Ciberseguridad, concienciación de los usuarios

Curso de síntesis de 1 día - 7h
Ref.: SES - Precio 2024: 660€ sin IVA

Este curso le permitirá identificar los riesgos y las consecuencias de una acción del usuario que atente contra la seguridad del sistema de información, explicar y justificar las limitaciones impuestas por la política de seguridad y comprender las principales contramedidas aplicadas en la empresa.

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Comprender los tipos de riesgos para la seguridad de la SI y sus posibles consecuencias

Identificar las medidas de protección de la información y de seguridad de los puestos de trabajo

Promover la aplicación de la política de seguridad informática de la empresa.

PROGRAMA

última actualización: 02/2024

1) Seguridad informática: conocer las amenazas y los riesgos

- Introducción: marco general, ¿qué se entiende por seguridad informática (amenazas, riesgos, protección)?
- ¿Cómo puede la negligencia provocar un desastre? He aquí algunos ejemplos. Responsabilidad civil.
- Componentes de SI y sus vulnerabilidades. Sistemas operativos cliente y servidor.
- Redes corporativas (locales, de sitio a sitio, acceso a Internet).
- Redes inalámbricas y movilidad. Aplicaciones de alto riesgo: web, correo electrónico, etc.
- Base de datos y sistema de archivos. Amenazas y riesgos.
- Sociología de los piratas. Redes clandestinas. Motivaciones.
- Tipología de los riesgos. La ciberdelincuencia en Francia. Vocabulario (sniffing, spoofing, smurfing, hijacking, etc.).

2) Protección de la información y seguridad de los puestos de trabajo

- Vocabulario. Confidencialidad, firma e integridad. Comprensión de las limitaciones asociadas al cifrado.
- Esquema general de los elementos criptográficos. Windows, Linux o macOS: ¿cuál es el más seguro?
- Gestión de datos sensibles. Problemas con ordenadores portátiles.
- ¿Cuál es la amenaza en la estación de trabajo del cliente? Entender qué es un código malicioso.
- ¿Cómo se gestionan las vulnerabilidades de seguridad? El puerto USB. El papel del cortafuegos cliente.

3) Autenticación de usuarios y acceso externo

- Control de acceso: autenticación y autorización.
- ¿Por qué es tan importante la autenticación?
- La contraseña tradicional.
- Autenticación mediante certificados y tokens.
- Acceso remoto a través de Internet. Comprensión de las VPN.
- Las ventajas de la autenticación mejorada.

PARTICIPANTES

Todos los usuarios con acceso al sistema de información a través de un puesto informático.

REQUISITOS PREVIOS

Ninguna.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

4) ¿Cómo puede participar en la seguridad de la SI?
- Análisis de riesgos, vulnerabilidades y amenazas.
- Restricciones reglamentarias y legales.
- ¿Por qué debe mi organización cumplir estos requisitos de seguridad?
- Las personas clave en seguridad: entender el papel del CISO y del gestor de riesgos.
- Actuar para mejorar la seguridad: aspectos sociales y jurídicos. CNIL y legislación.
- Cibervigilancia y protección de la intimidad.
- La carta de utilización de los recursos informáticos.
- Seguridad cotidiana. Los reflejos correctos. Conclusión.

FECHAS

Contacto