DIPLOMA DE ESPECIALIZACIÓN PROFESIONAL

CIBERSEGURIDAD Y GESTIÓN DE INCIDENTES

EXTRACTO GRATUITO — MUESTRA DE CONTENIDO

SESIÓN 5 · EXTRACTO

Amenazas actuales, el ciclo de vida de la gestión de incidentes (NIST SP 800-61), y las diferencias clave entre BCP, DRP e IRP para la continuidad del negocio.

Contenido de este Extracto

Sobre este documento

Este extracto presenta una introducción conceptual a la Sesión 5. El desarrollo completo —incluyendo el caso integrador de respuesta a incidentes, la estrategia de ciberseguridad para sistemas de IA, la ruta de preparación para certificaciones CISM/CISSP y el glosario técnico— está disponible en el Ebook exclusivo para estudiantes matriculados.

1. EL PANORAMA DE AMENAZAS ACTUALES

El panorama de riesgo cibernético no da tregua. Los incidentes de ransomware reportados en Latinoamérica han crecido más de 72% respecto al año previo, una de cada tres brechas de seguridad comienza con phishing o ingeniería social dirigida, y el tiempo promedio para identificar y contener una brecha se mantiene en torno a los 277 días.

A esto se suma un factor relativamente nuevo: los ataques que emplean inteligencia artificial generativa —deepfakes de voz y video, phishing hiperrealista— se han multiplicado por cuatro en el último periodo.

Anatomía de un ataque moderno

La mayoría de los ataques siguen una secuencia predecible, conocida como cyber kill chain: reconocimiento (OSINT y mapeo de la superficie expuesta), acceso inicial (phishing, credenciales filtradas, VPN débil), persistencia (malware, backdoors, cuentas privilegiadas), movimiento lateral (escalamiento y reconocimiento interno) e impacto (exfiltración, cifrado y extorsión).

Idea clave
Cada eslabón de esta cadena es un punto donde la detección y la respuesta oportuna pueden romper el ataque antes de que llegue al impacto final. Esta es la base conceptual de toda estrategia de defensa moderna.

2. CICLO DE VIDA DE LA RESPUESTA A INCIDENTES (NIST SP 800-61)

El estándar NIST SP 800-61 define un ciclo continuo de cinco fases para la gestión de incidentes de seguridad, que toda organización —incluso una PYME— debería conocer y adaptar a su escala:

- **Preparación:** políticas, herramientas y roles definidos antes de que ocurra un incidente.
- **Detección y análisis:** identificación temprana de indicios de compromiso.
- **Contención:** aislamiento inmediato de los sistemas afectados para frenar la propagación.
- **Erradicación y recuperación:** eliminación de la amenaza y restauración segura de los sistemas.
- **Lecciones aprendidas:** revisión posterior que retroalimenta la fase de preparación del siguiente ciclo.

Estas cinco fases no son lineales: forman un ciclo continuo, donde cada incidente gestionado mejora la preparación de la organización frente al siguiente.

3. BCP, DRP Y PLAN DE INCIDENTES: NO SON LO MISMO

Tres planes distintos, con propósitos distintos, suelen confundirse en la práctica:

Plan	Propósito
BCP — Plan de Continuidad de Negocio	Mantiene operando los procesos críticos del negocio ante cualquier disrupción
DRP — Plan de Recuperación de Desastres	Restaura la infraestructura de TI y los datos tras un evento mayor
IRP — Plan de Respuesta a Incidentes	Detecta, contiene y erradica un incidente de seguridad específico

¿QUIERES CONTINUAR TU APRENDIZAJE?

Contenido exclusivo para estudiantes matriculados
Este extracto es una muestra gratuita del contenido completo del diploma. El Ebook completo (25 páginas) incluye casos aplicados con normativa peruana, tablas de errores comunes, listas de verificación de auditoría, glosario técnico y preguntas de autoevaluación reflexiva. Disponible exclusivamente para estudiantes matriculados a través del Aula Virtual.

Accede al Aula Virtual: **www.institutoelevateperu.pe**
Consultas por WhatsApp: **973 336 333**

Elévate

MUCHAS GRACIAS

WhatsApp 973 336 333 | www.institutoelevateperu.pe