

Smartekh

CYBERSECURITY AWARENESS

Cada clic cuenta: enseña a tu equipo a reconocer y evitar las ciberamenazas.

En el entorno empresarial actual, las amenazas cibernéticas avanzadas, como el **ransomware y el phishing**, representan riesgos significativos que pueden comprometer la integridad de tus sistemas y datos sensibles.

La falta de preparación ante estos ataques puede resultar en pérdidas financieras sustanciales y daños irreparables a la reputación empresarial. Además, **los costos asociados a la gestión de incidentes de seguridad**, incluyendo la recuperación de datos y la interrupción de operaciones, pueden ser abrumadores. La protección de información confidencial es esencial para mantener la confianza de tus clientes y cumplir con las normativas vigentes.

Fomentar una cultura de seguridad entre nuestros empleados es crucial, ya que son la primera línea de defensa contra las amenazas cibernéticas. Implementar un servicio de **awareness** no solo prepara a tu equipo para identificar y responder eficazmente a estas amenazas, sino que también reduce la probabilidad de incidentes, minimiza costos asociados y fortalece la protección de nuestros datos sensibles, asegurando así la continuidad y el éxito de tu organización.



Beneficios Empresariales

Reducción de Incidentes y Costos

- La capacitación continua permite detectar y evitar prácticas inseguras.
- Previene ataques y brechas de seguridad, disminuyendo costos de recuperación.

Protección de Datos Sensibles

- La formación en ciberseguridad capacita a empleados para manejar información confidencial y reducir filtraciones.
- Al estar informados sobre amenazas, pueden reconocer y evitar técnicas de ingeniería social.

Prevención de Amenazas Avanzadas

- Los trabajadores, al conocer las tácticas de los ciberdelincuentes, se convierten en la primera línea de defensa.

Fomento de Cultura de Seguridad

- Una cultura de seguridad informática reduce la probabilidad de que los trabajadores cometan errores, como abrir correos sospechosos o visitar sitios inseguros.

No es magia, es estrategia: cuando el equipo entiende la ciberseguridad, el riesgo disminuye.

Fases de Desarrollo

¿Cómo lo hacemos?



Diagnóstico y evaluación inicial

- Análisis de madurez en ciberseguridad en usuarios.
- Identificación de roles críticos y necesidades específicas por área.
- Definición de KPIs y objetivos medibles.



Diseño del programa de concienciación

- Desarrollo de materiales interactivos como e-learning, videos, infografías y simulaciones.
- Implementación de campañas de simulación de phishing
- Personalización según cultura organizacional y normativas.



Implementación y entrenamiento

- Lanzamiento de sesiones presenciales o virtuales para reforzar participación.
- Entrenamientos para incentivar la participación y retención del conocimiento.
- Lanzamiento y concentrado de: infografías, newsletters y videos.



Medición, ajuste y cultura continua

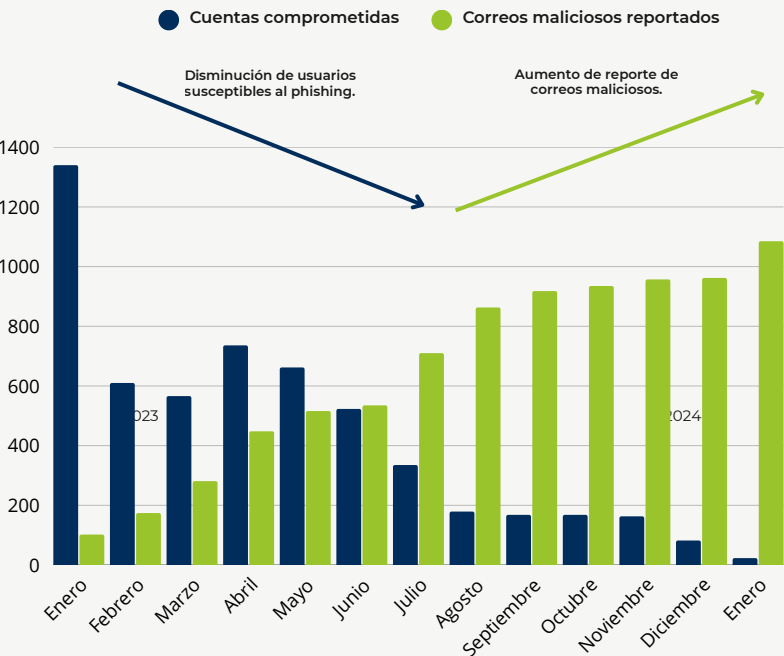
- Evaluación del impacto: métricas de mejora.
- Feedback y ajuste del programa según resultados y nuevos riesgos emergentes.
- Estrategia de sostenibilidad: integración de ciberseguridad en la cultura corporativa.

Algunos de nuestros resultados

“ El principal riesgo en ciberseguridad eran nuestros hábitos. Ahora, nuestros colaboradores reconocen señales de alerta y son nuestra primera línea de defensa, bien equipada y preparada. ”

-IS Governance Leader | Financial Company

CAMPAÑAS DE SIMULACIÓN DE PHISHING



Reducción del

98%

de cuentas comprometidas en 1 año.

TRANSFORMA TUS DESAFÍOS EN SOLUCIONES



Una estrategia holística de ciberseguridad, alineada con los objetivos, necesidades y riesgos latentes en tu organización. En un mundo cada vez más conectado, la ciberseguridad es más que una necesidad; es un imperativo estratégico.

Forma un equipo que detecte riesgos antes de que se vuelvan incidentes.

Nuestro programa **Cybersecurity Awareness** transforma a cada colaborador en una línea activa de defensa, con contenido práctico, dinámico y adaptado al nivel de cada área.

- Simulacros de phishing personalizados.
- Entrenamientos breves, efectivos y medibles.
- Reportes de riesgo humano y cultura de seguridad.

“La ciberseguridad no es solo tecnología, es comportamiento.”

— *NIST NICE Framework*

Tu equipo puede ser tu mejor defensa... o tu mayor riesgo.

Transformando la ciberseguridad para el futuro que tu negocio necesita



Grupo Smartekh Heriberto Frías 1451 Int. 101, Benito Juárez México 03100 800 2121 500 | smartekh.com

En Grupo Smartekh brindamos servicios de diseño, adopción y gestión de ciberseguridad que habilitan y protegen el negocio de amenazas en la era digital y ayudan a las empresas a ser más resilientes cada día con base a lo que tu negocio necesita. Diseñamos una estrategia y administramos (ejecutamos) servicios de ciberseguridad. Ayudamos a implementar y mantener la estrategia de seguridad mediante un modelo de madurez en dos verticales: Gestión de Amenazas de Seguridad (servicios administrados) y Seguridad en Nube. Ofreciendo servicios a la medida del cliente. ©2025 Grupo Smartekh S.A de C.V. Todos los derechos reservados.