Ecuador/Latam

Investigación de Ciber Incidentes basado en ISO/IEC 27035

PECB REGIONAL WEBINARS

Agenda

1. Términos y Definiciones
2. Gestión de Incidentes ISO 27035
3. Tendencias de Fraudes

Términos y Definiciones

- Seguridad de la Información
  ISO 27001: Preservación de la confidencialidad, integridad y disponibilidad de la información

- Riesgo
  ISO 31000: Efecto de la incertidumbre sobre los objetivos

- Ciberseguridad
  ISO 27032: Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio

- Ciberseguridad (actual)
  ISO 27100: Mantener los ciber-riesgos a un nivel tolerable, a las personas, la sociedad, las organizaciones y las naciones

Términos y Definiciones

Fraude

Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete.

- Motivación: Percepción de la necesidad económica, situación no compartible con otros. Esto es lo que motiva el delito.
- Oportunidad: La cual define el método por el cual se cometerá el acto ilícito.
- Racionalización: El defraudador justificará sus actos de una forma que sean aceptables o justificables, o al menos lo que cree.

Referencia: https://www.acfe-spain.com/recursos-contra-fraude/que-es-el-fraude/triangulo-del-fraude

Términos y Definiciones

Evento

Ocurrencia que indica una posible violación de la seguridad de la información o falla de los controles.

Incidente de Seguridad de la Información

Eventos de seguridad de la información relacionados e identificados, que pueden dañar los activos de una organización o comprometer sus operaciones

Respuesta ante Incidentes

Medidas adoptadas para mitigar o resolver un incidente de seguridad de la información, incluidas las adoptadas para proteger y restablecer las condiciones operativas normales de un sistema de información y la información almacenada en él.

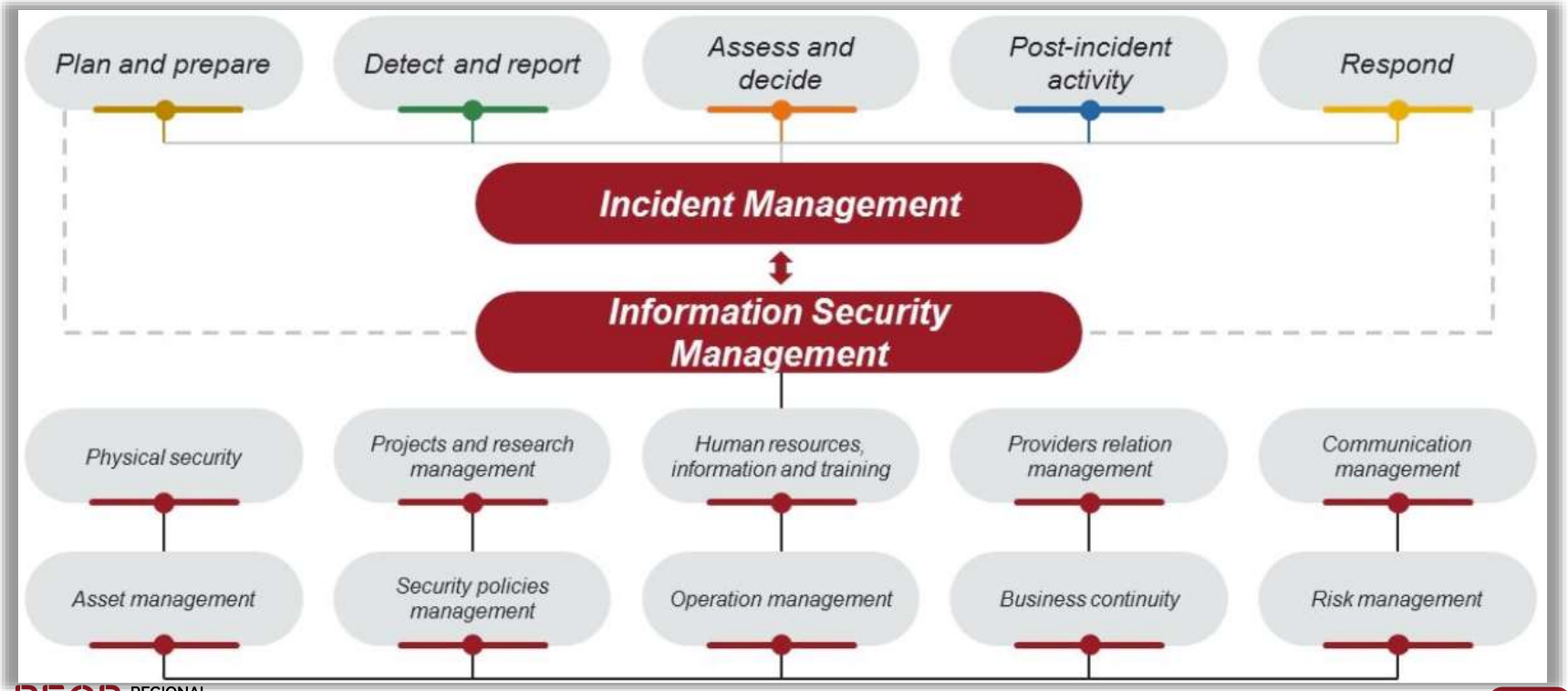
Manejo de Incidentes

Acciones para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información

Investigación de Incidente de Seguridad de la Información

Aplicación de examinación, análisis e interpretación para ayudar a comprender un incidente de seguridad de la información

Procesos integrables

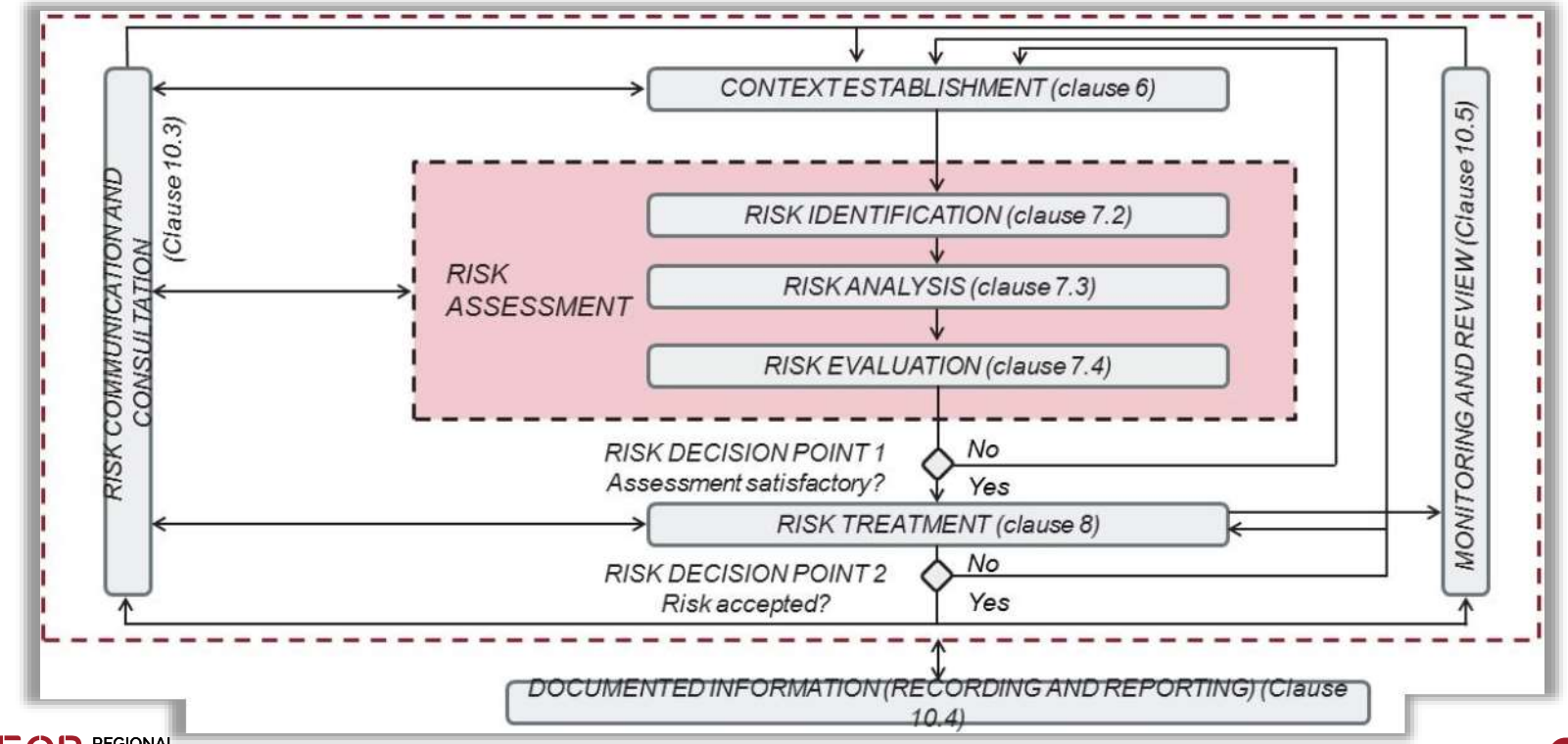


Gestión de Incidentes – ISO 27035

Plan	Detect and Report	Assess and Decide	Respond	Learn lessons
1.1 Context establishment	2.1 Monitor systems and networks	3.1 Information security event assessment	4.1 Resolve information security incidents	5.1 Lessons learned
1.2 Policies and procedures	2.2 Detect and alert		4.2 Containment, eradication, and recovery	5.2 Monitoring, measurement, analysis, and evaluation
1.3 Risk management	2.3 Information collection for incidents			5.3 Continual improvement
1.4 Incident management plan	2.4 Report information security events			
1.5 Incident management team				
1.6 Internal and external relationships				
1.7 Technical and other support				
1.8 Information security incident awareness and training				
1.9 Testing				

Gestión de Riesgos – ISO 27005

Gestión De Riesgos



Gestión de Incidentes – ISO 27035

Plan	Detect and Report	Assess and Decide	Respond	Learn lessons
1.1 Context establishment	2.1 Monitor systems and networks	3.1 Information security event assessment	4.1 Resolve information security incidents	5.1 Lessons learned
1.2 Policies and procedures	2.2 Detect and alert		4.2 Containment, eradication, and recovery	5.2 Monitoring, measurement, analysis, and evaluation
1.3 Risk management	2.3 Information collection for incidents			5.3 Continual improvement
1.4 Incident management plan	2.4 Report information security events			
1.5 Incident management team				
1.6 Internal and external relationships				
1.7 Technical and other support				
1.8 Information security incident awareness and training				
1.9 Testing				

Gestión de Incidentes – ISO 27035

Internal and external relationships

SOC
CERT
CSIRT

Gestión de Incidentes – ISO 27035

Plan	Detect and Report	Assess and Decide	Respond	Learn lessons
1.1 Context establishment	2.1 Monitor systems and networks	3.1 Information security event assessment	4.1 Resolve information security incidents	5.1 Lessons learned
1.2 Policies and procedures	2.2 Detect and alert		4.2 Containment, eradication, and recovery	5.2 Monitoring, measurement, analysis, and evaluation
1.3 Risk management	2.3 Information collection for incidents			5.3 Continual improvement
1.4 Incident management plan	2.4 Report information security events			
1.5 Incident management team				
1.6 Internal and external relationships				
1.7 Technical and other support				
1.8 Information security incident awareness and training				
1.9 Testing				

Gestión de Incidentes – ISO 27035

Testing

NIST 800-161

“Son un grupo de personas autorizadas y organizadas para simular las capacidades de ataque o explotación de un posible adversario contra la postura de seguridad de una empresa.

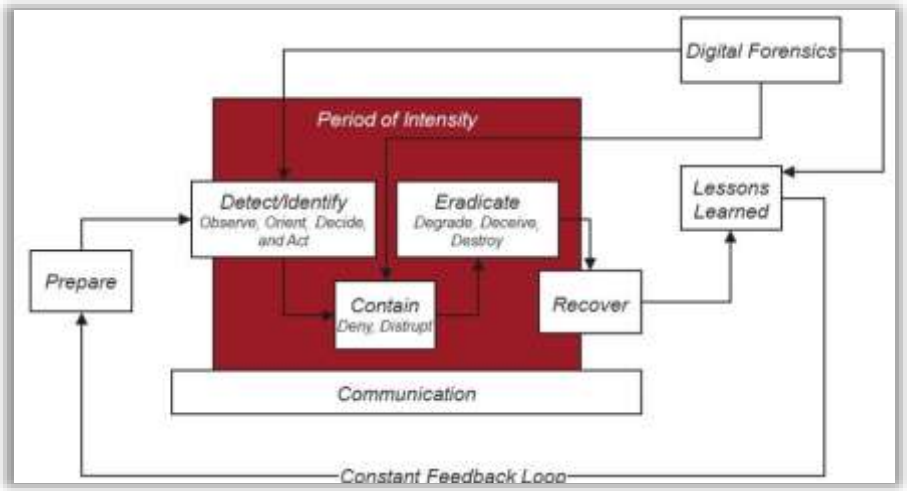
El objetivo del Equipo Rojo es mejorar la garantía de la información empresarial demostrando los impactos de los ataques exitosos y demostrando lo que funciona para los defensores (es decir, el Equipo Azul) en un entorno operativo"

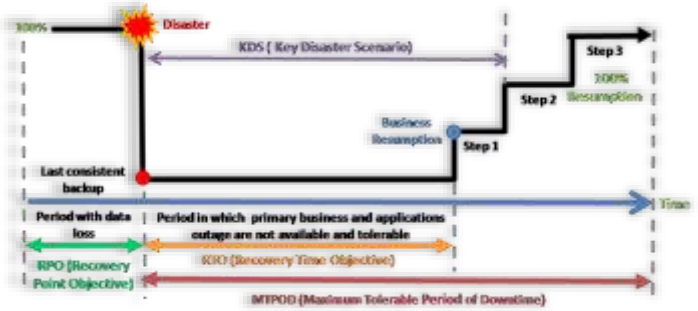
Gestión de Incidentes – ISO 27035

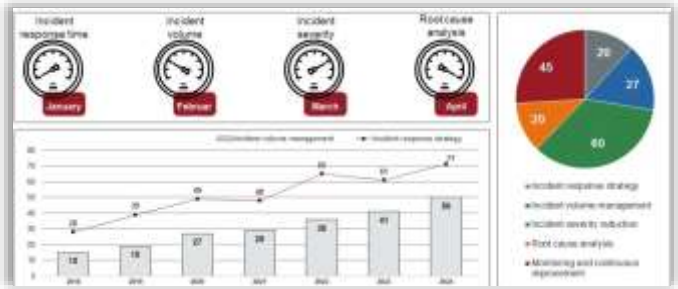
Plan	Detect and Report	Assess and Decide	Respond	Learn lessons
1.1 Context establishment	2.1 Monitor systems and networks	3.1 Information security event assessment	4.1 Resolve information security incidents	5.1 Lessons learned
1.2 Policies and procedures	2.2 Detect and alert		4.2 Containment, eradication, and recovery	5.2 Monitoring, measurement, analysis, and evaluation
1.3 Risk management	2.3 Information collection for incidents			5.3 Continual improvement
1.4 Incident management plan	2.4 Report information security events			
1.5 Incident management team				
1.6 Internal and external relationships				
1.7 Technical and other support				
1.8 Information security incident awareness and training				
1.9 Testing				

Manejo de Incidentes – NIST 800-61

Detectar y Reportar / Evaluar y Decidir / Responder

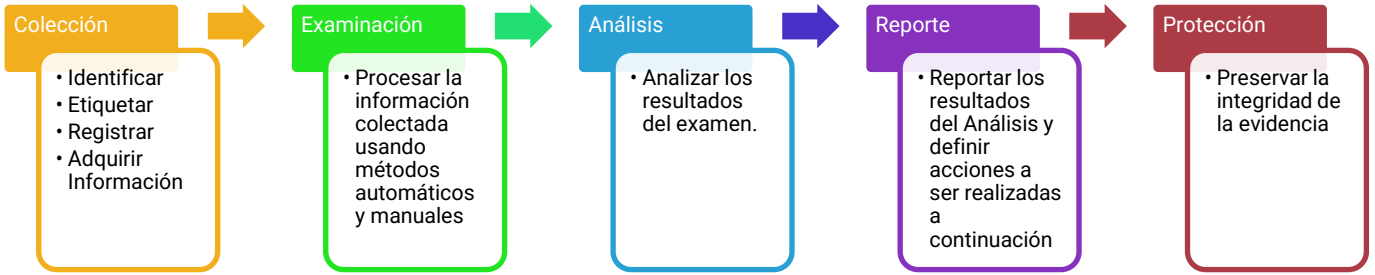






Manejo de Evidencia – ISO 27037

Fases de manejo de evidencia



Gestión de Incidentes – ISO 27035

Plan	Detect and Report	Assess and Decide	Respond	Learn lessons
1.1 Context establishment	2.1 Monitor systems and networks	3.1 Information security event assessment	4.1 Resolve information security incidents	5.1 Lessons learned
1.2 Policies and procedures	2.2 Detect and alert		4.2 Containment, eradication, and recovery	5.2 Monitoring, measurement, analysis, and evaluation
1.3 Risk management	2.3 Information collection for incidents			5.3 Continual improvement
1.4 Incident management plan	2.4 Report information security events			
1.5 Incident management team				
1.6 Internal and external relationships				
1.7 Technical and other support				
1.8 Information security incident awareness and training				
1.9 Testing				

Manejo de Evidencia – ISO 27037

Mejora en el tratamiento de riesgos asociados

Fraudes Informáticos

En 2024, los fraudes informáticos financieros más impactantes han sido:

- **Fraudes con Inteligencia Artificial (IA):** Los ciberdelincuentes han utilizado IA para crear anuncios, correos electrónicos y sitios web falsos que imitan a las instituciones financieras legítimas, haciendo difícil distinguir entre contenido auténtico y fraudulento.
- **Ataques a nuevos métodos de pago digitales**: Las billeteras digitales y los sistemas de pago inmediato, como PIX en Brasil y FedNow en Estados Unidos, han sido explotados para crear esquemas fraudulentos.
- **Troyanos bancarios móviles**: Estos programas maliciosos, especialmente los originados en Brasil, han sido utilizados para redirigir transferencias electrónicas desde smartphones infectados.
- **Ransomware selectivo**: Los ataques de ransomware se han vuelto más específicos, apuntando a víctimas que pueden pagar rescates más altos, lo que aumenta el impacto financiero.
- **Explotación de programas de código abierto**: Los ciberdelincuentes han aprovechado vulnerabilidades en programas de código abierto para comprometer la seguridad de las empresas, resultando en violaciones de datos y pérdidas financieras.

Tendencia en Fraudes Informáticos

En 2025, se esperan varias tendencias importantes en el ámbito de los fraudes informáticos financieros. Aquí te menciono algunas de las más destacadas:

- **Aumento del uso de inteligencia artificial (IA):** Los ciberdelincuentes están utilizando cada vez más la IA para automatizar y sofisticar sus ataques. Esto incluye la creación de phishing más convincente y ataques de ingeniería social más efectivos.
- **Ataques a sistemas de pago digitales**: Con la creciente adopción de pagos digitales y billeteras electrónicas, estos sistemas se están convirtiendo en un objetivo principal para los fraudes. Los dispositivos mal configurados y las nuevas tácticas de ataque están facilitando estos fraudes.
- **Fraude de identidad sintética**: Este tipo de fraude, que combina información real y ficticia para crear identidades falsas, seguirá siendo un desafío significativo. La presión regulatoria y la necesidad de mejorar la verificación de identidad serán cruciales para combatirlo.
- **Ransomware dirigido**: Los ataques de ransomware seguirán siendo una amenaza importante, especialmente dirigidos a instituciones financieras. Estos ataques no solo buscan rescates monetarios, sino también la interrupción de servicios críticos.
- **Regulación tecnológica y resiliencia operativa**: La regulación en torno a la resiliencia operativa digital será clave. Normativas como el Reglamento sobre Resiliencia Operativa Digital (DORA) se enfocarán en asegurar que las entidades financieras puedan resistir y recuperarse de incidentes tecnológicos.
- **Computación cuántica**: Aunque aún en sus primeras etapas, la computación cuántica comenzará a jugar un papel en la seguridad y protección de datos, ayudando a detectar y predecir vulnerabilidades y amenazas cibernéticas.

Q&A Session

Contact

- Website: www.bluehatcorp.com
- Phone: +593 99 275 1705
- Email: ramiro.pulgar@bluehatcorp.com

For any questions or comments you can contact us below:

- support@pecb.com