Ciberseguridad en Empresa

Usuarios básicos

¡Bienvenidos al curso de Ciberseguridad!

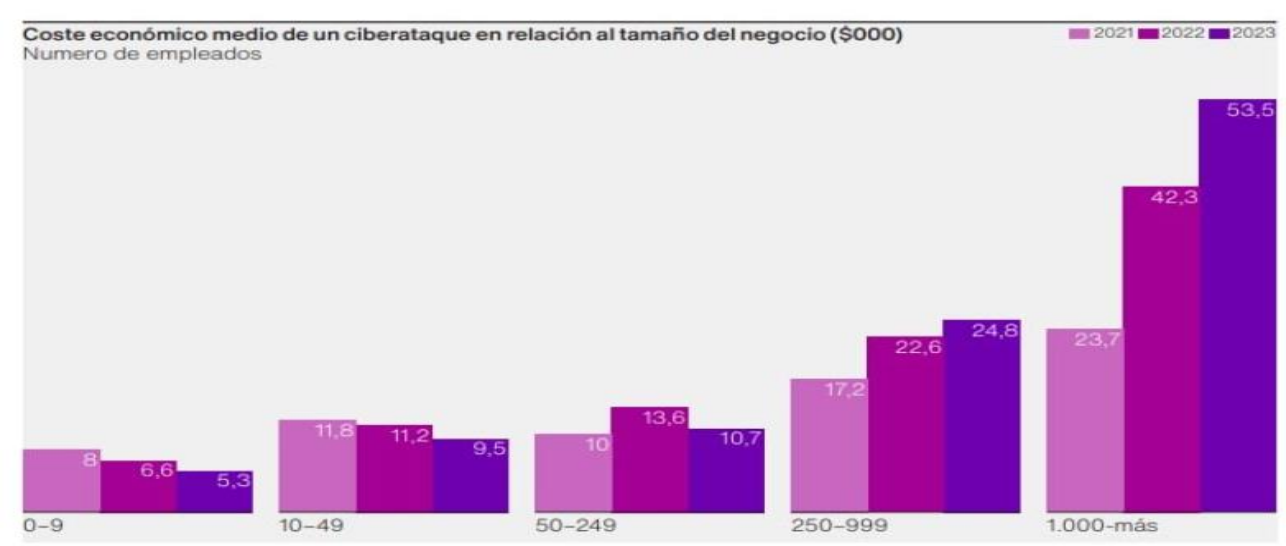
Protégete y protege la información de la empresa.

Índice

- Definición de ciberseguridad
- Políticas de ciberseguridad de TechSecure
- Tipos de Amenazas Cibernéticas Comunes
- ¿Cómo protegernos?
- Casos Reales
- ¡Mantén la Seguridad, Tu Trabajo y Tu Empresa Estarán a Salvo!
- Dudas o Extras

Importancia de la Ciberseguridad

- La ciberseguridad es una prioridad crítica para todas las organizaciones.
- Los ciberataques no solo amenazan los datos sensibles, sino que también comprometen la reputación empresarial.
- La protección de la información es responsabilidad de todos. Al estar comprometidos con las mejores prácticas, ayudamos a mantener la seguridad de la empresa y de nuestros clientes.



Políticas de Ciberseguridad de TechSecure

- **Proteger la confidencialidad, integridad y disponibilidad de la información:** Aseguramos que los datos sean accesibles solo para las personas autorizadas, precisos y siempre disponibles cuando se necesiten.
- **Prevenir, detectar y responder a amenazas cibernéticas**: Implementamos medidas para minimizar el riesgo de ataques, detectar amenazas a tiempo y dar respuestas rápidas y eficaces.
- **Establecer una base de cumplimiento legal y normativo**: Cumplimos con todas las leyes, regulaciones y estándares de la industria relacionados con la protección de datos.
- **Promover una cultura de ciberseguridad**: Fomentamos el compromiso de todos los empleados para integrar prácticas seguras en su día a día.
- **Fortalecer la resiliencia organizacional**: Creamos una infraestructura sólida que permite a la empresa recuperarse rápidamente de cualquier incidente cibernético.
- **Optimizar la gestión de riesgos**: Implementamos un enfoque proactivo para identificar, evaluar y mitigar riesgos antes de que se materialicen.

Amenazas Cibernéticas Comunes

Las amenazas más comunes que enfrentamos en TechSecure incluyen:

- **Phishing:** Correos electrónicos fraudulentos diseñados para engañar a los empleados y robar información sensible.
- **Malware:** Software malicioso que puede dañar sistemas, robar información o proporcionar acceso no autorizado.
- **Contraseñas débiles:** La utilización de contraseñas fáciles de adivinar pone en riesgo la seguridad de las cuentas de la empresa.

Buenas Prácticas de Ciberseguridad

Para protegerte y proteger a la empresa, sigue estas buenas prácticas:

- **Contraseñas seguras:** Utiliza contraseñas complejas que combinan letras, números y caracteres especiales.
- **Revisión de correos electrónicos:** Desconfía de correos electrónicos de fuentes no verificadas, especialmente si incluyen enlaces o archivos adjuntos.
- **Actualización constante de software:** Asegúrate de que todos los dispositivos y aplicaciones estén actualizados para protegerte de vulnerabilidades conocidas.
- **Autenticación de dos factores:** Activa esta opción siempre que sea posible, para una capa extra de seguridad.

Impacto de **NO SEGUIR** las Buenas Prácticas

- **Caso real de phishing:** Un correo malicioso solicita credenciales de acceso. Si se responde, el atacante obtiene acceso a información crítica de la empresa.
- **Consecuencias:** Pérdida de datos, daños económicos y reputacionales, sanciones legales.
- **Lecciones aprendidas:** Detectar señales de alerta y actuar rápidamente puede prevenir ataques graves.

Mantén la Seguridad: Tu Papel es Crucial

La **ciberseguridad** no es solo un área técnica, es una responsabilidad compartida por cada miembro del equipo. Al seguir las políticas y las buenas prácticas, contribuyes activamente a la protección de la empresa.

Recursos y Soporte

Si tienes alguna pregunta o necesitas más información, estamos aquí para ayudarte.

- **Soporte de TI:** juanma.herrera.mer@gmail.com
- **Documentos adicionales: Accede a guías y recursos de ciberseguridad aquí: Enlace a la intranet de seguridad**

¡Gracias por vuestra atención!

Espero que os haya resultado y ameno y útil