Fortiseg

Empresa Cibersegura — Programa de Concienciación

Identificador	SRV-CYB-010
Versión	v1.0
Fecha	2026-02-23
Generado	202602241123
URL de control	https://docs.fortiseg.eu/SRV-CYB-010.pdf

Versión online

Servicio: Empresa Cibersegura — Programa de Concienciación en Ciberseguridad

1. Descripción del servicio

Empresa Cibersegura es un programa continuado de **concienciación en ciberseguridad** dirigido a empresas de servicios esenciales (suministro de agua, saneamiento, utilities y sector industrial).
El programa tiene dos vertientes:

- **Interna:** material de concienciación para los **empleados** de la empresa, desde operarios de planta hasta dirección.
- **Externa:** material de concienciación para los **clientes y usuarios** del servicio, reforzando la imagen de la empresa como operador responsable y seguro.
  Nota: La formación reglada en ciberseguridad (cursos eLearning, certificados, etc.) se gestiona a través de las plataformas de formación Fortiseg (SRV-CYB-020, SRV-CYB-030) y los cursos en directo (SRV-CYB-040).

2. ¿Por qué es necesario?

Para la empresa

- La **Directiva NIS2** exige concienciación continua en ciberseguridad para los empleados de entidades esenciales (Art. 20).
- Los **órganos de dirección** son personalmente responsables de garantizar una cultura de seguridad.
- El factor humano es la causa del **80-90% de los incidentes** de ciberseguridad.
- Un programa de concienciación reduce significativamente el riesgo de phishing, ransomware y errores operativos.

Para los clientes/usuarios

- Refuerza la **confianza** en la empresa como operador de un servicio esencial.
- Demuestra **compromiso con la ciberseguridad** ante reguladores, auditorías y licitaciones.
- Contribuye a la **protección del ecosistema** (clientes más seguros = menos vectores de ataque).

3. Componentes del programa

3.1 Material de concienciación interna

Material gráfico periódico para uso interno de la empresa:

- **Píldoras semanales** — imágenes con consejos de ciberseguridad, listas para publicar en intranet, pantallas de salas comunes, tablones de anuncios o grupos internos.
- **Cartelería** — pósters para plantas de tratamiento, oficinas, salas de control.
- **Alertas temáticas** — material específico cuando surgen amenazas relevantes (campañas de phishing, nuevos ransomware, etc.).

Temáticas

- Phishing y correos sospechosos
- Contraseñas y autenticación
- Uso seguro de dispositivos móviles y portátiles
- Seguridad en redes WiFi
- Protección de datos y confidencialidad
- Seguridad física (acceso a instalaciones, dispositivos USB)
- Ingeniería social y estafas telefónicas
- Protocolos ante incidentes: qué hacer y a quién avisar
- Seguridad en entornos OT: no conectar dispositivos no autorizados, actualizaciones, acceso remoto

3.2 Material de concienciación para clientes

Material personalizado con la **marca e imagen corporativa** de la empresa, dirigido a los usuarios finales del servicio:

- **Imágenes para redes sociales** (1080×1080 y 1080×1920) con píldoras de ciberseguridad adaptadas al sector.
- **Contenido para la web corporativa** o app de clientes.
- **Material imprimible** para incluir con facturas o comunicaciones periódicas.

Ejemplos de píldoras para clientes

- “Tu empresa de agua nunca te pedirá contraseñas por teléfono o email”
- “Accede a tu área de cliente escribiendo la dirección web, no desde enlaces en emails”
- “Si recibes un SMS sospechoso sobre tu suministro, contacta directamente con nosotros”
- “Protege el acceso a tu cuenta: usa una contraseña única y segura”

- “Desconfía de llamadas que te pidan datos urgentes sobre tu contrato”

4. Personalización

Todo el material se entrega **personalizado con la imagen corporativa** de la empresa:

- Logo y colores corporativos
- Nombre de la empresa
- Datos de contacto para incidentes
- Tono y estilo adaptados a la comunicación de la empresa

5. Simulaciones de phishing

El programa incluye **campañas periódicas de simulación de phishing** para medir y mejorar la capacidad real de los empleados para detectar correos fraudulentos.

¿En qué consiste?

- Se envían **correos simulados de phishing** realistas a los empleados, imitando amenazas reales del sector (suplantación de proveedores, notificaciones falsas de la administración, facturas fraudulentas, etc.).
- El sistema registra quién **abre el correo**, quién **hace clic en el enlace** y quién lo **reporta correctamente** como sospechoso.
- Cada trimestre se entrega un **informe de resultados** con métricas de evolución y recomendaciones.

Formación automática de refuerzo

Los empleados que caen en la simulación reciben **automáticamente** acceso a módulos de formación de refuerzo específicos sobre phishing y fraude por correo electrónico. El sistema se integra con la plataforma eLearning para que la formación sea inmediata y personalizada.

Frecuencia

- **12 campañas al año** (1 por mes), con escenarios variados y crecientes en dificultad.
- **Informes trimestrales** con métricas: tasa de apertura, tasa de clic, tasa de reporte, evolución temporal.

Beneficios

- **Mide el riesgo real** — saber qué porcentaje de la plantilla es vulnerable no es lo mismo que hacer un curso.

- **Mejora continua** — las métricas mejoran campaña a campaña, con evidencias medibles.
- **Cumplimiento normativo** — genera evidencias concretas para auditorías ENS, NIS2 e ISO 27001.
- **Efecto disuasorio** — los empleados que saben que hay simulaciones están más alerta en su día a día.

6. Frecuencia y entregables

Elemento	Frecuencia	Formato
Píldoras internas (empleados)	Semanal	Imagen digital (PNG)
Píldoras externas (clientes)	Quincenal	Imagen digital (PNG)
Cartelería	Trimestral	PDF imprimible (A3/A4)
Alertas temáticas	Según necesidad	Imagen digital + texto
Simulaciones de phishing	Mensual (12/año)	Correo simulado + landing
Informe simulaciones	Trimestral	PDF con métricas
Informe de actividad	Semestral	PDF

7. Beneficios

Cumplimiento normativo

- Satisface los requisitos de concienciación de **NIS2** (Art. 20).
- Genera **evidencias auditables** (material distribuido, registros de entrega).
- Demuestra **diligencia debida** de los órganos de dirección.

Reducción de riesgo

- Disminución drástica de incidentes por factor humano.
- Empleados capaces de identificar y reportar amenazas.
- Cultura de seguridad integrada en la operación diaria.

Imagen y reputación

- Posicionamiento como empresa comprometida con la ciberseguridad.
- Diferenciación en licitaciones y auditorías.
- Confianza reforzada de clientes y reguladores.

8. ¿Por qué Fortiseg Technology?

- Especialistas en **ciberseguridad para entornos OT e infraestructuras críticas**.
- Capacidad de generar material personalizado a escala.
- Enfoque práctico y adaptado a la realidad operativa de las plantas.
- Contenido actualizado con las últimas amenazas y tendencias.