FICHA DE PROCEDIMIENTO

Código	E2.4.5-PRO-006	**Versión**	2
Nombre del Procedimiento	Gestión de Incidentes de Seguridad de la Información		

	Puesto	**Órgano, unidad orgánica, unidad funcional**
Elaborado por:	Coordinador/a de la Unidad Funcional de Calidad e Innovación	Unidad Funcional de Calidad e Innovación
Revisado por:	Jefe/a de la Oficina de Planificación y Presupuesto	Oficina de Planificación y Presupuesto
Aprobado por:	Gerente/a General	Gerencia General

Objetivo del procedimiento

Establecer las actividades a seguir para la gestión de incidentes de seguridad de la información dentro del OSINFOR.

Alcance del procedimiento

Aplica a todo el personal interno y externo del OSINFOR que tiene acceso a algún servicio o activo de información.

Base normativa

1) Ley N° 27444, Ley del Procedimiento Administrativo General y modificatorias, consolidada en el Decreto Supremo N° 004-2019-JUS, Texto Único Ordenado de la Ley del Procedimiento Administrativo General.
2) Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y modificatoria.
3) Decreto Legislativo N° 1085, Ley que crea el Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre y modificatorias.
4) Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
5) Decreto Supremo N° 024-2010-PCM, que aprueba el Reglamento del Decreto Legislativo Nº 1085 y modificado por Decreto Supremo N° 126-2019-PCM.
6) Decreto Supremo N° 029-2017-PCM, que aprobó el Reglamento de Organización y Funciones del OSINFOR.
7) Decreto Supremo Nº 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
8) Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.
9) Decreto de Urgencia N° 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento.
10) Resolución Ministerial N° 004-2016-PCM, Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
11) Resolución Presidencial N° 121-2018-OSINFOR, que aprueba la Política SIG-E1-POL-001-V.01 Política del Sistema Integrado de Gestión del Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre – OSINFOR.
12) Norma ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de la Información.

OSINFOR

Firmado digitalmente por: SANCHEZ SALDAÑA Sandra FAU 20522224783 soft
Motivo: Soy el autor del documento
Fecha: 21/12/2021 16:46:46-0500

Siglas y definiciones

- ISO: International Organization for Standardization (Organización Internacional de Normalización).
- MAPRO: Manual de Procedimientos.
- OSINFOR: Organismo de Supervisión de los Recursos Forestales y de Fauna Silvestre.
- SIG: Sistema Integrado de Gestión.
- SIGO: Sistema de Información Gerencial del OSINFOR.
- SGSI: Sistema de Gestión de Seguridad de la Información.

Para efectos del presente procedimiento, se aplican las siguientes definiciones:

1) **Activo:** Todo aquello que tenga valor para la Entidad y por lo tanto debe proteger.
2) **Amenaza:** Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.
3) **Debilidad de seguridad de la información:** Es una debilidad o fallo en un sistema que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.
4) **Evento de seguridad de la información:** Es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.
5) **Impacto:** Consecuencias que produce un incidente de seguridad de la información sobre la organización.
6) **Incidente de seguridad de la información**: Es un evento o serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una significativa probabilidad de comprometer las operaciones del proceso y amenazan la seguridad de la información.
7) **Incidente de seguridad digital**. Evento o serie de eventos que pueden comprometer la confianza, la prosperidad económica, la protección de las personas y sus datos personales, la información, entre otros activos de la organización, a través de tecnologías digitales.
8) **Mesa de Ayuda:** Es el canal autorizado para reporte y registro de eventos, debilidades e incidentes de seguridad de la información
9) **Punto de contacto:** Está compuesto por usuarios internos (servidores/as) y externos (proveedores/as, visitantes, administrados, etc.; que tengan acceso a los servicios y/o información del OSINFOR, quienes identifican debilidades, eventos o incidentes de seguridad de la información.
10) **Respuesta a Incidentes:** Se define así a las actividades de respuesta en forma sistemática, minimizando la ocurrencia, facilita una respuesta y recuperación rápida y eficiente, minimizando la pérdida de la información y la interrupción de los servicios.
11) **Vulnerabilidad:** Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.

Requisitos para iniciar el procedimiento

Descripción del requisito	Fuente
- Aparición de evento, debilidad o incidente de seguridad de la información.	- Comunicación realizada a través de la Mesa de Ayuda por usuarios internos. - Comunicación realizada por personal externo que visita las instalaciones del OSINFOR. - Centro Nacional de Seguridad Digital

Actividades			
N°	**Descripción de la actividad**	**Órgano, unidad orgánica, unidad funcional**	**Responsable**
1	Comunicar eventos, debilidades o incidentes de seguridad de la información detectados. Nota: Si usuario/a externo/a no tiene acceso a la Mesa de Ayuda, comunicar al área usuaria a la que esté prestando o de la cual recibe el servicio.	Todos	Punto de contacto
2	Revisar y clasificar evento, debilidad o incidente de seguridad de la información. ¿Es un evento, incidente o debilidad de seguridad de la información? NO: Ir a la actividad 3 SI: Ir a Actividad 4 Nota: Utilizar la tabla de tipos de eventos e incidentes de seguridad de la información. (Anexo 3)	Oficina de Tecnología de la Información	Gestor/a de Mesa de Ayuda
3	A5.3.1-PRO-00- 1 Gestión de Mesa de Ayuda de la OTI. (Fin del procedimiento)	Oficina de Tecnología de la Información	Gestor/a de Mesa de Ayuda
4	Notificar al Oficial de Seguridad y Confianza Digital y asignar especialista para atención.	Oficina de Tecnología de la Información	Gestor/a de Mesa de Ayuda
5	Determinar modalidad de tratamiento. ¿Es una debilidad? SI: Ir a la actividad 6 NO: Ir a la actividad 8	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
6	Resolver ticket de Mesa de Ayuda y generar Acción Correctiva o de Mejora	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
7	E2.4.5-PRO-002 - Acciones Correctivas y de Mejora del SIG (Fin del procedimiento)	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital

Actividades			
N°	**Descripción de la actividad**	**Órgano, unidad orgánica, unidad funcional**	**Responsable**
8	Evaluar y priorizar la atención del evento o incidente de seguridad de acuerdo al impacto. Nota: Utilizar la tabla de niveles de impacto precisada en el Anexo 4	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
9	Coordinar la atención con el/la responsable de solución. Nota: Extender la comunicación a usuarios involucrados de ser necesario.	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
10	Ejecutar e registrar acciones de contención. Nota: Utilizar las pautas para asegurar la evidencia digital, precisadas en el Anexo 5	Órgano Responsable	Especialista responsable de tratamiento
11	Coordinar con el personal involucrado, realizar análisis de causa y planificar acciones. ¿Es necesario escalar el incidente? SI: Ir a la Actividad 12. NO: Ir a la actividad 13. Nota: Equipo de Respuesta a Incidentes de Seguridad Digital para los incidentes de seguridad digital	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
12	Escalar el incidente y supervisar acciones. Nota: Utilizar la tabla de niveles de escalamiento precisada en el Anexo 4	Órgano Responsable	Especialista responsable de tratamiento
13	Implementar solución, recolectar evidencias y registrar todas las acciones tomadas.	Órgano Responsable	Especialista responsable de tratamiento
14	Comunicar la solución y resolver el ticket en la Mesa de Ayuda.	Órgano Responsable	Especialista responsable de tratamiento
15	Validar las acciones tomadas para tratamiento del evento o incidente. Nota: Validar que se tenga registrada toda la información asociada al evento o incidente en	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital

Actividades			
N°	**Descripción de la actividad**	**Órgano, unidad orgánica, unidad funcional**	**Responsable**
	la Bitácora de incidentes de seguridad de la información		
16	Evaluar necesidad de actualizar base de conocimientos. ¿Es necesario actualizar Base de Conocimientos? NO: Ir a la actividad 17 SI: Ir a la actividad 18 Nota: Cada mes evaluar la Bitácora de incidentes de seguridad de la información.	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
17	Cerrar ticket de Mesa de Ayuda. (Fin del procedimiento)	Oficina de Tecnología de la Información	Gestor/a de Mesa de Ayuda
18	Evaluar daños y determinar si hay lugar a sanción al personal. ¿Se requiere acción disciplinaria o administrativa? SI: Ir a actividad 19 NO Ir a actividad 20	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
19	Comunicar al órgano competente los daños ocasionados por el personal involucrado, adjuntando las evidencias respectivas Nota: URH: Personal OSINFOR UA: Proveedores y/o contratistas	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
20	Actualizar base de conocimientos para incidentes de seguridad de la información. Nota: En base a lecciones aprendidas del incidente presentado.	Unidad Funcional de Calidad e Innovación	Oficial de Seguridad y Confianza Digital
Fin del procedimiento			

Documentos que se generan
- Bitácora de Incidentes de Seguridad de la Información

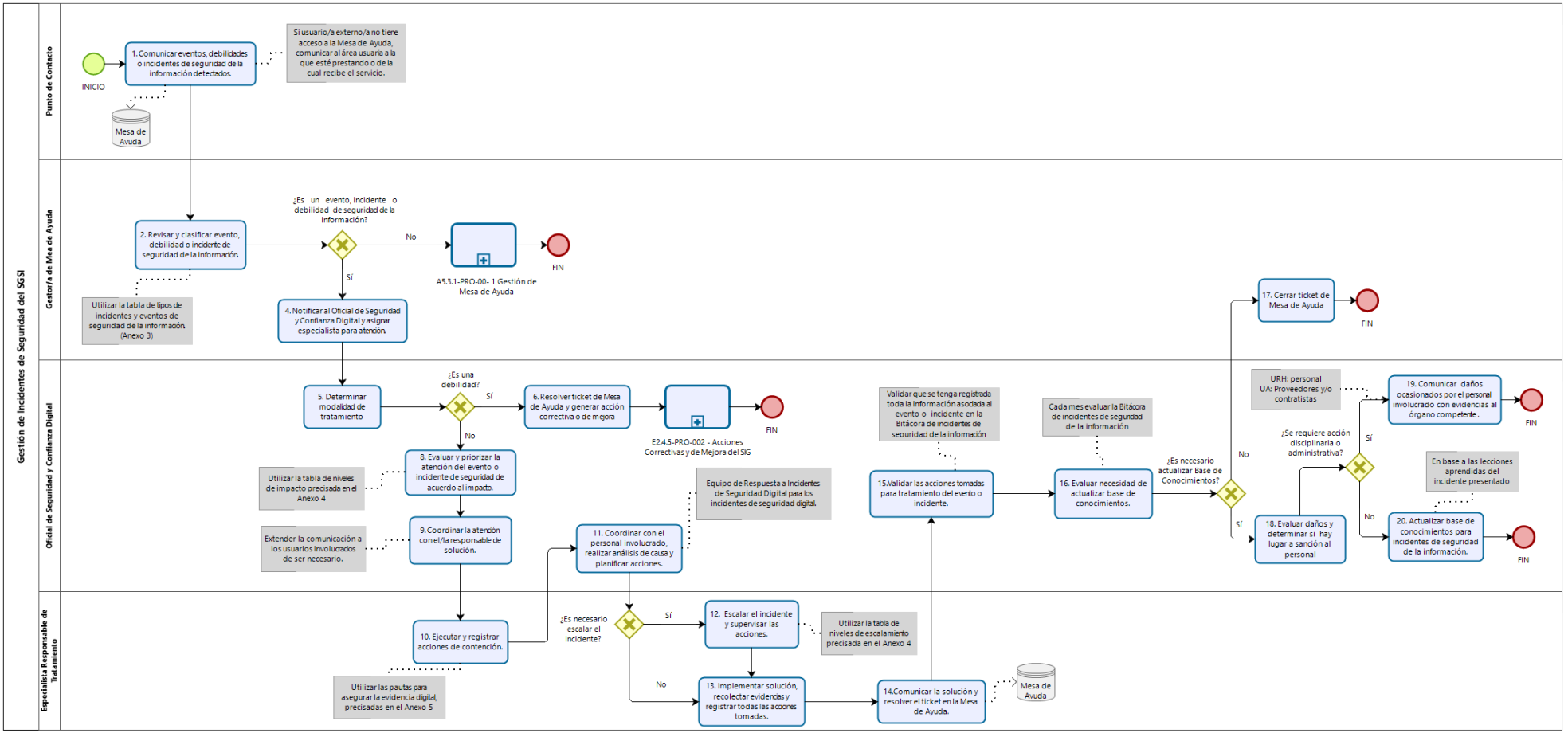
Proceso relacionado
E2.4.5 Implementación y mantenimiento de Sistemas de Gestión (ISO).

Sistemas informáticos:
Sistema de Mesa de Ayuda, correo electrónico

Anexos:
Anexo 1: Diagrama. Anexo 2: Formato Bitácora de Incidentes de Seguridad de la Información (E2.4.5-PRO-006-FOR-001-V.01). Anexo 3: Tipos de incidentes y eventos de seguridad de la información. Anexo 4: Niveles de impacto y escalamiento de eventos e incidentes de seguridad de la información. Anexo 5: Pautas para asegurar la evidencia digital en la atención de incidentes de seguridad de la información.

Nota:

Anexo 1: Diagrama



Anexo 2: Formato Bitácora de incidentes de seguridad (E2.4.5-PRO-006-FOR-001-V.01)

BITACORA DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

N° de Registro	N° mesa de ayuda	Descripción de Evento	Persona que Notifica	Fecha de Notificación	Clasificación Evento/incidente	Tipo de Evento	Breve Descripción del evento	Nivel de impacto del evento	Personal asignado para atender el Incidente	Causas del Incidente	Evidencias	Escalamiento	Solución	Fecha de Cierre	Lecciones Aprendidas
					Incidente			Alto							
					Evento			Medio							
					Incidente			Bajo							

Anexo 3: Tipos de eventos e incidentes de seguridad de la información

a) Tabla tipo de incidentes de seguridad

Clase de incidente	Tipo de incidente
Acceso no autorizado	Acceso a sistemas de información
	Acceso a instalaciones
Abuso de privilegios y usos inadecuados	Abuso de privilegios de seguridad
	Infracciones de derecho de autor
	Suplantación de identidad
	Uso indebido de cuentas de usuarios
	Vulneración de la integridad de la información
	Divulgación de información confidencial
Ataque informático	Ataque dirigido
	Modificación del sitio web
	Ataque de phishing e ingeniería social
	Ataque de intermediario(man-in-the-middle)
	Denegación de servicio (DDoS)
Código malicioso	Infección única de virus / malware
	Infección extendida virus / malware
Daños físicos	Daño físico a instalaciones
Pérdida de datos	Pérdida o robo de la información en medios físicos
	Pérdida de información en medios digitales
	Daño o deterioro de información física o digital
Pérdida masiva de servicio	Indisponibilidad del almacenamiento de datos
	Indisponibilidad del servicio de Internet
	Indisponibilidad del correo electrónico
	Indisponibilidad de sistemas de información
	Indisponibilidad del enlace de datos
	Indisponibilidad de la telefonía
	Indisponibilidad de servicios del Centro de Datos
	Indisponibilidad de la red de datos
Infracción de la LPDP	Incidente de datos personales
Pruebas y reconocimientos	Pruebas/detecciones no autorizadas

b) Tabla tipo de eventos

Evento	Tipo de evento
Eventos de seguridad de la información	Correo sospechoso
	Incumplimiento de políticas, normas y/o procedimientos sobre seguridad de la información que no hayan originado divulgación, pérdida o indisponibilidad de la información
	Falla temporal infraestructura de TI que no afecta la disponibilidad de servicios

Anexo 4: Niveles de impacto y escalamiento de eventos e incidentes de seguridad de la información

a) Tabla Niveles de impacto de eventos e incidentes de seguridad de la información

Nivel	Descripción
Alto	Interrumpe totalmente al menos uno de los procesos misionales, el evento puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos de información. Podría llegar a afectar más de un tipo de activo. • Amenaza la preservación de la integridad, confidencialidad o disponibilidad de la información. • Afecta el nombre de la entidad. • Pérdida o robo de información confidencial de la organización o de los usuarios en general. • Afecta infraestructura crítica para los procesos de la entidad. • Genera incumplimiento de normas legales o contratos.
Medio	Interrumpe parcialmente los procesos generales, el evento compromete un activo crítico. • Compromete el nombre de la entidad. • Afecta la integridad, confidencialidad o disponibilidad de la información generada por la entidad.
Bajo	No interrumpe los procesos generales de OSINFOR, el evento se detecta y se puede controlar fácilmente con recursos existentes en la entidad. • No afecta la integridad, confidencialidad o disponibilidad de la información de la entidad. • Impacta un número mínimo de activos de información que no son críticos.

b) Tabla Niveles de escalamiento de eventos e incidentes de seguridad de la información

Relevancia	Escalamiento
Alto	Se escala a los proveedores pertinentes y si es el caso a las autoridades externas competentes.
Medio	Apoyo del equipo técnico especializado de diferentes áreas en coordinación con el/la Oficial de Seguridad y Confianza Digital.
Bajo	Área involucrada en coordinación con el/la Oficial de Seguridad y Confianza Digital.

Anexo 5 - Pautas para asegurar la evidencia digital en la atención de incidentes de seguridad de la información

Para el caso en que se requiera evidencias (pruebas) con el fin de ejercer una acción disciplinaria y/o legal, debe preservarse la integridad y disponibilidad de la evidencia, para lo cual se establece una cadena de custodia y no se elimina ningún registro hasta que el incidente de seguridad de la información se haya cerrado. Se debe recolectar registros (logs) de auditoría y evidencias del evento con los siguientes fines:

a) Análisis del incidente.
b) Búsqueda de información.
c) Preservación de evidencia.
d) Evidencia en caso de incumplimiento con requerimientos contractuales, regulatorios o legales.

Se debe tener en consideración las siguientes pautas:

1. Durante la recolección de evidencias:
   a) Capturar una imagen del sistema tan precisa como sea posible.
   b) Realizar notas detalladas, incluyendo fechas y horas, e indicando si se utiliza horario local o UTC.
   c) Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
   d) Recoger la información según el orden de volatilidad (de mayor a menor).
   e) Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.

   Nota:
   - El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información, por lo que se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.
   - De acuerdo con esta escala se tiene la siguiente lista, en orden de mayor a menor volatilidad:
     i. Registros y contenido del caché.
     ii. Tabla de enrutamiento, tabla de procesos, estadísticas del kernel, memoria.
     iii. Información temporal del sistema.
     iv. Disco duro
     v. Logs del sistema.
     vi. Configuración física y topología de la red.
     vii. Documentos.

2. Acciones que deben evitarse para no invalidar el proceso de recolección de información:
   a) No apagar la computadora hasta que se haya recopilado toda la información que constituyan la evidencia.
   b) No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos. Se debe recopilar la información mediante programas desde un medio protegido.
   c) No ejecutar programas que modifiquen la fecha y hora de acceso de todos los archivos del sistema.

3. Consideraciones sobre la privacidad
   a) Es muy importante tener en consideración lo establecido en los acuerdos de confidencialidad en lo que a privacidad se refiere. El/La Oficial de Seguridad y Confianza Digital debe solicitar una autorización por correo electrónico o por escrito a quien corresponda para poder llevar a cabo la recolección de evidencias en el caso que se trabaje con información confidencial o de vital importancia para la organización, o que la disponibilidad de los servicios se vea afectada.
   b) No se debe dar la intromisión en la privacidad de los usuarios sin que se amerite una adecuada justificación. No se deben recopilar datos de lugares a los que normalmente no hay motivo razonable para acceder, como archivos personales, a menos que existan los indicios suficientes.

4. Consideraciones de almacenamiento y cadena de custodia
   a) La cadena de custodia debe estar claramente documentada, asimismo se deben detallar, en lo posible, los siguientes puntos:
      i. ¿Dónde?, ¿cuándo? y ¿quién? descubrió y recolectó la evidencia.
      ii. ¿Dónde?, ¿cuándo? y ¿quién? manejó la evidencia.
      iii. ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo? Y ¿cómo se ha almacenado?
      iv. En el caso de que la evidencia cambie de custodio, indicar cuándo y cómo se realizó el intercambio.
   b) Se debe almacenar la información en dispositivos cuya seguridad haya sido demostrada y que permitan detectar intentos de acceso no autorizados.