(AC-S04-PC1) – Práctica Calificada 1

15.67/20

Ver indicaciones

Has utilizado 1 de 1 intento

Intento 1 (15.67pts.)

Desarrollado el: 20/04/25 a las 09:00 p.m.

Tiempo de desarrollo: 85 min

Revisa tu exámen y valida tus respuestas

1

Tienes 2.00/4 pts.

MediDatos, una empresa dedicada al manejo de historiales clínicos electrónicos sufrió recientemente un intento de acceso no autorizado a su base de datos principal. El ataque fue detectado en tiempo real gracias a un sistema de monitoreo que alertó sobre un comportamiento inusual proveniente de una IP extranjera.

El equipo de seguridad reaccionó rápidamente, bloqueó el acceso, y activó su protocolo de respuesta a incidentes. Aunque no se comprometió información sensible, la investigación reveló que el origen del incidente fue un empleado que había utilizado una contraseña débil y la misma en varios servicios.

Este hecho impulsó a la organización a fortalecer su estrategia de ciberseguridad mediante tres acciones clave:

- Implementación de políticas más estrictas sobre contraseñas y autenticación multifactor.
- Realización de una auditoría de seguridad para identificar vulnerabilidades.
- Ejecución de una campaña interna de concienciación y formación en prácticas seguras para todo el personal.

¿Qué medidas de prevención y respuesta aplicó la empresa para controlar el incidente de ciberseguridad?

Respondiste

Sin respuesta

(AC-S04-PC1) – Práctica Calificada 1

C25805@utp.edu.pe

La rpta es corta, hay varias cosas que no están consideradas en el caso.
MediDatos aplicó **medidas de respuesta rápida**, como **el bloqueo del acceso y la activación del protocolo ante incidentes**. En cuanto a la prevención, mejoraron la gestión de contraseñas, aplicaron autenticación multifactor y reforzaron la formación del personal.

2

Tienes 2.67/4 pts.

BioData, una empresa que gestiona información médica, detectó tráfico sospechoso dentro de su red interna. El equipo de seguridad temía que un atacante ya se hubiera infiltrado y estuviera intentando moverse lateralmente entre servidores. Ante esta situación, decidieron aplicar tecnologías que permitieran detectar, bloquear y prevenir el avance del ataque.

¿Qué dispositivos o soluciones debería implementar BioData para detectar y detener posibles intrusiones en su red?

Respuesta Correcta

A. **Enrutadores sin contraseña para facilitar auditorías**

B. **Desactivar las actualizaciones automáticas de seguridad**

C. **Sistemas de detección y prevención de intrusiones (IDS/IPS)**

D. **Software antimalware actualizado en todos los dispositivos**

E. **Firewalls configurados para bloquear conexiones sospechosas**

3

Tienes 3.00/4 pts.

TechNova S.R.L. es una empresa tecnológica dedicada al desarrollo de aplicaciones web y móviles para clientes del sector financiero. En una auditoría externa, se identificaron múltiples debilidades en la gestión de accesos, almacenamiento de credenciales y protección de la información confidencial de los usuarios.

(AC-S04-PC1) – Práctica Calificada 1

Sistema de Gestión de Seguridad robusto y alineado con las mejores prácticas internacionales.

Comenzaron por establecer una Política de Seguridad de la Información, respaldada por la alta dirección, y definieron el alcance incluyendo todos los sistemas y equipos relacionados con el desarrollo y mantenimiento de software.

Mediante un ejercicio de evaluación y tratamiento de riesgos, identificaron puntos críticos, como desarrolladores reutilizando contraseñas y bases de datos mal configuradas. Para abordarlo, implementaron controles técnicos (del Anexo A) como autenticación multifactor, cifrado de datos, y segregación de ambientes de desarrollo, prueba y producción.

TechNova también fortaleció sus procesos internos mediante concienciación y capacitación en ciberseguridad, incluyendo sesiones prácticas para el personal de desarrollo y soporte.

El equipo de seguridad estableció una estrategia de auditoría y monitoreo continuo para detectar accesos no autorizados y anomalías en tiempo real. Además, se desarrolló un protocolo para la gestión de incidentes y se formalizó un Plan de Continuidad del Negocio, enfocado en mantener la operación de los servidores principales y sistemas críticos de los clientes.

Finalmente, todo el sistema fue integrado dentro del ciclo de mejora continua PDCA, con revisiones semestrales para mantenerlo actualizado.

Explica cómo la implementación de la ISO/IEC 27001 ayudó a TechNova S.R.L. a fortalecer su entorno de desarrollo y proteger los datos de sus clientes. Menciona al menos cinco elementos clave del SGSI aplicado y su impacto del caso.

Respondiste

Sin respuesta

Maria Elena Pareja Ventura
C25805@utp.edu.pe

EL SGSI, debe estar orientado al caso justificando cada elemento de la ISO

4

Tienes 4.00/4 pts.

NetDev S.A.C. es una empresa peruana de tecnología que desarrolla soluciones web y servicios en la nube para clientes corporativos. Su equipo está dividido entre tres sedes físicas en Lima, Arequipa y Trujillo. Además, parte del personal trabaja de forma remota

(AC-S04-PC1) – Práctica Calificada 1

objetivos:

- Asegurar el acceso seguro y rápido a datos compartidos entre sedes.
- Permitir a los trabajadores remotos conectarse a los servidores centrales sin interrupciones.
- Mantener la confidencialidad de la información de los clientes.
- Escalar la red en el futuro sin grandes modificaciones.

Tras una evaluación técnica, el equipo de TI propone implementar una red WAN segura y escalable, complementada con redes LAN en cada sede, así como una intranet interna para gestión organizacional, y una extranet para clientes premium.

Analiza por qué es pertinente usar redes LAN en cada sede, y cómo esta decisión mejora el rendimiento y la seguridad interna de la red.

5

Tienes 4.00/4 pts.

La *Universidad Tecnológica del Pacífico* es una institución de educación superior con una población estudiantil diversa y una planta docente activa. La universidad cuenta con una infraestructura tecnológica que permite:

- El uso de una plataforma virtual para clases y entrega de trabajos.
- El acceso al correo institucional por parte de estudiantes y docentes.
- La disponibilidad de una biblioteca digital y recursos académicos en línea.
- La conexión Wi-Fi en todo el campus.
- Videoconferencias entre sedes regionales.

Analiza el caso de la *Universidad Tecnológica del Pacífico* e identifica al menos dos protocolos TCP/IP que probablemente estén siendo utilizados en la red de esta organización. Explica para qué sirve cada uno de los protocolos que menciones en el contexto de las actividades descritas.

Respondiste

Sin respuesta