Plan de Formación y Concienciación en Seguridad

1. Programas de formación en seguridad

Con el fin de sensibilizar y capacitar a empleados en prácticas de seguridad de la información, alineadas con los procesos críticos de la empresa y normativas aplicables (RGPD, ISO 27001) se llevará a cabo una capacitación obligatoria anual en seguridad de la información.

La capacitación estará a cargo de una empresa especializada en formación en seguridad de la información y tendrá en cuenta las siguientes necesidades según el público objetivo:

Grupo	Riesgos Asociados	Temas Prioritarios
Alta Dirección	Filtración de estrategias, fraudes financieros.	- Gobierno de la seguridad.
		- Cumplimiento legal (RGPD, PCI-DSS).
Desarrollo Software	Pérdida de código fuente, ataques a APIs.	- Seguridad en DevOps (DevSecOps).
		- Gestión de secretos (HashiCorp Vault).
Consultoría/Soporte	Fugas de datos de clientes, ingeniería social.	- Protección de datos personales.
		- Uso seguro de VPN y DLP.
Marketing	Phishing, fraude publicitario.	- Seguridad en redes sociales.
		- Detección de campañas falsas.
Finanzas	Fraudes bancarios, suplantación de identidad.	- MFA en sistemas contables.
		- Detección de transacciones sospechosas.
Teletrabajadores	Malware en dispositivos personales, accesos no autorizados.	- Políticas BYOD.
		- Uso de VPN/MFA.
		- Cifrado de disco.

(anexo plan formativo anual)

2. Campañas de concienciación

La concienciación continua del personal es un pilar fundamental para la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) de Techsystem. Con el objetivo de asegurar que la seguridad de la información sea una prioridad constante, minimizar los

riesgos asociados a errores humanos y fomentar una cultura de seguridad proactiva, se establece un programa anual estructurado de concienciación y verificación. Este programa está diseñado para reforzar las políticas y procedimientos de seguridad, mantener al personal informado sobre las amenazas actuales y evaluar periódicamente la preparación de la organización.

El programa se basa en un calendario planificado de actividades que se distribuyen a lo largo del año, garantizando una exposición y refuerzo constantes. Combina diferentes métodos, incluyendo comunicación, simulación práctica, formación formal y evaluación. Los componentes clave de este programa son:

- **Comunicación Periódica (Información de Novedades):** Distribución mensual de boletines informativos, alertas de seguridad, mejores prácticas y recordatorios de políticas a través de los canales de comunicación interna. Su objetivo es mantener un nivel basal de concienciación y alertar sobre riesgos emergentes.
- **Simulacros de Phishing:** Ejecución trimestral de campañas controladas de simulación de phishing dirigidas a todo el personal o a grupos específicos. Permiten evaluar la capacidad de detección y reporte, y proporcionan oportunidades de aprendizaje inmediato.
- **Simulacros de Ataques Diversos:** Realización semestral de simulacros que van más allá del phishing, pudiendo incluir escenarios de ingeniería social (telefónica, presencial), intentos de introducción de malware (ej. USB), o pruebas de seguridad física, adaptados a los riesgos identificados para Techsystem. El objetivo es evaluar la respuesta ante un espectro más amplio de amenazas.
- **Formación Anual Obligatoria:** Desarrollo de una sesión de formación anual, conforme al Plan Formativo (Ver Anexo X), adaptada a los distintos roles y responsabilidades (Dirección, Desarrollo, TI, etc.) y cubriendo los aspectos más relevantes de la política de seguridad, la normativa aplicable (RGPD) y las amenazas específicas del sector.
- **Evaluación Anual de Conocimientos:** Administración de una evaluación formal tras la capacitación anual para medir la asimilación de los conceptos clave de seguridad por parte de los empleados. Los resultados pueden orientar futuras acciones de refuerzo. (Ver Anexo X para ejemplo de evaluación).
- **Auditoría Interna Anual del SGSI:** Como parte del ciclo de mejora continua y en cumplimiento con ISO 27001, se realiza una auditoría interna anual para verificar la

conformidad y efectividad de los controles implementados, incluyendo aquellos relacionados con la concienciación y competencia del personal.

- **Revisión Anual de la Política de Seguridad:** El Comité de Seguridad, con la aprobación de la Alta Dirección, revisa anualmente la Política de Seguridad y toda la documentación asociada para asegurar su vigencia, adecuación y alineación con los objetivos estratégicos y el panorama de riesgos. Los cambios significativos son comunicados a toda la organización.

Calendario del Programa Anual de Concienciación y Verificación - Techsystem 2025

Mes	Actividad(es) Clave	Frecuencia	Objetivo Principal	Responsable Clave (Sugerido)
Enero	Boletín Mensual: - Novedades y Consejos de Seguridad	Mensual	Mantener concienciación general, informar sobre amenazas actuales.	Dpto. TI / Comité Seguridad
Febrero	Boletín Mensual: - Simulacro Trimestral de Phishing	Mensual, Trimestral	Concienciación: Evaluar y reforzar la detección de correos maliciosos.	Dpto. TI / Comité Seguridad
Marzo	Boletín Mensual: - Novedades y Consejos de Seguridad	Mensual	Mantener concienciación general, informar sobre amenazas actuales.	Dpto. TI / Comité Seguridad
Abril	Boletín Mensual: - Simulacro Semestral de Ataque (Ej. Ingeniería Social, Malware Simulado)	Mensual, Semestral	Concienciación: Evaluar la respuesta del personal ante diversos vectores de ataque.	Dpto. TI / Comité Seguridad
Mayo	Boletín Mensual: - Simulacro Trimestral de Phishing	Mensual, Trimestral	Concienciación: Evaluar y reforzar la detección de correos maliciosos.	Dpto. TI / Comité Seguridad
Junio	Boletín Mensual: - Novedades y Consejos de Seguridad	Mensual	Mantener concienciación general, informar sobre amenazas actuales.	Dpto. TI / Comité Seguridad

Julio	Boletín Mensual: - Novedades y Consejos de Seguridad	Mensual	Mantener concienciación general, informar sobre amenazas actuales.	Dpto. TI / Comité Seguridad
Agosto	Boletín Mensual: Simulacro Trimestral de Phishing	Mensual, Trimestral	Concienciación: Evaluar y reforzar la detección de correos maliciosos.	Dpto. TI / Comité Seguridad
Septiembre	Boletín Mensual: - Formación Obligatoria Anual en Seguridad - Evaluación Anual de Conocimientos	Mensual, Anual	Concienciación: - Actualizar conocimientos y cumplir requisitos normativos -Medir la comprensión post-formación.	Dpto. TI / RRHH / Comité Seg.
Octubre	Boletín Mensual: - Simulacro Semestral de Ataque (Ej. Ingeniería Social, Malware Simulado)	Mensual, Semestral	Concienciación: Evaluar la respuesta del personal ante diversos vectores de ataque.	Dpto. TI / Comité Seguridad
Noviembre	Boletín Mensual: - Simulacro Trimestral de Phishing - Auditoría Interna Anual (ISO 27001)	Mensual, Trim./Anual	Concienciación: - Evaluar detección - Verificar cumplimiento y eficacia del SGSI.	Dpto. TI / Comité Seg. / Auditores
Diciembre	Boletín Mensual: - Revisión Anual de la Política de Seguridad	Mensual, Anual	Concienciación: Asegurar la actualidad, adecuación y comunicación de la política.	Comité Seguridad / Alta Dirección