimientos o añadir nuevas mejoras o controles para limitar futuros daños. Podemos realizar acciones preventivas con el fin de entrenar a la plantilla ante la aparición de un posible incidente [5].
- **Caducidad del plan de gestión.** Determinaremos la periodicidad con la qué debe actualizar el plan y las medidas a adoptar. También puede ser necesaria una actualización del plan tras un cambio significativo en nuestros sistemas.
- **Detección del incidente.** Debemos concretar las situaciones [6] que se considerarán incidentes. Desplegaremos herramientas con mecanismos de detección automáticos y estableceremos un sistema de alerta que nos informe detalladamente de lo sucedido en tiempo real.
- **Evaluación del incidente.** Una vez detectado el incidente debemos categorizarlo convenientemente [7] y establecer la gravedad y la prioridad en su tratamiento.
- **Notificación del incidente.** Procuraremos establecer un punto de contacto único donde los empleados deben notificar los posibles incidentes o puntos débiles detectados. Asimismo, se debe indicar la información a recabar y las acciones inmediatas a seguir en el momento de la notificación. Conviene tener un listado de contactos para actuar con rapidez en caso de incidente.
- **Resolución de incidentes.** Desarrollaremos y documentaremos procedimientos de respuesta para cada uno de los tipos de incidentes definidos previamente, poniendo especial énfasis en aquellos incidentes más habituales y peligrosos [8] [9]. Se detallarán al menos los procedimientos para las siguientes acciones.
    - recogida de evidencias tan pronto como sea posible tras la aparición del incidente, con cuidado de mantener la cadena de custodia, la integridad de las evidencias (cifrándolas si es necesario), soportes, etc.;
    - estimación del tiempo de resolución;
    - realización de un análisis forense en los supuestos requeridos;
    - escalado conveniente del incidente en caso de no poder ser solventado;
    - ejecución de acciones concretas para intentar reparar, mitigar o contener los daños causados por el incidente.
- **Tratamiento del registro del incidente.** Para disponer de toda la información acerca del incidente se registrarán convenientemente, almacenándose, entre otra, la información relativa a:
    - fecha y hora de aparición del incidente;
    - tipología y gravedad del mismo;
    - recursos afectados;
    - posibles orígenes;
    - estado actual del incidente;
    - acciones realizadas para solventarlo y quienes las ejecutaron;
    - fecha y hora de resolución y cierre del incidente.

- **Cumplimiento del RGPD**: El RGPD [10] obliga a notificar las violaciones de datos de carácter personal que podamos sufrir en la empresa a la autoridad de protección de datos competente y a las personas afectadas, salvo que sea improbable que suponga un riesgo para los derechos y libertades de los afectados.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog -¿Estás preparado para hacer frente a un ciberincidente? https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-ciberincidente

[2]. Incibe – Protege tu empresa – Blog -¿Qué camino debo seguir para gestionar correctamente un incidente de seguridad en mi empresa? https://www.incibe.es/protege-tu-empresa/blog/incidentes-seguridad-empresa

[3]. Incibe – Protege tu empresa – ¿Qué te interesa? – Plan de Contingencia y Continuidad de Negocio https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio

[4]. ENISA *Threat Taxonomy. A tool for structuring threat information* https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information/at_download/file

[5]. Incibe – Protege tu empresa – Formación – Juego de rol. ¿Estás preparado para ser atacado? https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad

[6]. Incibe – Protege tu empresa – Blog – 10 «síntomas» de dispositivos tecnológicos «enfermos» https://www.incibe.es/protege-tu-empresa/blog/10-sintomas-dispositivos-tecnologicos-enfermos

[7]. CERTSI – Taxonomía https://www.certsi.es/respuesta-incidentes/rediris/taxonomia

[8]. Incibe – Protege tu empresa – Blog – Cómo hacer frente a los 5 incidentes de ciberseguridad más comunes (1/2) https://www.incibe.es/protege-tu-empresa/blog/hacer-frente-los-5-incidentes-ciberseguridad-mas-comunes-12

[9]. Incibe – Protege tu empresa – Blog – Cómo hacer frente a los 5 incidentes de ciberseguridad más comunes (2/2) https://www.incibe.es/protege-tu-empresa/blog/hacer-frente-los-5-incidentes-ciberseguridad-mas-comunes-22

[10]. AGPD – Reglamento General de protección de datos http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php

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

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

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD