¿Estáis preparados?

Solución del Reto 3: fuga de información

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

R.3 Solución al RETO 3: fuga de información

Este es el material que se ha de entregar al equipo cuando hayan debatido sobre el incidente.

1.1 ¿Qué puedes hacer?

- Mantener la calma, evaluar la situación para valorar los daños y las causas, y así actuar en consecuencia. Consultar la Guía de Fuga de Información de Incibe para conocer las implicaciones y la forma de actuar en este caso.
- Identificar si ha habido una causa técnica, un error de procedimiento o una causa intencional (algún empleado interno) que haya permitido la fuga de información.
- Ponerte en contacto con la policía y con Incibe para saber qué podemos hacer y cómo actuar.
- Revisar si se está cifrando la información confidencial.
- Revisar los permisos de los antiguos empleados. Revocar los permisos de los colaboradores que ya no trabajan en la empresa.
- El soporte informático ayudará a investigar los accesos remotos a nuestros sistemas, presentando las copias de los registros de acceso a los sistemas (*logs*) para hacer la denuncia.
- Revisar si los colaboradores que ya no trabajan en vuestra empresa habían firmado acuerdos de confidencialidad, y podéis emprender acciones legales por esta parte.

R.3 Fuga de Información

- Para que no vuelva a ocurrir, adoptar medidas para proteger la información, su integridad, disponibilidad y confidencialidad:
  - clasificar la información para identificar la información confidencial y controlarla durante todo su ciclo de vida (desde que se crea o adquiere hasta su destrucción)
  - cifrar la información confidencial
  - establecer controles de acceso a la información:
    - crear grupos de acceso, en función del tipo de información a la que deben acceder;
    - establecer permisos específicos a cada uno de los grupos sobre la información, diferenciando entre los que solo deben consultar la información y los que la pueden modificar;
    - dar permisos sobre la información crítica de los directorios de los proyectos sólo a los empleados que realmente van a trabajar en ellos, con credenciales de acceso personalizadas y controladas;
    - establecer la periodicidad con la que se actualizarán los permisos asociados a los grupos y los componentes de los mismos;
    - diseñar un procedimiento de eliminación de permisos que nos permita, de forma rápida y ágil, revocar permisos sobre usuarios y grupos.
- Firmar acuerdos de confidencialidad con cada empleado y colaborador donde acepten, por escrito, las políticas internas de confidencialidad y seguridad, y las sanciones a las que se exponen en caso de incumplirse. Estos acuerdos se extenderán en el tiempo después de terminada la relación laboral/contractual.
- Registrar los *logs* de los sistemas de acceso remoto y hacer *backup* periódicos de los mismos.
- Incorporar medidas técnicas que detecten e impidan la fuga de información confidencial.

R.3 Fuga de Información

1.2 ¿Qué no debes hacer?

- Ocultar información que pueda estar relacionada con el problema.
- Intentar resolverlo tú sólo, sin buscar ayuda.
- Buscar culpables antes de analizarlo todo.
- No establecer control de acceso a los documentos confidenciales.
- No cifrar la información confidencial, no destruirla convenientemente o no aplicar los procedimientos sistemáticamente.
- No tener control sobre las cuentas de acceso a los colaboradores.
- No guardar registro de los accesos a los sistemas.
- Dar permisos a los servicios críticos de la empresa o de acceso a directorios con información confidencial de manera indiscriminada, a todos los usuarios.

1.3 Lecciones aprendidas: ¿cómo podrías evitarlo?

- Es importante realizar una clasificación para tener identificada la información confidencial. Así la podremos proteger adecuadamente (cifrado, control de accesos,...)
- Tenemos que analizar nuestros riesgos, pues está claro que esto puede ocurrir pero no debe volver a pasar, tenemos que tomar medidas.
- Siempre firmaremos acuerdos de confidencialidad con los empleados y colaboradores que hayan de manejar información confidencial. Estos acuerdos se extenderán más allá del contrato laboral.
- Hemos de estar preparados por si ocurre un incidente, es decir tener un procedimiento de gestión de incidencias que todo el mundo conozca para saber cómo actuar.
- Tenemos que tener a mano la lista de contactos de apoyo y de denuncia para estos casos.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL