

Proceso de operaciones de respuestas a incidente ISO 27035-3

► Jorge Luis Zambrano Martinez, Ph.D.

Capítulo 2. Proceso de operaciones de respuesta a incidentes

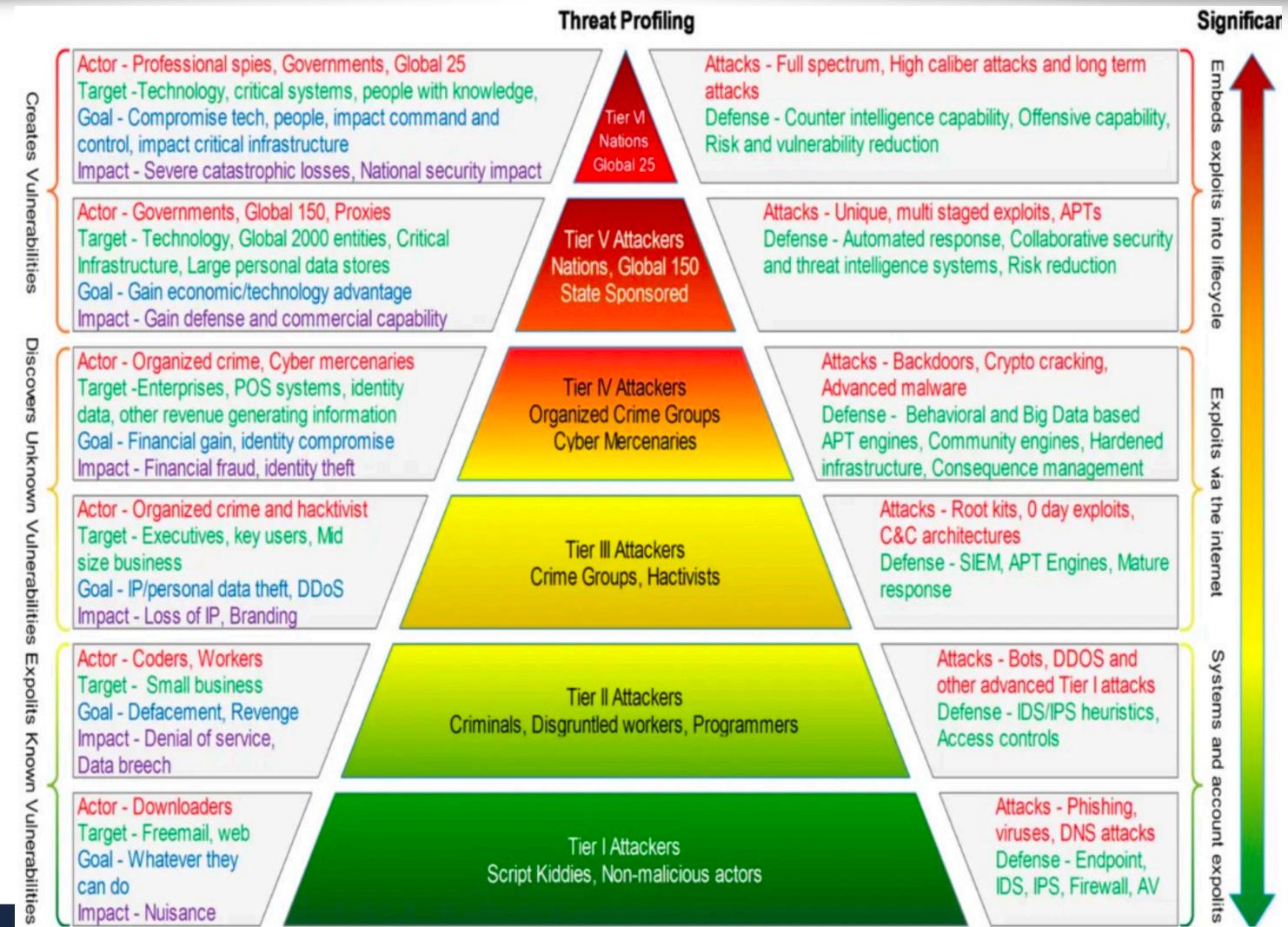
ISO 27035-3

- ✓ Presentación de capítulo y objetivos
- ✓ Categorización de las amenazas
- ✓ Guía de clasificación de incidentes de Enisa
- 1. Introducción a la Norma ISO/IEC 27035
- 2. ¿Qué es la gestión de incidentes de seguridad de la información o ISO/IEC 27035?
- 3. Estructura de la Norma ISO/IEC 27035
- 4. Definiciones básicas
- 5. Proceso de operaciones de respuesta a incidentes
- 6. ISO/IEC 27035-3: Guía para operaciones de respuesta a incidentes de TIC

Presentación del capítulo y objetivos

- La norma ISO 27035-3 proporciona directrices para las operaciones de respuesta a incidentes de seguridad de la información en las operaciones de seguridad de las tecnologías de la información y la comunicación (TIC), basándose en fases estandarizadas.
- Objetivos
 - Desarrollar habilidades valiosas en ciberseguridad.
 - Aumentar su conocimiento de las amenazas ciberneticas.
 - Conocer el cumplimiento de los requisitos legales y regulatorios.

Categorización de las amenazas



Guía de clasificación de incidentes de European Union Agency For Cybersecurity (Enisa)

CRÍTICO	Otros	APT Ciberterrorismo Daños informáticos PIC
MUY ALTO	Código dañino	Distribución de malware Configuración de malware
	Intento de intrusión	Ataque desconocido Robo Sabotaje
	Intrusión	
	Disponibilidad	Interrupciones
	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
ALTO	Código dañino	Sistema infectado Servidor C&C (Mando y Control) Malware dominio DGA
		Intento de intrusión
		Compromiso de aplicaciones
	Disponibilidad	DoS (Denegación de servicio) DDoS (Denegación distribuida de servicio)
		Acceso no autorizado a información Modificación no autorizada de información

MEDIO		Pérdida de datos
MEDIO	Fraude	Phishing Contenido abusivo Obtención de información Intento de intrusión Intrusión
		Discursivo de odio Ingeniería social Explotación de vulnerabilidades conocidas Intento de acceso con vulneración de credenciales Compromiso de cuentas con privilegios
	Fraude	Uso no autorizado de recursos Derechos de autor Suplantación
	Vulnerable	Criptografía débil Amplificador DDoS Servicios con acceso potencial no deseado Revelación de información Sistema vulnerable
	BAJO	Contenido abusivo Obtención de información Intrusión Otros
		Spam Escaneo de redes (scanning) Análisis de paquetes (sniffing) Compromiso de cuenta sin privilegios Otros

1. Introducción a la Norma ISO/IEC 27035

- Empezó como un reporte técnico (TR 18044:2004) como guía para la gestión de incidentes (2004),
 - guiar a los administradores de sistemas y seguridad sobre la adecuada gestión de incidentes de seguridad de la información.
- Este reporte técnico consistía en dividir a la gestión de incidentes en 4 procesos.



2. ¿Qué es la gestión de incidentes de seguridad de la información o ISO/IEC 27035?

- Ejercicio de un enfoque consistente y efectivo para el correcto manejo de incidentes de seguridad de la información.
- Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.



3. Estructura de la Norma ISO/IEC 27035

- Esta norma proporciona directrices para la gestión eficaz de incidentes de seguridad de la información,
 - muestra la forma de operar y las respuestas prácticas a tomar contra incidentes.
- Establece un enfoque estructurado y planificado para:
 - Detectar, informar y evaluar los incidentes de seguridad de información;
 - Responder a incidentes y gestionar incidentes de seguridad de la información;
 - Detectar, evaluar y gestionar las vulnerabilidades de seguridad de la información,
 - Mejorar continuamente la seguridad de la información y la gestión de incidentes, como resultado de la gestión de seguridad de la información y las vulnerabilidades.

3. Estructura de la Norma ISO/IEC 27035

- Esta norma se compone en tres partes:
 - **ISO/IEC 27035-1:** Principios de gestión de incidentes
 - **ISO/IEC 27035-2:** Pautas para planificar y preparar la respuesta ante incidentes
 - **ISO/IEC 27035-3:** Directrices para las operaciones de respuesta a incidentes



4. Definiciones básicas

- Evento de seguridad de la información
 - ➡ Ocurrencia que indica una posible violación de la seguridad de la información o falla de los controles.
- Incidente de Seguridad de la Información
 - ➡ Uno o varios eventos de seguridad de la información relacionados e identificador que pueden afectar a los activos de la organización o comprometer sus operaciones

5. Proceso de operaciones de respuesta a incidentes



5.1. Fases del ISO 27035 - Planificar y preparar

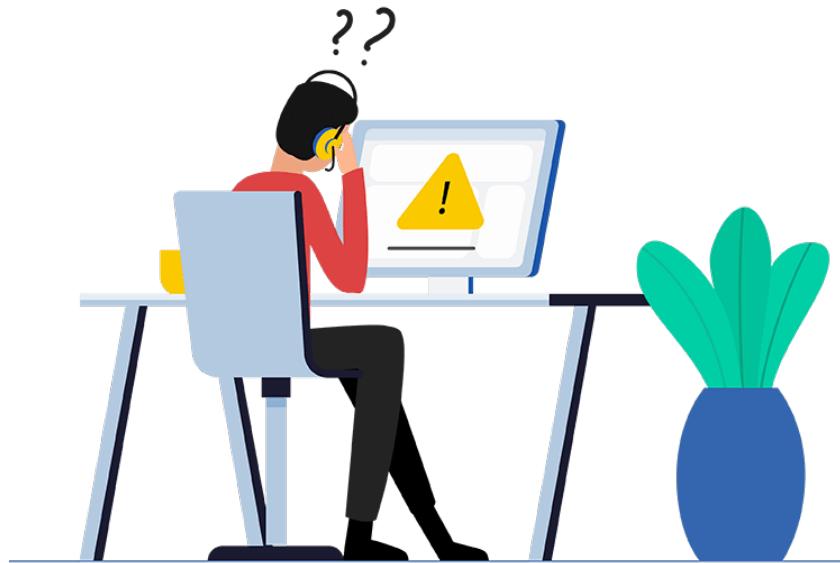
- Se trata de la creación de un plan eficaz y adecuado de gestión de incidentes de seguridad de la información para que una vez desarrollado sea puesto en funcionamiento, previo a esto una organización tiene que realizar una serie de actividades preparatorias.
- Las actividades principales de esta fase son:
 - La evaluación e identificación de activos y procesos en riesgos.
 - Elaborar una política de gestión de seguridad de la información y comprometiendo a la alta gerencia con la política.
 - Actualización de políticas actuales de seguridad de la información, incluyendo las de gestión de riesgos todo esto a nivel corporativo y de sistemas implícitos.
 - Definir y documentar un plan detallado de seguridad de la información de gestión de incidencias.

5.1. Fases del ISO 27035 - Planificar y preparar

- Establecer un equipo de respuesta a incidentes (IRT) capacitado para los propósitos del plan de gestión de incidencias de seguridad de la información.
- Fortalecer y establecer de ser necesario relaciones con organizaciones internas y externas que se encuentren involucradas en los eventos de seguridad de la información.
- Implementar y establecer mecanismos técnicos, organizativos y operativos para apoyar el trabajo del IRT y el funcionamiento del plan de gestión de incidencias de seguridad de la información.
- Concientización a toda la organización respecto a la seguridad de la información.
- Prueba del plan, verificando los procesos y procedimiento.

5.2. Fases del ISO 27035 - Detectar y reportar

- Esta segunda fase implica la detección de eventos y vulnerabilidades de seguridad de la información con la respectiva recopilación de información detallada, para su notificación en relación con los lineamientos de las políticas de seguridad y su posterior análisis.



5.2. Fases del ISO 27035 - Detectar y reportar

- Para esta fase una organización debe realizar las siguientes actividades:
 - ➡ Monitoreo de los sistemas y la red implícita.
 - ➡ Detección y notificación de forma manual, personal o automática respecto a la existencia de algún evento o vulnerabilidad de seguridad de la información.
 - ➡ Recopilación de información detallada sobre eventos o vulnerabilidades de seguridad de la información.
 - ➡ Precautelar la documentación de todas las actividades respecto a la seguridad de la información para su posterior análisis.
 - ➡ Precautelar el respaldo de pruebas digitales como evidencia que pueda utilizarse en casos legales o medidas disciplinarias.
 - ➡ Asegurarse de la monitorización y notificación de eventos o vulnerabilidades de seguridad de la información.

5.3. Fases del ISO 27035 - Evaluación y Decisión

- Esta fase es crucial debido a que la clasificación del incidente deriva en la certera solución de este.
- La clasificación de los incidentes se ejecuta contemplando varios parámetros como la magnitud del impacto que causen en las operaciones, la escala del daño que el mismo provoque y los efectos que tengan los sistemas implícitos.



5.3. Fases del ISO 27035 - Evaluación y Decisión

- Asociada a la toma de decisiones sobre los incidentes previa a una evaluación, para su clasificación según el impacto o gravedad.
- Una vez detectado y reportado el evento de seguridad de la información las actividades a realizar son:
 - ▶ Asignación de responsabilidades tanto al personal de seguridad como a usuarios.
 - ▶ Establecer procedimientos para la toma de decisiones dependiendo del tipo y gravedad de incidente.
 - ▶ Documentación de los acontecimientos y acciones a realizar posterior a la incidencia de seguridad de la información.
 - ▶ Mediciones y otros datos de seguridad de la información.
 - ▶ Evaluación del administrador de incidentes para determinar la veracidad de la notificación.
- Esta fase es crucial debido a que la clasificación del incidente deriva en la certeza solución de este.
- La clasificación de los incidentes se ejecuta contemplando varios parámetros como la magnitud del impacto que causen en las operaciones, la escala del daño que el mismo provoque y los efectos que tengan los sistemas implícitos.

5.4. Fases del ISO 27035 - Respuesta

- Consiste en acciones implementadas para la mitigación y resolución de incidentes de seguridad de la información. En esta fase se efectuarán las acciones predeterminadas en la fase de evaluación y decisión. Dichas acciones se pueden ejecutar de manera inmediata, casi en tiempo real; otras requerirán de una investigación de seguridad de la información. Para esta fase una organización debe realizar las siguientes actividades:
 - ➔ Clasificación del incidente en la escala de seguridad de la información.
 - ➔ El IRT debe realizar una evaluación determinando que el incidente esté bajo control,
y en caso contrario, se requiere ejecutar el plan de contingencia.
 - ➔ Asignación de recursos internos y externos para responder a los incidentes.
 - ➔ Documentación detallada de la incidencia y acciones realizadas.

5.4. Fases del ISO 27035 - Respuesta

- Comunicación de incidencias y respuestas con otros IRTs.
- Distribuir responsabilidades de la gestión de la información jerárquicamente para la toma de decisiones y acciones.
- Establecer procedimientos formales al personal involucrado siendo estos la revisión, modificación, reevaluación de daños y notificación al personal correspondiente. Las acciones individuales dependerán del tipo y gravedad de incidente.

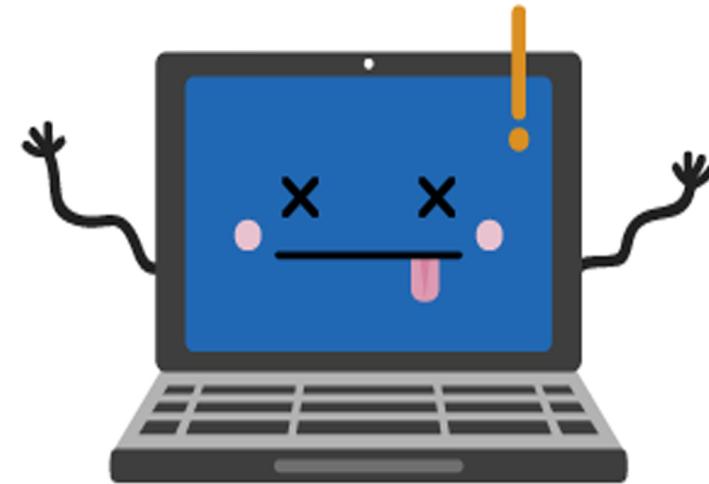


5.5. Fases del ISO 27035 - Lecciones aprendidas

- Se produce cuando han sido resueltos los incidentes, consiste en lecciones de aprendizajes de cómo se han manejado los incidentes y vulnerabilidades. Las actividades principales son:
 - Identificar las lecciones aprendidas de los incidentes y vulnerabilidades de seguridad de la información.
 - Revisar, identificar y mejorar la aplicación de controles y evaluaciones de incidentes, así como también de la política de seguridad de la información.
 - Comprobación de eficacia de procesos, procedimientos y estructura de la organización respecto a respuestas y recuperación de los incidentes de seguridad de la información.
 - Evaluación exhaustiva sobre el rendimiento y eficacia del IRT periódicamente.

6. ISO/IEC 27035-3: Guía para operaciones de respuesta a incidentes de TIC

- Los incidentes de seguridad de la información son una realidad inevitable para las organizaciones de todos los tamaños.
- Los incidentes pueden tener un impacto significativo en las operaciones comerciales, la reputación y la confianza del cliente.
- Un proceso de respuesta a incidentes bien definido es esencial para minimizar el impacto de los incidentes y restaurar la normalidad lo antes posible.



6.1. Objetivos del ISO/IEC 27035-3

- Proporcionar directrices para las operaciones de respuesta a incidentes de TIC.
- Ayudar a las organizaciones a mejorar su capacidad para responder a incidentes de seguridad de la información de manera efectiva.
- Minimizar el impacto de los incidentes en las operaciones comerciales, la reputación y la confianza del cliente.
- Promover la adopción de prácticas consistentes y efectivas de respuesta a incidentes en toda la organización.



6.2. Alcance del ISO/IEC 27035-3

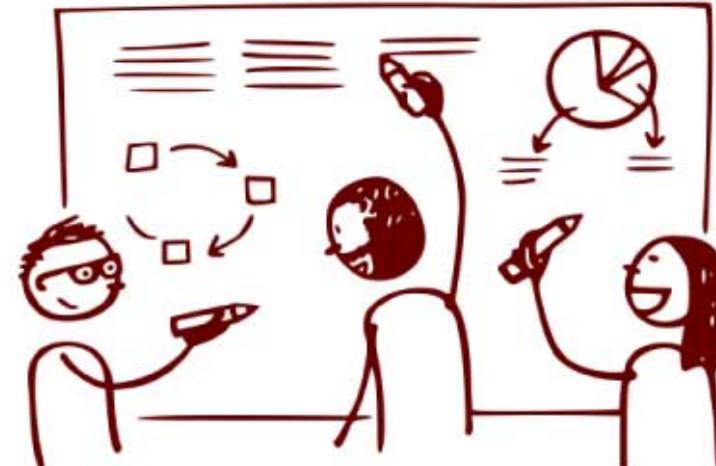
- El ISO/IEC 27035-3 se aplica a las operaciones de respuesta a incidentes de TIC en todos los tipos de organizaciones.
- El estándar cubre una amplia gama de actividades, incluyendo:
 - Identificación y análisis de incidentes
 - Contención y erradicación de incidentes
 - Recuperación y aprendizaje posterior al incidente
 - Comunicación y gestión de partes interesadas
 - Mejora continua del proceso de respuesta a incidentes

6.3. Componentes clave del ISO/IEC 27035-3

- El ISO/IEC 27035-3 se basa en un modelo de proceso de respuesta a incidentes de cuatro fases:
 - ➔ Preparación
 - ➔ Identificación y análisis
 - ➔ Contención y erradicación
 - ➔ Recuperación y aprendizaje posterior al incidente
- El estándar también incluye directrices para la gestión de partes interesadas, la mejora continua y la medición del rendimiento.

6.3.1. ISO/IEC 27035-3 - Fase Preparación

- **Establecer una política y un procedimiento de respuesta a incidentes:** Este documento debe definir el alcance del programa de respuesta a incidentes, las roles y responsabilidades, y los procesos para identificar, analizar, contener, erradicar, recuperar y aprender de los incidentes.
- **Identificar activos de información críticos:** Es importante identificar y clasificar los activos de información de la organización para comprender cuáles son los más vulnerables y requieren mayor protección.



6.3.1. ISO/IEC 27035-3 - Fase Preparación

- **Establecer planes de respuesta a incidentes específicos:** Se deben desarrollar planes específicos para diferentes tipos de incidentes, como ataques de malware, fugas de datos y denegación de servicios.
- **Capacitar al personal:** El personal debe estar capacitado en el proceso de respuesta a incidentes y en sus roles y responsabilidades específicos.
- **Probar y revisar los planes de respuesta a incidentes:** Los planes deben probarse y revisarse periódicamente para garantizar que sean efectivos y estén actualizados.

6.3.2. ISO/IEC 27035-3 - Fase Identificación y análisis

- **Establecer métodos para la detección de incidentes:** Esto puede incluir el uso de herramientas de monitoreo de seguridad, registros de sistemas y informes de empleados.
- **Analizar los incidentes para determinar su naturaleza y alcance:** Esto implica recopilar y analizar información sobre el incidente para comprender qué sucedió, cómo sucedió y qué impacto tuvo.
- **Priorizar los incidentes:** No todos los incidentes son iguales, por lo que es importante priorizarlos en función de su gravedad y potencial impacto.



6.3.3. ISO/IEC 27035-3 - Fase Contención y erradicación

- **Contener el incidente para evitar más daños:** Esto puede implicar aislar los sistemas afectados, deshabilitar cuentas de usuario o eliminar datos infectados.
- **Erradicar la causa del incidente:** Esto implica identificar y eliminar la fuente del incidente, como un virus, un malware o una vulnerabilidad de software.
- **Documentar las acciones de contención y erradicación:** Es importante registrar todas las acciones tomadas para contener y erradicar el incidente para fines de auditoría y aprendizaje posterior al incidente.



6.3.4. ISO/IEC 27035-3 - Fase recuperación y aprendizaje

- **Restaurar los sistemas y datos afectados:** Esto implica restaurar los sistemas y datos a su estado anterior al incidente.
- **Revisar el proceso de respuesta a incidentes:** Es importante revisar el proceso de respuesta a incidentes para identificar áreas de mejora.
- **Aprender del incidente y actualizar los planes de respuesta:** Las lecciones aprendidas del incidente deben usarse para actualizar los planes de respuesta a incidentes y mejorar la postura de seguridad general de la organización.



6.4. Beneficios de la implementación del ISO/IEC 27035-3

- **Mejora de la capacidad de respuesta a incidentes:** El estándar proporciona un marco para desarrollar e implementar un proceso de respuesta a incidentes que sea efectivo, eficiente y adaptado a las necesidades específicas de la organización. Esto puede ayudar a las organizaciones a responder a los incidentes de manera más rápida y efectiva, lo que puede minimizar el daño y la pérdida de datos.
- **Reducción del impacto de los incidentes:** Un proceso de respuesta a incidentes bien definido puede ayudar a las organizaciones a contener y erradicar los incidentes más rápidamente, lo que puede reducir el impacto en las operaciones comerciales, la reputación y la confianza del cliente.
- **Mejora de la comunicación y la colaboración:** El estándar proporciona directrices para la gestión de partes interesadas, lo que puede ayudar a mejorar la comunicación y la colaboración entre diferentes departamentos y niveles de la organización durante un incidente.

6.4. Beneficios de la implementación del ISO/IEC 27035-3

- **Aumento de la confianza del cliente:** Los clientes están cada vez más preocupados por la seguridad de sus datos. La implementación del ISO/IEC 27035-3 puede demostrar a los clientes que la organización está comprometida con la protección de su información, lo que puede aumentar la confianza y la lealtad.
- **Mejora de la postura de seguridad general:** El proceso de respuesta a incidentes es un componente clave de un programa de seguridad de la información completo. La implementación del ISO/IEC 27035-3 puede ayudar a las organizaciones a mejorar su postura de seguridad general y reducir el riesgo de incidentes de seguridad de la información.

6.4. Beneficios de la implementación del ISO/IEC 27035-3

- **Preparación para el cumplimiento normativo:** Muchas regulaciones de privacidad de datos, como el RGPD, requieren que las organizaciones tengan un proceso de respuesta a incidentes en vigor. La implementación del ISO/IEC 27035-3 puede ayudar a las organizaciones a cumplir con estos requisitos.
- **Mejora continua:** El estándar incluye directrices para la mejora continua, lo que puede ayudar a las organizaciones a identificar áreas de mejora en su proceso de respuesta a incidentes y hacerlas más efectivas con el tiempo.

Proceso de operaciones de respuestas a incidente ISO 27035-3

► Jorge Luis Zambrano Martinez, Ph.D.