

	<b>RECOPIACIÓN DE EVIDENCIAS INCIDENCIAS</b>	IT-62-02
		Clasificación: Confidencial
		R00 27/01/2025

## 1. Propósito y Alcance

Este procedimiento cubre la identificación, recopilación, adquisición y preservación de evidencias relacionadas con incidentes de seguridad de la información dentro de la organización, para asegurar que la información recogida sea válida, mantenida en su integridad, y pueda ser utilizada en acciones disciplinarias o legales si fuese necesario.

El objetivo de este procedimiento es establecer un proceso coherente y controlado para la recopilación de evidencias, asegurando que las pruebas sean identificadas, recogidas, adquiridas y preservadas adecuadamente, respetando la cadena de custodia, la integridad de la evidencia y protegiendo los derechos de las personas involucradas. Esto permitirá a la organización tomar medidas correctivas, resolver incidentes de seguridad y asegurar que las evidencias puedan ser utilizadas en procedimientos legales si es necesario.


El alcance de esta política aplica a todos los sistemas, aplicaciones, infraestructura y servicios críticos gestionados por la organización, así como a los terceros que brinden servicios tecnológicos para **VIARIUM** que sirvan como evidencia para gestionar una incidencia.

## 2. Desarrollo

A pesar de las medidas que tenemos establecidas en **VIARIUM**, existen riesgos de que ocurran incidentes que pueden afectar a la seguridad de la información y no se refiera a un ataque de seguridad. Por ello, hemos preparado un plan de acción que nos indica cómo actuar de la manera más eficaz posible en estos casos.

Existen muchos tipos de incidentes que pueden afectar a la seguridad de la información, algunos son más habituales que otros. Por ello, se han identificado las siguientes amenazas:

- Entrada de malware en los sistemas
- Ataque cibernético
- Phishing
- Metodología no válida
- Ataque físico
- Boicot
- Robo de datos o metodología
- Fallo de los proveedores de servicio
- Correo electrónico u online meetings no seguros
- Fallo de comunicaciones
- Fallo de infraestructuras
- Borrado incompleto de datos
- Acceso no autorizado a un dispositivo
- Fallo de las medidas preventivas
- Fallo de hosting

	<b>RECOPIACIÓN DE EVIDENCIAS INCIDENCIAS</b>	IT-62-02
		Clasificación: Confidencial
		R00 27/01/2025

- Personal insuficiente
- Error de los recursos humanos en la operación
- Fallo eléctrico
- Siniestro Natural
- Dependencia excesiva de un solo proveedor
- Dependencia de servicios en la nube
- Implementación de IA o machine learning sin control adecuado

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

En caso de que ocurran incidentes graves o desastres que paralicen nuestra actividad principal, aplicaremos el **RE-068 Plan de Contingencias**.

### Objetivos

Aseguramos 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 incluye medidas para comunicar de forma correcta los incidentes a quien corresponda tanto dentro como fuera de la empresa. También incluye los mecanismos para registrar los incidentes con sus pruebas y evidencias con objeto de estudiar su origen y evitar que ocurran en un futuro.

También se incluirá la recopilación, adquisición, identificación y preservación de evidencias conforme a la cadena de custodia y la integridad de estas. Esto debe tener en cuenta la certificación de las herramientas y personal competente involucrado.

### Checklist

Incluimos una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la respuesta a incidentes de seguridad de la información.

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.


	<b>RECOPIACIÓN DE EVIDENCIAS INCIDENCIAS</b>	IT-62-02
		Clasificación: Confidencial
		R00 27/01/2025

- Personas (PER): aplica a todo el personal.


NIVEL	ALCANCE	CONTROL	
A	PRO	<b>Recopilación de evidencias</b> Se realiza de manera adecuada y oportuna, garantizando la preservación de la cadena de custodia y la integridad de estas. Se categoriza de manera adecuada la información y se emplean las herramientas aptas y personal certificado en el proceso. Las evidencias deben ser adquiridas conforme a los procedimientos establecidos.	<input type="checkbox"/>
B	PRO	<b>Equipo responsable</b> Selección del equipo que se encargará de gestionar los incidentes de seguridad de la información	<input type="checkbox"/>
B	PRO	<b>Mejora continua</b> Utilización de la información recogida en la gestión de los incidentes para adoptar mejoras en tus sistemas.	<input type="checkbox"/>
B	PRO	<b>Caducidad del plan de gestión</b> Revisamos cada 6 meses el plan de gestión y respuesta ante incidentes de seguridad de la información	<input type="checkbox"/>
B	PRO	<b>Caducidad de la documentación</b> Registramos y mantenemos un registro detallado de las evidencias durante el proceso de resolución del incidente, con la certificación de que la integridad y autenticidad de las evidencias se conservan. El proceso debe contar con auditorías periódicas que certifiquen la efectividad de la preservación.	<input type="checkbox"/>
B	TEC	<b>Evaluación del incidente</b> Categorizamos convenientemente el incidente y le otorgamos la criticidad correspondiente.	<input type="checkbox"/>
B	TEC	<b>Notificación del incidente</b> Establecemos correctamente la manera de notificar un incidente.	<input type="checkbox"/>
A	TEC	<b>Resolución de incidentes</b> Desarrollamos procedimientos detallados de actuación para dar respuesta a cada tipología de incidente de seguridad de la información.	<input type="checkbox"/>
B	TEC	<b>Tratamiento del registro del incidente</b> Registramos de forma conveniente toda la información relativa a la gestión del incidente.	<input type="checkbox"/>

### Puntos Clave

Los puntos clave de esta política son:

	<b>RECOPIACIÓN DE EVIDENCIAS INCIDENCIAS</b>	IT-62-02
		Clasificación: Confidencial
		R00 27/01/2025

- **Recopilación de evidencias.** Es importante tener una cadena de custodia donde se documente cada acción realizada sobre las evidencias desde su recolección hasta su análisis, asegurando que no se alteren ni manipulen de forma indebida. Debe haber protección física y lógica, se deben almacenar de forma segura y en lugares donde su acceso esté restringido a personal autorizado. Por último, cada evidencia debe registrarse detalladamente con fecha, hora, origen, descripción del incidente y responsables de su recolección. Siempre que la evidencia implique datos personales, la empresa debe asegurarse de que se notifique adecuadamente a los individuos afectados y que se obtenga el consentimiento necesario cuando corresponda. Si se recogen evidencias en diferentes ubicaciones (como en un entorno internacional), deben cumplirse las leyes locales de protección de datos y privacidad.
- **Equipo responsable.** Para garantizar una respuesta eficaz durante el tratamiento de incidentes de seguridad de la información, nombramos un equipo responsable de su gestión. Tenemos que considerar no solo al personal técnico encargado de su resolución, sino también personal de la dirección que debería estar informado en todo momento del estado del incidente. Dirección.
- **Equipo técnico:** debe estar capacitado en la gestión y preservación de evidencias, incluyendo conocimientos sobre la cadena de custodia, la protección de las personas involucradas y el uso de herramientas certificadas.
- **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 evitar futuros incidentes. Realizamos acciones preventivas con el fin de entrenar a la plantilla ante la aparición de un posible incidente. Esta mejora debe incluir la capacitación del personal involucrado en la recolección de evidencias y la revisión de los procedimientos de adquisición de evidencias.
- **Caducidad del plan de gestión.** Determinaremos la periodicidad con la que debe actualizar el plan y las medidas a adoptar. También puede ser necesaria una actualización del plan tras un cambio significativo en nuestros sistemas. Este plan debe incluir la evaluación continua de los mecanismos de recopilación y preservación de evidencias.
- **Caducidad de la documentación.** Las evidencias deben estar almacenadas durante el tiempo necesario para su análisis y procesamiento. La documentación relacionada con incidentes y evidencias debe tener una fecha de caducidad definida, tras la cual, debe ser eliminada o destruida de manera segura para que los datos no puedan ser recuperados o utilizados indebidamente.

	<b>RECOPIACIÓN DE EVIDENCIAS INCIDENCIAS</b>	IT-62-02
		Clasificación: Confidencial
		R00 27/01/2025

- **Detección del incidente.** Definimos las situaciones que se considerarán incidentes. Desplegamos herramientas con mecanismos de detección automáticos y establecemos un sistema de alerta que nos informe detalladamente de lo sucedido en tiempo real.
- **Evaluación del incidente.** Una vez detectado el incidente, lo categorizamos y establecemos la gravedad y la prioridad en su tratamiento. En el caso de robo o sustracción de un portátil, la gravedad es alta ya que dispone de información de la empresa y clientes. Por lo tanto, se activa rápidamente el protocolo de actuación.
- **Notificación del incidente.** El punto de contacto es avisar a Dirección de manera inmediata para poder desactivar los accesos a la información. Asimismo, se debe indicar la información a recabar y las acciones inmediatas a seguir en el momento de la notificación.
- **Resolución de incidentes.** Todo queda perfectamente documentado y registrado para hacer seguimiento y dar respuesta a este tipo de incidentes de manera inmediata.
  - 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 registra convenientemente, almacenándose, entre otra, la información relativa a:
  - fecha y hora de aparición del incidente;
  - tipología y gravedad de este;
  - 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.

La DIRECCIÓN, a 12 de febrero de 2025.