Programa anual de Ciberseguridad y Protección de la Información

Contenidos

Mes 1: Fundamentos de ciberseguridad y cultura organizacional

- Principios básicos de seguridad de la información
- Responsabilidad individual y colectiva frente al riesgo
- Presentación de políticas internas vigentes

Mes 2: Ingeniería social e ingeniería social asistida por IA

- Reconocimiento de phishing hiperpersonalizado
- Smishing y phishing por código QR
- Casos reales recientes del sector

Mes 3: Suplantación de identidad mediante deepfake

- Identificación de señales en audio y video sintético
- Protocolo de verificación por canal secundario
- Simulacro dirigido a roles críticos

Mes 4: Gestión de credenciales y autenticación

- Buenas prácticas de contraseñas y gestores de credenciales
- Autenticación multifactor resistente a phishing
- Riesgos de reutilización y exposición de credenciales

Mes 5: Seguridad en dispositivos móviles e IoT

- Riesgos de malware móvil y ataques vía NFC
- Configuración segura de dispositivos corporativos y BYOD
- Buenas prácticas en redes públicas y conexiones inalámbricas

Mes 6: Seguridad en entornos Cloud y SaaS

- Riesgos de configuración incorrecta en la nube
- Uso seguro de aplicaciones y almacenamiento colaborativo
- Visibilidad y control sobre datos en múltiples plataformas

Mes 7: Uso responsable de inteligencia artificial generativa

- Límites en el manejo de información sensible con herramientas de IA
- Riesgos de exposición de datos corporativos y de clientes
- Políticas internas de uso aceptable

Mes 8: Ransomware y continuidad operativa

- Vectores de entrada más frecuentes
- Procedimiento ante cifrado de archivos o sistemas
- Rol individual en la contención temprana

Mes 9: Seguridad en la cadena de suministro y terceros

- Riesgos derivados de proveedores y accesos externos
- Verificación de solicitudes provenientes de terceros
- Reporte de comportamientos anómalos en integraciones externas

Mes 10: Privacidad de datos y cumplimiento normativo

- Tratamiento adecuado de datos personales y sensibles
- Obligaciones regulatorias aplicables a la organización
- Consecuencias de la exposición o filtración de información

Mes 11: Seguridad física y convergencia con lo digital

- Control de acceso a instalaciones y equipos
- Riesgos de dispositivos extraviados o robados
- Manejo seguro de documentación e información impresa

Mes 12: Simulacro integral y evaluación anual

- Ejercicio combinado de phishing, vishing y respuesta a incidentes
- Revisión de indicadores de desempeño del programa
- Retroalimentación y planificación del ciclo siguiente