CAIGG

CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

Ministerio Secretaría General de la Presidencia

"Guía GASIC N° 9" - Mayo 2024

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°9

INTRODUCCIÓN A LA GESTIÓN DE INCIDENTES

ÍNDICE

Nota

PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°9: Introducción a la Gestión de Incidentes.

Esta guía es parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG) que busca fortalecer la posición del sector público en materias de Seguridad de la Información y Ciberseguridad, dotando de instrumentos a los Auditores Internos y Servicios Públicos de instrumentos y herramientas que permitan desarrollar un levantamiento de información en base a las mejores prácticas y la legislación vigente.

Santiago, Mayo 2024.

Daniela Caldana Fulss
Auditora General de Gobierno

Capítulo 1

INTRODUCCIÓN A LA GESTIÓN DE INCIDENTES

Los incidentes cibernéticos son capaces de causar daños demostrables a los intereses de seguridad nacional, las relaciones exteriores o la economía del pais, así como a la confianza pública, las libertades civiles o la salud y seguridad pública. Debido a este riesgo, todas las organizaciones e incluso los individuos deben tener estrategias claras y ejecutables para la detección, respuesta y prevención de incidentes cibernéticos. Los ciberataques están evolucionando y volviéndose cada vez más complejos y difíciles de detectar.

Fuente: CISA - Incident Detection, Response, and Prevention

Los ataques comprometen con frecuencia datos personales y empresariales, y es fundamental responder rápida y eficazmente cuando ocurren brechas de seguridad. El concepto de respuesta a incidentes de seguridad informática se ha aceptado e implementado ampliamente.

Nota Importante

Estrictamente hablando, **Seguridad de la Información y Ciberseguridad** son dos conceptos diferentes.

La **"Seguridad de la Información"** es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información en los activos de información, en cualquier medio (incluso, las personas); por otro lado **"Ciberseguridad"** hace referencia exclusiva al ciberespacio y activos digitales.

En esta guía adoptamos el concepto de "Seguridad de la Información y Ciberseguridad", pero para evitar la redundancia y el exceso de texto, utilizaremos los conceptos de "Seguridad de la Información", "Ciberseguridad" o el acrónimo "SIC" como sinónimos para mejorar la comprensión lectora.

Uno de los beneficios de contar con una capacidad de respuesta a incidentes es que permite responder de manera sistemática (es decir, siguiendo una metodología consistente de manejo de incidentes) para que se tomen las acciones apropiadas. La respuesta a incidentes ayuda al personal a minimizar la pérdida o el robo de información y la interrupción de servicios causados por los incidentes. Otro beneficio de la respuesta a incidentes es la capacidad de utilizar la información obtenida durante el manejo de incidentes para estar mejor preparado en la gestión de futuros incidentes y para proporcionar una protección más sólida a los sistemas y datos. Una capacidad de respuesta a incidentes ayuda a tratar adecuadamente los problemas legales que puedan surgir durante los incidentes.

Fuente: NIST 800-61r2

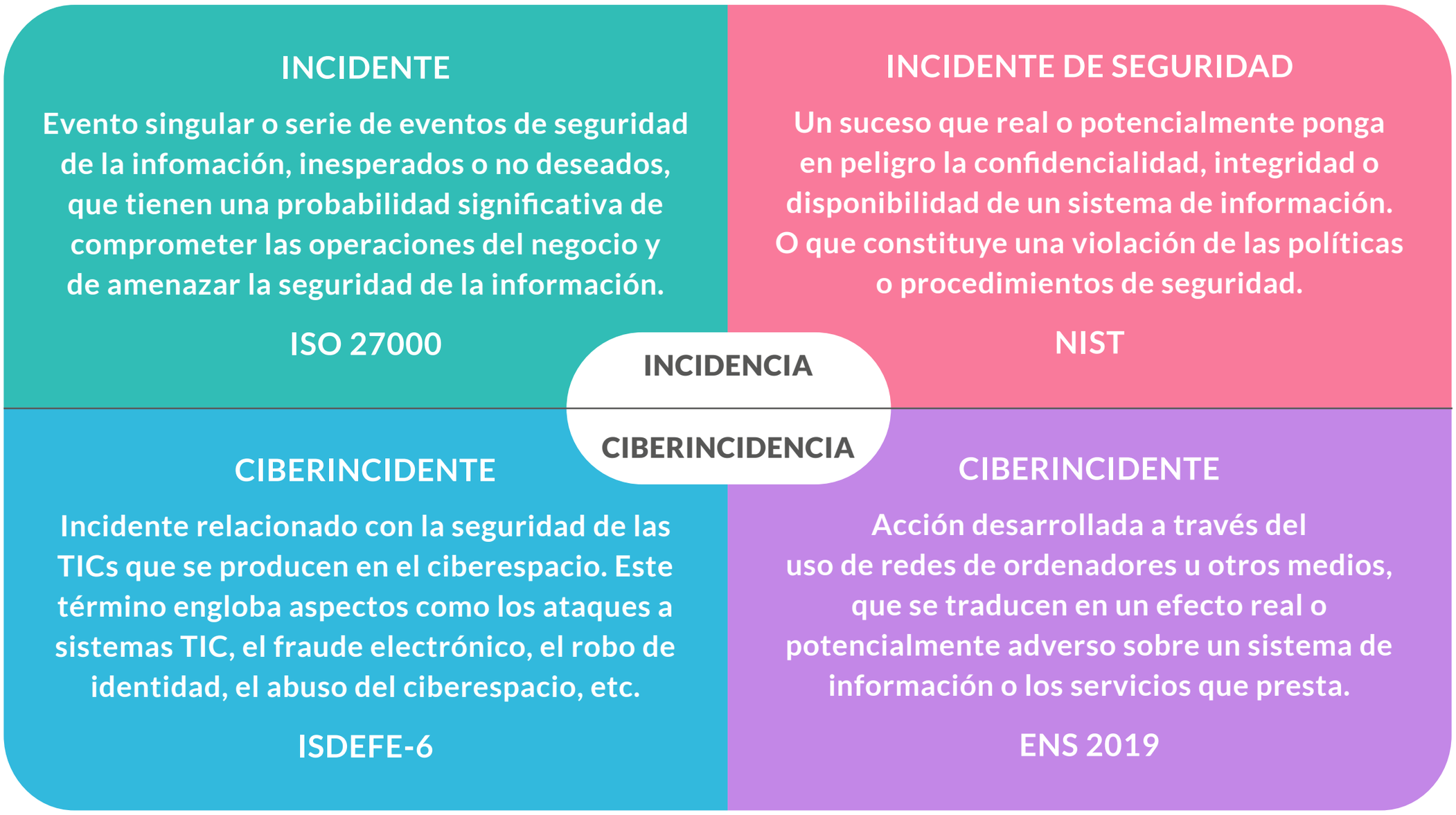
Conceptos Clave

Un **evento** es cualquier ocurrencia observable en un sistema o red. Los eventos incluyen un usuario conectándose a un recurso compartido de archivos, un servidor recibiendo una solicitud para una página web, un usuario enviando un correo electrónico y un firewall bloqueando un intento de conexión.

Los **eventos adversos** son aquellos que tienen consecuencias negativas, como caídas del sistema, inundaciones de paquetes, uso no autorizado de privilegios del sistema, acceso no autorizado a datos sensibles y la ejecución de malware que destruye datos.

Un **incidente de seguridad** informática es una violación o una amenaza inminente de violación de las políticas de seguridad informática, las políticas de uso aceptable o las prácticas de seguridad estándar.
Algunos ejemplos de incidentes son:

- Un atacante controla una botnet y envía un alto volumen de solicitudes de conexión a un servidor web, provocando que se bloquee.
- El usuario es engañado para abrir un "informe trimestral" enviado por correo electrónico que en realidad es malware; al ejecutar la herramienta, su computadora se infecta y se establecen conexiones con un host externo.
- Un atacante obtiene datos sensibles y amenaza con divulgar los detalles públicamente si la organización no paga una suma de dinero determinada.
- Un usuario proporciona o expone información sensible a otros a través de servicios de intercambio de archivos de tipo peer-to-peer.



Definiciones Base Desde ISO 27035

01 **Manejo de Incidentes *(Incident Handling)***
"Acciones de detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información".

02 **Respuesta a Incidentes *(Incident Response)***
"Acciones tomadas para mitigar o resolver un incidente de seguridad de la información, incluidas aquellas tomadas para proteger y restaurar las condiciones operativas normales de un sistema de información y los datos almacenados en él".

03 **Equipo de Respuesta a Incidentes *IRT***
Equipo de miembros de la organización debidamente capacitados y confiables que manejan incidentes durante su ciclo de vida.

1.1 POLÍTICA DE GESTIÓN DE INCIDENTES

La política de gestión de incidentes es un documento formal que establece las directrices que rigen la respuesta a incidentes. La política es una parte integral del marco de seguridad y debe ser personalizada para cada organización. Sin embargo, la mayoría de las políticas incluyen los mismos elementos clave.

Fuente: ISO 27035-2

Puntos Mínimos de la Política de Gestión de Incidentes según ISO 27035

Elemento	*Descriptor*
Compromiso de Gestión	La alta dirección debe apoyar las iniciativas establecidas en la política y asegurarse de que todos los miembros de la organización comprendan el valor y la importancia de una política eficaz y los procesos asociados en esta área. De hecho, cuando se produce un incidente, nadie debería tener alguna duda sobre el trabajo en línea y la importancia de la política con los requisitos.
Definición de un Incidente de Seguridad de la Información	De manera clara y sin ambigüedad. Cualquier persona de la organización debería poder identificar si un evento o un conjunto de eventos constituyen un incidente. Es vital tanto para elaborar informes precisos como para una respuesta efectiva.
Resumen de Procesos y Actividades para Detectar y Responder a Incidentes	---
Roles y Responsabilidades	Todos los involucrados en la organización deben comprender claramente sus roles y posición cuando se trata de identificar incidentes, informar incidentes y responder a incidentes.
Recopilación y Conservación de Registros	Durante el reporte, respuesta y análisis de un incidente, se generarán varios registros. Se debe dejar en claro lo que deberían ser registros, dónde se deben guardar los registros, el formato y la seguridad que se aplicará.
Formación y Sensibilización Ante Incidentes de Seguridad	En general, la conciencia de la seguridad de la información es fundamental para la postura de seguridad general de una organización. Una parte clave de este proceso de concienciación debe incluir la descripción clara de qué es un incidente y la importancia de informar el incidente al canal de denuncia correcto.
Referencia a Requisitos Legales, Reglamentarios y Contractuales	Asegurarse de que las personas involucradas en la gestión de incidentes comprendan las leyes y regulaciones pertinentes es fundamental para tener un proceso de gestión de incidentes eficaz. Algunas leyes/reglamentos requieren que los incidentes se aborden y se informen dentro de un plazo establecido. Desde un punto de vista contractual, las organizaciones pueden tener requisitos para informar o manejar incidentes en ciertos plazos por parte de los clientes.

1.2 PLAN DE RESPUESTA A INCIDENTES

El estándar NIST 800-61r2 define los componentes del plan de respuesta a incidentes que proporcione una hoja de ruta para implementar la capacidad de respuesta a incidentes. Cada organización necesita un plan que satisfaga sus requisitos únicos, los cuales están relacionados con la misión, el tamaño, la estructura y las funciones de la organización. El plan debe establecer los recursos necesarios y el apoyo de la gestión.
El plan de respuesta a incidentes debe incluir los siguientes elementos:

01	**Misión.**
02	**Estrategias y Objetivos.**
03	**Aprobación de la Alta Dirección.**
04	**Enfoque Organizacional para la Respuesta a Incidentes.**
05	**Manera en que el Equipo de Respuesta a Incidentes se Comunicará con el Resto de la Organización y Otras Organizaciones.**
06	**Métricas para Medir la Capacidad de Respuesta a Incidentes y su Efectividad.**
07	**Hoja de Ruta para Madurar la Capacidad de Respuesta a Incidentes.**
08	**Manera en que el Programa Encaja en la Organización en su Conjunto.**

La misión, estrategias y objetivos de la organización para la respuesta a incidentes deberían ayudar a determinar la estructura de su capacidad de respuesta a incidentes. La estructura del programa de respuesta a incidentes también debe discutirse dentro del plan.

Fuente: NIST 800-61r2

1.3 PROCESO DE RESPUESTA A INCIDENTES

Los procedimientos deben basarse en la política y el plan de respuesta a incidentes. Los procedimientos operativos estándar (SOP en inglés, conocidos también como Playbooks) son una delineación de los procesos técnicos específicos, técnicas, listas de verificación y formularios utilizados por el equipo de respuesta a incidentes. Los procedimientos operativos estándar deben ser razonablemente exhaustivos y detallados para garantizar que las prioridades de la organización se reflejen en las operaciones de respuesta. Además, seguir respuestas estandarizadas debería minimizar los errores, especialmente aquellos que podrían ser causados por situaciones estresantes durante el manejo de incidentes.

Estos procedimientos deben ser probados para validar su exactitud y utilidad, y luego distribuidos a todos los miembros del equipo.
Se debe proporcionar capacitación a los usuarios de estos documentos, y pueden utilizarse como herramienta instructiva.
La forma en la que se genera el flujo de trabajo para cumplir con estas tareas puede variar, a continuación, ejemplos:

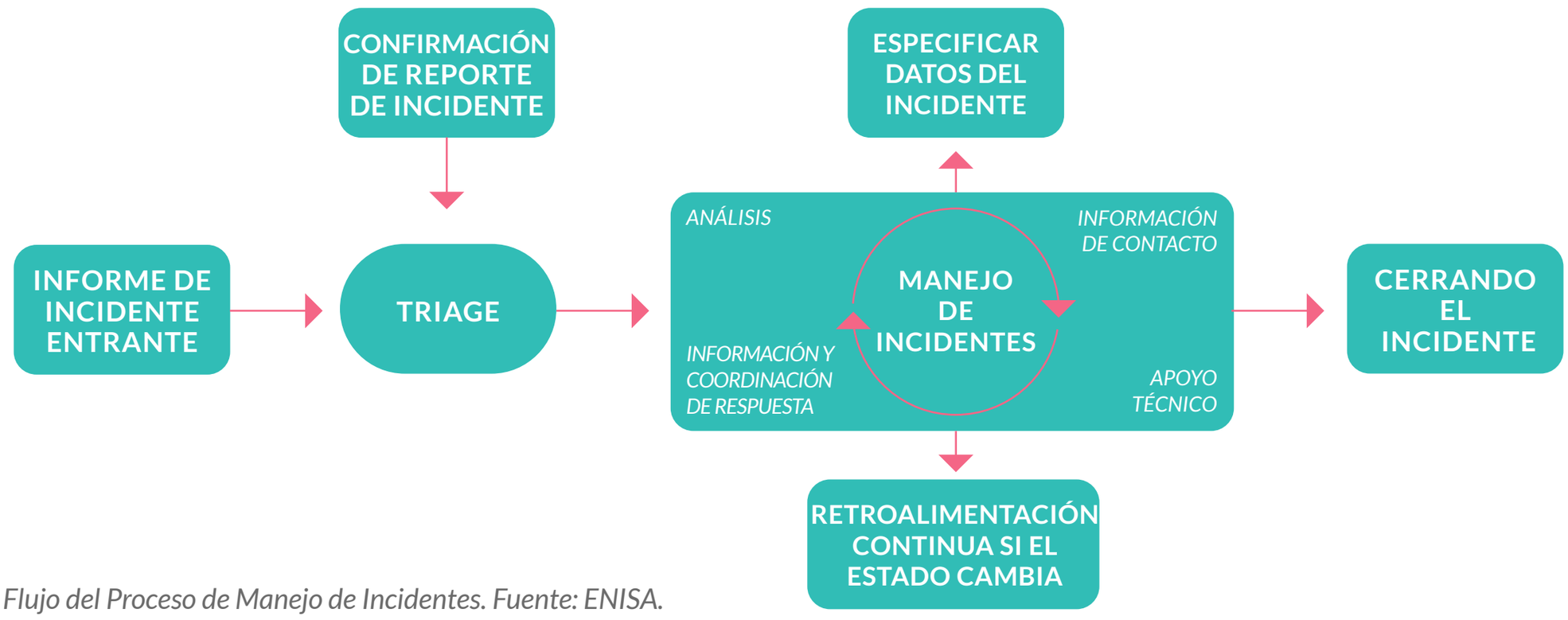


Figura 1: Flujo del Proceso de Manejo de Incidentes. Fuente: ENISA.

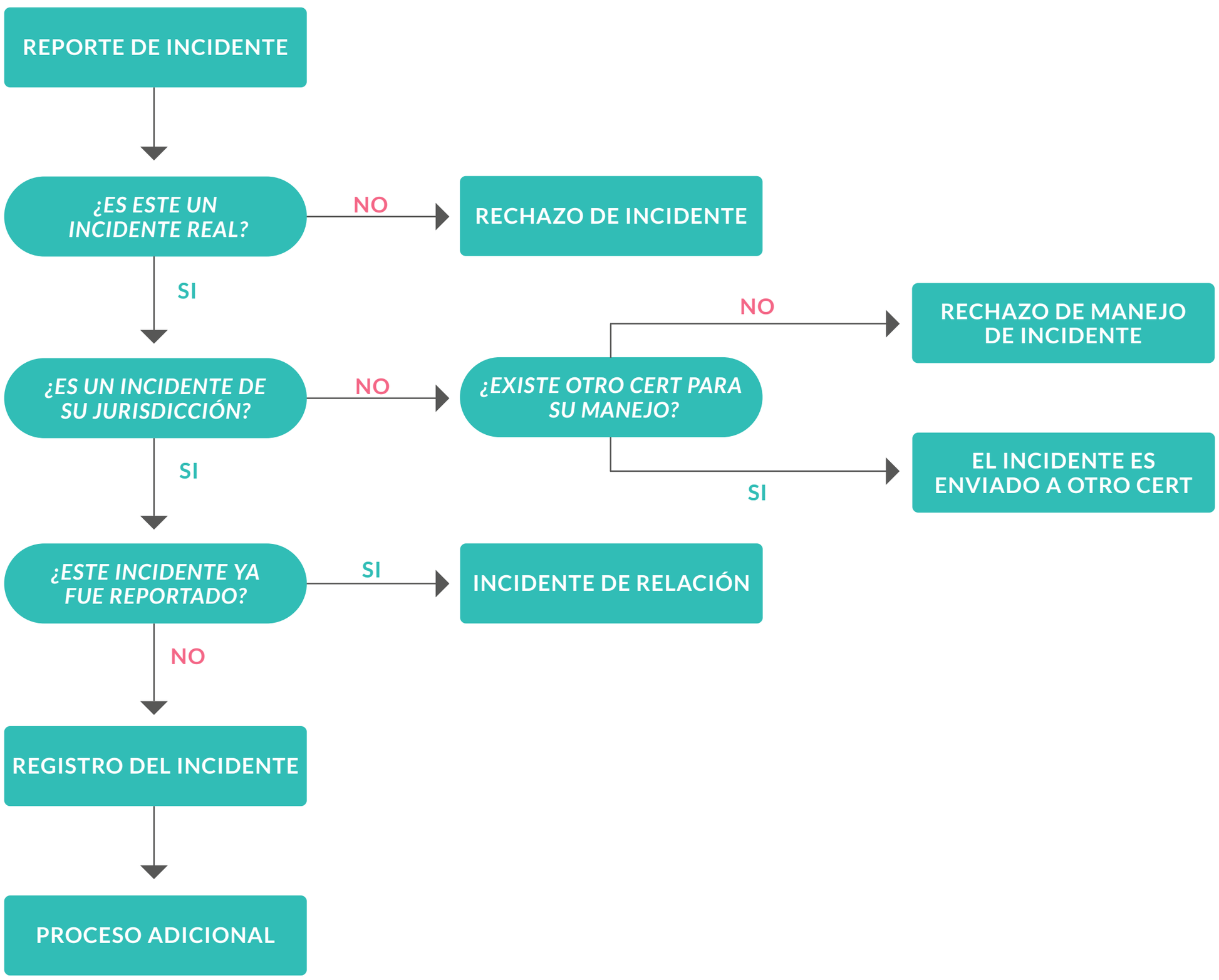


Figura 2: Parte de un Flujo de Trabajo Detallado para el Manejo de Incidentes. Fuente: ENISA.

Sin embargo, los procedimientos contra incidentes comparten elementos en común. Una organización popular de estas fases es: Preparar, Identificar, Contener, Erradicar, Recuperar y Aprender de los incidentes.

Fuente: ENISA Good Practice Incident Handling Playbook

Fase de Identificación

PREPARACIÓN

IDENTIFICACIÓN

CONTENCIÓN

ERRADICACIÓN

RECUPERACIÓN

LECCIONES APRENDIDAS

Esta fase tiene el propósito de verificar si ha ocurrido un incidente y determinar mayores detalles sobre este. Puede obtener reportes de posibles incidentes de los sistemas de información, usuarios finales u otras organizaciones. No todos los reportes corresponden a incidentes válidos. (Falsas Alarmas)

Acciones

- Asignar la propiedad de un incidente real o posible a un administrador de incidentes.
- Verificar que los reportes o eventos reunen los requisitos para considerarse incidentes.
- Establecer una cadena de custodia durante la identificación al manejar posibles evidencias.
- Determinar la gravedad de un incidente y escalarlo según sea necesario.

Fases de Contención, Erradicación y Recuperación

PREPARACIÓN
IDENTIFICACIÓN
CONTENCIÓN
ERRADICACIÓN
RECUPERACIÓN
LECCIONES APRENDIDAS

Una vez que se ha identificado y confirmado un incidente, el IMT se activa y se comparte la infomación del administrador de incidentes.

Acciones

- Activar al equipo de incidentes IMT / IRT para frenar el incidente.
- Notificar a las partes interesadas pertinentes que se hayan visto afectadas por el incidente.
- Obtener un acuerdo sobre acciones tomadas que pudieran afectar la disponibilidad del sevicio.
- Obtener y mantener evidencia.
- Documentar y generar respaldos de las acciones tomadas a partir de esta fase.
- Controlar y gestionar los comunicados RRPP enviados al publico.

PREPARACIÓN
IDENTIFICACIÓN
CONTENCIÓN
ERRADICACIÓN
RECUPERACIÓN
LECCIONES APRENDIDAS

Cuando se han aplicado medidas de contención, es tiempo para determinar la causa del incidente y erradicarla.

Acciones

- Determinar las señales y causas de los incidentes.
- Localizar la versión más reciente de respaldo (Backups) o soluciones alternas.
- Mejorar las defensas mediante la implementación de técnicas de protección.
- Realizar analisis de vulnerabilidad buscando nuevas amenazas que haya introducido la causa raiz.
- Eliminar la causa raíz. En caso de infección por gusano o virus, se puede eliminar aplicando los parches apropiados y software antivirus actualizado.

PREPARACIÓN
IDENTIFICACIÓN
CONTENCIÓN
ERRADICACIÓN
RECUPERACIÓN
LECCIONES APRENDIDAS

Esta fase garantiza que los sistemas o servicios afectados se reestablezcan a una condición específica de acuerdo al RPO. La limitación de tiempo hasta esta fase se documenta en el RTO.

Acciones

- Reestablecer las operaciones a su estado normal.
- Validar que las acciones tomadas sobre los sistemas restablecidos hayan sido exitosas.
- Involucrar a los dueños del proceso / sistema en la prueba al sistema.
- Facilitar a los duenos del proceso / sistema la declaracion de operacion normal.

Fase de Lecciones Aprendidas

PREPARACIÓN

IDENTIFICACIÓN

CONTENCIÓN

ERRADICACIÓN

RECUPERACIÓN

LECCIONES APRENDIDAS

Al final del proceso de respuesta a incidentes, siempre se debe elaborar un reporte para compartir lo que sucedió, las medidas que se tomaron y los resultados obtenidos luego de que se ejecutó el plan. Parte del reporte debe incluir las lecciones aprendidas que brindan al IMT y a otras partes interesadas, puntos de aprendizaje valiosos de lo que se pudo haber hecho mejor. Estas lecciones deben desarrollarse en un plan para mejorar la capacidad de gestión de incidentes y la documentación del plan de respuesta.

Acciones

- Redactar el reporte del incidente.
- Analizar los problemas encontrados durante el trabajo de respuesta a incidentes.
- Proponer mejoras con base en los problemas encontrados.
- Presentar el reporte a las partes interesadas pertinentes.

Fuente: ISACA CSX Cybersecurity Nexus.

1.4 COMUNICACIÓN DEL INCIDENTE

Las organizaciones a menudo necesitan comunicarse con partes externas con respecto a un incidente, y deben hacerlo cuando sea apropiado, como contactar a las autoridades, responder consultas de los medios y buscar experiencia externa. Otro ejemplo es discutir incidentes con otras partes involucradas, como proveedores de servicios de Internet (ISP), proveedores de software vulnerable u otros equipos de respuesta a incidentes.

	¿Cómo notificar un incidente de ciberseguridad al CSIRT de Gobierno? Coordinación Nacional de Ciberseguridad
01	Ingresa a https://csirt.gob.cl y haz clic en “Reportar Incidente” arriba a la derecha.
02	¿Necesitas ayuda para responder al incidente? Ingresa tu nombre, email y/o tu teléfono, para que te contacte un especialista del CSIRT. La ayuda puede ser remota y/o física, dependiendo de la gravedad del incidente y de la disponibilidad del equipo.
03	Completa el formulario con tus datos y los de tu institución:

- En "Nombre completo" ingresa tu nombre. Si deseas permanecer anónimo puedes solicitarlo más abajo.
- En "Correo electrónico" ingresa tu dirección de correo. Si estás reportando un incidente ocurrido a tu organización, coloca el email institucional; si no trabajas ahí, pon tu email personal. (Dato obligatorio).
- En “Entidad de la persona que reporta” registra el nombre de la institución donde trabajas.
- En "Teléfono" pon el número de teléfono donde puedes ser contactado o contactada.
- En “Institución afectada”, identifica el nombre de la institución afectada por el incidente. (Dato obligatorio)
- En “Mensaje” escribe toda la información que tengas sobre el incidente, en el momento en que estés reportando:

  ¿No tienes mucha información? No importa, luego puedes ampliar la información en un segundo reporte.

  Incluye toda la información que tengas sobre el sistema afectado:
  ¿Es un sistema expuesto a Internet? Ingresa la IP del sistema, aunque el sistema esté actualmente abajo.
  ¿No sabes la IP? Coloca la URL del sitio web que afectado.
  ¿No es un sitio web? Registra lo que sepas sobre qué sistemas o aplicaciones fueron afectadas.

- Finalmente, si podemos confirmar tu notificación y deseas que tu nombre sea publicado en nuestro "Muro de la Fama", marca el checkbox debajo del título "Muro de la Fama".
- Para enviar la notificación, debes hacer click en el botón de verificación de Cloudflare ("Verify you are a human"). Luego, haz click en "Enviar reporte" y enfócate en seguir respondiendo a la emergencia.

CSIRT Equipo de Respuesta ante Incidentes de Seguridad Informática

Capítulo 2

CÓMO UTILIZAR LA GUÍA PARA LA AUDITORÍA INTERNA

2. CÓMO UTILIZAR LA GUÍA PARA LA AUDITORÍA INTERNA

Para que el auditor interno pueda aprovechar al máximo esta publicación, es conveniente que se refiera a los instrumentos complementarios: Las preguntas de auditoría temáticas y el modelo de madurez general. Cada GASIC se compone de tres componentes:

Guía de Auditoría de la Seguridad de la Información y Ciberseguridad (GASIC):
Este es el cuerpo teórico y consiste en el marco contextual necesario para que el auditor interno comprenda el alcance y del dominio de seguridad que está evaluando. Es un instrumento con los conceptos fundamentales recopilados de mejores prácticas.

Modelo de Madurez:
Recopila controles desde las mejores prácticas asociadas al tema central de Guía de Auditoría, organiza los controles en una propuesta de madurez y permite al auditor conocer los requisitos que debería evaluar.

Ejemplos de Preguntas de Auditoría:
Complementa el modelo de madurez a través de una serie de preguntas organizadas en varios documentos. Cada documento representa un control que pertenece a uno de los ejes temáticos definidos al interior de la Guía de Auditoría.

La ilustración a continuación presenta esta estructura documental:

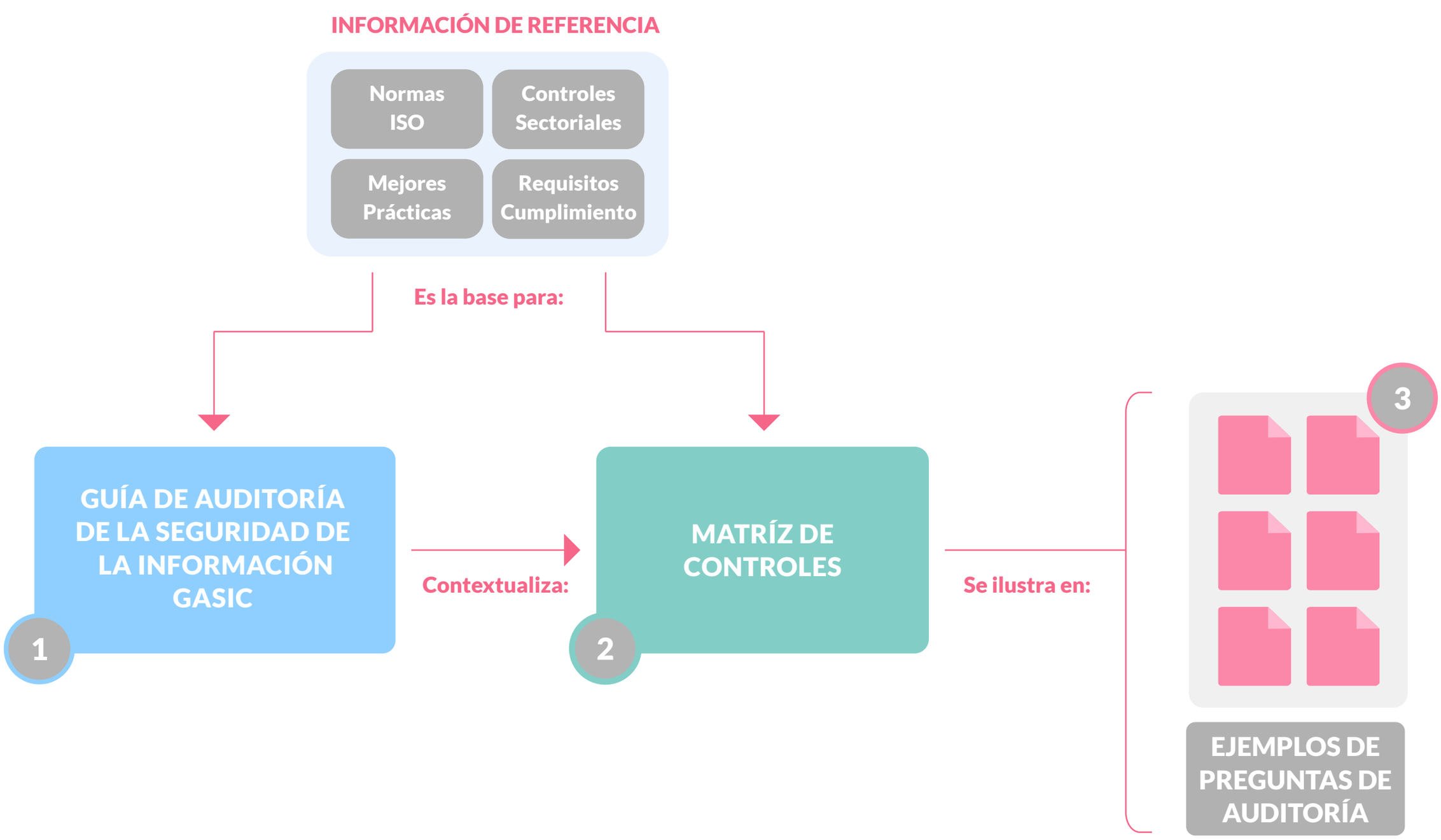


Ilustración n°5. Modo de uso y Estructura Documental GASIC. Fuente: Elaboración Propia

El método de trabajo sugerido es el siguiente:

01 **El auditor interno debe estudiar cada Guía de Auditoría y su contexto para tener plena comprensión del tema a trabajar.**

02 **A continuación, puede utilizar el Modelo de Madurez para seleccionar los controles que sean apropiados para la organización. La selección de controles debe estar alineados con:**

- **a. La estrategia de la organización.**
- **b. Los resultados de la evaluación de riesgos.**
- **c. Los requisitos de cumplimiento.**
- **d. La estrategia de auditoría interna, expresada en el plan.**

03 **Por último, puede utilizar los documentos de ejemplo para la planificación de las preguntas y pruebas que fuese a realizar. El formato del programa, plan, instrumentos, pruebas y reportería debe ser aquel solicitado en el contexto de cada auditoría, que está fuera del alcance de esta guía.**

NOTA

Los ejemplos de pruebas tienen como propósito ilustrar la forma en la que los requisitos de los marcos que se encuentran en el matriz de controles. El auditor puede elegir utilizar un conjunto de estos ejemplos o diseñar sus propias pruebas para evaluar el nivel de cumplimiento de cada control.

En ningun caso, los ejemplos pretenden ser una lista completa; recuerde, debe contextualizar el ejercicio a la realidad de su organización.

Eje temático

Gestión de Incidentes de Seguridad : Este eje tiene por objetivo establecer el procedimiento de gestión de incidentes de seguridad, considerando las mejores prácticas de seguridad.

	CONTROL	DESCRIPTOR
1	**Capacitación y Concientización**	**La organización define y opera un proceso de capacitación y concientización que permita a todos los miembros de la organización conocer su rol frente a un incidente de seguridad.**
2	**Comunicación con Terceros**	**La organización establece mecanismos de comunicación con todas las partes interesadas relevantes para notificar el inicio y el cierre de un incidente de seguridad.**
3	**Contención, Erradicación y recuperación**	**La organización establece actividades que permitan detener la interrupción en sus sistemas, las controla y optimiza.**
4	**Monitoreo, Detección y Análisis**	**La organización establece actividades que monitoreen continuamente el entorno de TI, prioriza y clasifica los incidentes para su respuesta.**
5	**Plan de respuesta a Incidentes**	**La organización establece un plan de respuesta a incidentes que establezca de forma clara las actividades necesarias para la gestión de los incidentes de seguridad.**
6	**Políticas y Procedimientos**	**La organización establece políticas y procedimientos que establecen el rumbo que la dirección ha establecido para la gestión de los incidentes de seguridad.**
7	**Preparación para la Respuesta a Incidentes**	**La organización establece procedimientos para prepararse preventivamente frente a los incidentes de seguridad.**