Glosario

CIBERSEGURIDAD PARA LÍDERES NO TÉCNICOS

CIBERSEGURIDAD

Conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas, redes y datos frente a accesos no autorizados, ataques o daños.

INGENIERÍA SOCIAL

Técnicas utilizadas por atacantes para manipular a personas y obtener información confidencial. Se basa en engaños, no en tecnología.

CONCIENTIZACIÓN EN CIBERSEGURIDAD

Capacitación y campañas educativas para que los colaboradores reconozcan riesgos y adopten hábitos seguros al usar tecnología.

PHISHING

Ataque que llega normalmente por correo electrónico, donde el atacante se hace pasar por una entidad confiable para robar información como contraseñas o datos bancarios.

AUTENTICACIÓN MULTIFACTOR (MFA)

Medida de seguridad que requiere dos o más pasos para acceder a un sistema (por ejemplo: contraseña + código enviado al celular).

RANSOMWARE

Tipo de malware que secuestra los archivos de una empresa cifrándolos, y luego exige un pago (rescate) para liberarlos.

FIREWALL (CORTAFUEGOS)

Sistema que filtra el tráfico entre redes para bloquear accesos no autorizados. Actúa como una “muralla digital”.

VULNERABILIDAD

Debilidad en un sistema que puede ser aprovechada por un atacante para causar daño o acceder sin permiso.

Glosario

CIBERSEGURIDAD PARA LÍDERES NO TÉCNICOS

GESTIÓN DE RIESGOS

Proceso para identificar, evaluar y tratar los riesgos que pueden afectar la seguridad de la información en una organización.

ISO/IEC 27001

Norma internacional que define cómo gestionar de forma segura la información en una organización. Es una guía formal para establecer buenas prácticas.

COPIAS DE SEGURIDAD (BACKUPS)

Respaldo de información importante para poder recuperarla en caso de pérdida, ataque o fallo técnico.

INCIDENTE DE SEGURIDAD

Evento que compromete o amenaza la confidencialidad, integridad o disponibilidad de la información.

CULTURA DE SEGURIDAD

Conjunto de hábitos, valores y prácticas compartidas por los colaboradores que favorecen un entorno más seguro frente a riesgos digitales.

EVALUACIÓN DE VULNERABILIDADES

Proceso técnico para identificar debilidades en sistemas, redes o aplicaciones antes de que los atacantes las encuentren.

PLAN DE RESPUESTA A INCIDENTES

Procedimiento formal que define cómo actuar ante un ataque o falla de seguridad, para minimizar daños y recuperar operaciones rápidamente.

¿POR QUÉ ES IMPORTANTE ESTE GLOSARIO?

Comprender estos términos permite a líderes y tomadores de decisiones:

- Hacer las preguntas correctas
- Tomar decisiones estratégicas con información clara
- Alinear la seguridad con los objetivos del negocio

¿Quieres implementar una estrategia de concientización para tus líderes y equipos? Contáctanos en Guardianes del Golfo y diseñamos un programa a tu medida.

info@guardianesdelgolfo.com
www.guardianesdelgolfo.net
+52 22 95 91 22 46