MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

GUIA DE ACCIÓN ANTE INCIDENTES DE FILTRACIONES Y FUGA DE INFORMACIÓN

PROCESO DE GESTIÓN DE INCIDENTES

Octubre - 2023

TABLA DE CONTENIDO

1. FASE DE IDENTIFICACIÓN 5
2. FASE DE CONTENCIÓN 6
3. FASE DE MITIGACIÓN 8
4. FASE DE RECUPERACIÓN 9
5. FASE POST- INCIDENTE 10
6. LECCIONES APRENDIDAS 10
7. DIAGRAMA DE FLUJO 11

Concepto de filtraciones y fuga de información: Divulgación no autorizada o accidental de datos sensibles, confidenciales o privados, ya sea a través de medios digitales o físicos.

Detalles: la *filtración o fuga de información* se refiere a la divulgación deliberada o involuntaria de información confidencial a terceros no autorizados, es decir, ocurre la pérdida de confidencialidad de información privilegiada.

Estas filtraciones pueden ser el resultado de actividades maliciosas, como la piratería informática o el robo de datos, o pueden ocurrir debido a errores humanos, tales como enviar un correo electrónico o archivo adjunto al receptor equivocado, la pérdida de una memoria USB o el extravío de documentos importantes.

La información filtrada suele estar relacionada con datos de distinta índole, entre ellos datos de usuarios, datos de clientes, contraseñas, información interna de la organización, proyectos, cuentas bancarias, etc.

Los orígenes de las fugas de información pueden venir de dos factores distintos:

- ✓ **Internos:** cuando la fuga de información proviene de la propia organización. Puede deberse a un descuido o ser intencionado.
- ✓ **Externos:** cuando la fuga de información proviene del exterior de la empresa, ya sea por explotar una vulnerabilidad, por una mala configuración, etc.

Impacto: las filtraciones y fugas de información pueden tener graves consecuencias, tales como:

- ✓ **Pérdida de confianza**: la revelación de información privada puede llevar a una pérdida de confianza por parte de los clientes, socios comerciales o empleados, especialmente si se trata de datos personales o financieros.
- ✓ **Daño a la reputación:** las organizaciones que sufren este tipo de incidentes a menudo experimentan un daño significativo en su reputación, lo que puede afectar su imagen y credibilidad en el mercado.
- ✓ **Riesgo de robo de identidad:** la información personal filtrada puede utilizarse para el robo de identidad, lo que puede dar lugar a fraudes y pérdidas financieras para las personas afectadas.
- ✓ **Violación de la privacidad:** la divulgación no autorizada de información privada puede violar la privacidad de las personas y resultar en violaciones de leyes y regulaciones de protección de datos.

1. Fase de Identificación

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciber incidente que pueda sufrir un organismo o entidad, y notificarlo a la brevedad para tomar acciones ante el incidente.

Verificar la fuga de informacion y detectar su origen

- ✓ Utilizar soluciones de monitoreo de seguridad y sistemas de detección de amenazas para identificar actividades inusuales o patrones de tráfico sospechosos que puedan indicar una posible filtración o fuga de información.
- ✓ Confirmar la existencia y alcance de la filtración o fuga de información a través de análisis forenses y verificación de datos.
- ✓ Comunicar internamente a los equipos pertinentes, para coordinar la respuesta y garantizar una acción rápida.
- ✓ Notificar al equipo de seguridad, al personal de TI y a la alta dirección sobre la detección del incidente.
- ✓ Si se trata de datos personales o información sensible de clientes, proveedores o empleados, consultar las leyes y regulaciones aplicables para determinar los requisitos de notificación a las partes afectadas y a las autoridades de protección de datos.
- ✓ En caso de disponer de procedimientos de gestión de crisis, considerar la posibilidad de activarlos.

2. Fase de Contención

La máxima prioridad en esta fase es contener el impacto negativo que pueda sufrir la organización a causa del defacement.

Evaluación de la situación

- ✓ Recabar toda la información posible sobre la fuga de información. o Si aún está vigente, terminar las conexiones externas o internas relacionadas con la fuga de información.
- ✓ Determinar la criticidad y cantidad de la información revelada. En ocasiones, la información revelada puede encontrarse en la web y es de carácter público. En ese caso, no trascendiera como una fuga de información.
- ✓ Recopilar y analizar todos los logs de los sistemas donde se encuentra almacenada la información con el fin de determinar:
    - Cuando se produjo la fuga y si sigue vigente.
    - Cuánta información se ha filtrado.
    - Cómo se produjo.
    - Desde dónde se produjo:
        - En caso de tratarse de una filtración interna, determinar el equipo y cuenta de usuario empleada.

- Si es externa, determinar IP de origen, tiempos de conexión y geolocalización.

✓ Acotar las posibles causas de la fuga de información:

- Error en el software: determinar qué software ha fallado.
- Error humano: determinar si se ha producido por algún fallo humano o mala configuración.
- Premeditado: determinar si ha sido intencionado desde dentro de la organización.

✓ Comprobar la repercusión en los medios de comunicación: o Determinar el alcance de la publicación.

- Concretar la cantidad de información que se ha hecho pública.
- Estipular el impacto y cómo afecta a la organización
- Recabar toda la información posible.

✓ Documentar y recopilar pruebas, como registros de actividad, informes de rendimiento y cualquier otro dato relevante.

✓ Realizar copias de respaldo de la evidencia recopilada para su posterior análisis y referencia.

✓ Documentar los daños causados y las acciones tomadas para su posterior revisión y mejora.

Contención:

✓ Realizar una investigación exhaustiva para determinar la causa raíz del incidente.

- ✓ Identificar las vulnerabilidades o debilidades en las políticas, procedimientos o sistemas que permitieron la filtración.
- ✓ Implementar medidas correctivas y parches para cerrar las brechas de seguridad.

3. Fase de Mitigación

- ✓ Tomar acciones para terminar la fuga de información: o Restringir temporalmente el acceso a la información expuesta.
- ✓ Si es producto de un elemento software desactualizado, actualizar aquellos servicios que se encuentren vulnerables o desactualizados.
- ✓ Si existen evidencias de un acto premeditado por personal interno, contactar con RRHH de la organización.
- ✓ Si afecta a credenciales de usuario, revocar todas las cuentas afectadas y llevar a cabo un procedimiento para generar unas credenciales nuevas.
- ✓ Si los certificados o claves privadas PGP se han visto comprometidos, revocarlos y generar unos nuevos.
- ✓ En caso de afectar a terceros, notificar la situación a los afectados, qué información ha sido filtrada y, en caso de verse afectadas las credenciales, solicitar unas nuevas credenciales de acceso.
- ✓ Realizar comunicados internos y externos para controlar la repercusión mediática de la fuga de información.
- ✓ Determinar las posibles consecuencias económicas.

4. Fase de Recuperación

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante buscar cualquier signo de actividad sospechosa en los servicios afectados y monitorizarlos temporalmente.

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante buscar cualquier signo de actividad sospechosa en los servicios afectados y monitorizarlos temporalmente.

- ✓ En caso de disponer de un equipo legal, coordinarse con éste para tener en cuenta las posibles consecuencias legales y de reputación.
- ✓ En caso de que la información filtrada contuviese datos de carácter personal, notificar y tratar la filtración según la legislación vigente.
- ✓ Fortalecer las medidas de seguridad para prevenir futuras filtraciones o fugas de información.
- ✓ Incluir mejoras en la seguridad de los sistemas, políticas de seguridad más estrictas, capacitación del personal y el uso de soluciones de protección de datos más robustas.

5. Fase Post- Incidente

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

6. Lecciones aprendidas

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

- ✓ Realizar una revisión post-incidente para identificar las lecciones aprendidas y las áreas de mejora en las políticas y prácticas de seguridad.
- ✓ Actualizar los procedimientos y políticas de seguridad en función de las lecciones aprendidas y las mejores prácticas.

7. Diagrama de flujo