CONSULTING SYSTEMS

Modelo de Respuesta a Incidentes en 5 Pasos

01

Identificación del Incidente

Inicia el proceso de respuesta detectando rápidamente cualquier actividad inusual en la red. Emplea herramientas como SIEM y sistemas de detección de intrusos para monitorear logs y alertar sobre posibles incidentes.

02

Contención

Toma medidas urgentes para frenar el ataque y prevenir su propagación. Aísla los dispositivos afectados y aplica bloqueos temporales, mientras planificas soluciones más duraderas.

03

Erradicación de Amenazas

Elimina todo malware, puertas traseras y revisa la seguridad para prevenir futuras intrusiones.

04

Recuperación de Sistemas

Restaura tus sistemas a su funcionamiento normal y verifica que no queden amenazas ocultas. Asegúrate de que todas las operaciones se realicen de manera segura y efectiva.

05

Evaluación y Mejora Continua

Haz un análisis post-incidente, documenta hallazgos y lecciones. Actualiza políticas y estrategias de seguridad para mejorar la defensa ante futuros incidentes. Implementa soluciones de Ciberhibiene.

info@consulting-systems.tech - https://consulting-systems.tech