Sistema de Gestión de Seguridad de la Información UNE-ISO/IEC 27001:2017

Modalidad:

e-learning con una duración 112 horas

Objetivos:

- Dotar a los alumnos de los lineamientos básicos para la aplicación de la Norma ISO/IEC 27001 dentro de su organización.- Ofrecer las pautas para implementar un sistema de gestión de seguridad de información basado en el estándar ISO/IEC 27001 siguiendo los controles recomendados por el estándar ISO/IEC 27002 en sus respectivas cláusulas.- Exponer y explicar una serie de buenas prácticas para conseguir la seguridad de la información.

Contenidos:

MÓDULO 1. LA SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. NATURALEZA Y DESARROLLO DE LA SEGURIDAD DE LA INFORMACIÓN

La sociedad de la información
¿Qué es la seguridad de la información?
Importancia de la seguridad de la información
Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
- Principio Básico de Confidencialidad
- Principio Básico de Integridad
- Disponibilidad
Descripción de los riesgos de la seguridad
Selección de controles
Factores de éxito en la seguridad de la información

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE SEGURIDAD DE LA INFORMACIÓN

Marco legal y jurídico de la seguridad de la información
Normativa comunitaria sobre seguridad de la información
- Planes de acción para la utilización más segura de Internet
- Estrategias para una sociedad de la información más segura
- Ataques contra los sistemas de información
- La lucha contra los delitos informáticos
- La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
Normas sobre gestión de la seguridad de la información: Familia de Normas ISO 27000
- Familia de Normas ISO 27000
- Norma ISO/IEC 27002:2009
Legislación española sobre seguridad de la información
- La protección de datos de carácter personal
- La Ley Orgánica - de 13 de diciembre, de Protección de Datos de Carácter Personal
- El Real Decreto - de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica - de 13 de diciembre, de protección de datos de carácter personal
- La Agencia Española de Protección de Datos
- El Real Decreto - de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Ley - de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- La Ley - de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico
- La Ley - de 9 de mayo, General de Telecomunicaciones
- La Ley - de 19 de diciembre, de firma electrónica
- La Ley de propiedad intelectual
- La Ley de propiedad industrial

UNIDAD DIDÁCTICA 3. BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN: NORMA ISO/IEC 27002

Aproximación a la norma ISO/IEC 27002
Alcance de la Norma ISO/IEC 27002
Estructura de la Norma ISO/IEC 27002
- Las cláusulas del control de seguridad
- Las principales categorías de seguridad
Evaluación y tratamiento de los riesgos de seguridad
- Evaluación de los riesgos de seguridad
- Tratamiento de los riesgos de seguridad

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com

UNIDAD DIDÁCTICA 4. POLÍTICA DE SEGURIDAD, ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE ACTIVOS

Política de seguridad de la información
- Etapas en el desarrollo de una política de seguridad de la información
- Características esenciales de una política de seguridad de la información
- Documento de política de la seguridad de la información
- Revisión de la política de seguridad de la información

Organización de la seguridad de la información
Organización interna de la seguridad de la información
- Compromiso de la dirección con la seguridad de la información
- Coordinación de la seguridad de la información
- Asignación de responsabilidad de seguridad de la información
- Autorización de procesos para facilidades procesadoras de la información
- Acuerdos de confidencialidad para la protección de la información
- Contacto con las autoridades y con grupos de interés especial en los incidentes de seguridad
- Revisión independiente de la seguridad de la información

Grupos o personas externas: el control de acceso a terceros
- Identificación de los riesgos de seguridad relacionados con personas externas
- Tratamiento de la seguridad de la información en las relaciones con los clientes
- Tratamiento de la seguridad de la información en acuerdos con terceros

Clasificación y control de activos de seguridad de la información
Responsabilidad por los activos de seguridad de la información
- Inventario de los activos de seguridad de la información
- Propiedad de los activos de seguridad de la información
- Uso aceptable de los activos de seguridad de la información

Clasificación de la información
- Lineamientos de clasificación de la información
- Etiquetado y manejo de información

UNIDAD DIDÁCTICA 5. SEGURIDAD FÍSICA, AMBIENTAL Y DE LOS RECURSOS HUMANOS

Seguridad de la información ligada a los recursos humanos
Medidas de seguridad de la información antes del empleo
- Establecimiento de roles y responsabilidades de los candidatos
- Investigación de antecedentes de los candidatos para el empleo
- Términos y condiciones del empleo

Medidas de seguridad de la información durante el empleo
- Responsabilidades de la gerencia o dirección de la organización

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com

- Conocimiento, educación y capacitación en seguridad de la información
- Incumplimiento de las previsiones relativas a la seguridad de la información: el proceso disciplinario

Seguridad de la información en la finalización de la relación laboral o cambio de puesto de trabajo

- Responsabilidades de terminación
- Devolución de los activos
- Cancelación de los derechos de acceso a la información

Seguridad de la información ligada a la seguridad física y ambiental o del entorno

Las áreas seguras

- El perímetro de seguridad física
- Los controles de ingreso físico
- Seguridad de oficinas, locales, habitaciones y medios
- Protección contra amenazas internas y externas a la información
- El trabajo en áreas aseguradas
- Áreas de carga y descarga

Los equipos de seguridad

- Seguridad en el emplazamiento y protección de equipos
- Instalaciones de suministro seguras
- Protección del cableado de energía y telecomunicaciones
- Mantenimiento de los equipos
- Seguridad de los equipos fuera de las instalaciones
- Reutilización o retirada segura de equipos
- Retirada de materiales propiedad de la empresa
- Equipo de usuario desatendido
- Política de puesto de trabajo despejado y pantalla limpia

UNIDAD DIDÁCTICA 6. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

Aproximación a la gestión de las comunicaciones y operaciones

Procedimientos y responsabilidades operacionales

- Documentación de los procesos de operación
- La gestión de cambios en los medios y sistemas de procesamiento de información
- Gestión de capacidades
- Separación de los recursos de desarrollo, prueba y operación para reducir los riesgos de acceso no autorizado

Gestión de la prestación de servicios de terceras partes

- Política de seguridad de la información en las relaciones con los proveedores
- Requisitos de seguridad en contrato con terceros
- Cadena de suministros de tecnología de la información y de las comunicaciones

Planificación y aceptación del sistema

- Políticas para la seguridad de la información
- Revisión de las políticas para la seguridad de la información

Protección contra códigos maliciosos y móviles
- Controles contra el código malicioso
- Control contra códigos móviles

Copias de seguridad de la información

Gestión de la seguridad de la red
- Los controles de red
- La seguridad de los servicios de red
- Segregación en redes

Gestión de medios
- Gestión de medios removibles o extraíbles
- Eliminación de soportes o medios
- Soportes físicos en tránsito
- La seguridad de la documentación del sistema

El intercambio de información
- Políticas y procedimientos de intercambio de información
- Acuerdos de intercambio
- Seguridad de los soportes físicos en tránsito
- Mensajería electrónica
- Acuerdos de confidencialidad o no revelación

Los servicios de comercio electrónico
- Información relativa al comercio electrónico
- Las transacciones en línea
- La seguridad de la información puesta a disposición pública

Supervisión para la detección de actividades no autorizadas
- Registro de eventos
- Protección de la información de los registros
- La protección de la información de los registros
- Sincronización de reloj

UNIDAD DIDÁCTICA 7. EL CONTROL DE ACCESOS A LA INFORMACIÓN

El control de accesos: generalidades, alcance y objetivos

Requisitos de negocio para el control de accesos
- Política de control de acceso

Gestión de acceso de usuario
- Registro del usuario
- Gestión o administración de privilegios

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com

- Gestión de contraseñas de usuario
- Revisión de los derechos de acceso de usuario

Responsabilidades del usuario
- El uso de contraseñas
- Protección de equipos desatendidos
- Política de puesto de trabajo despejado y pantalla limpia

Control de acceso a la red
- La política de uso de los servicios en red
- Autentificación de los usuarios de conexiones externas
- Identificación de equipos en las redes
- Diagnóstico remoto y protección de los puertos de configuración
- Segregación de las redes
- Control de la conexión a la red
- El control de routing o encaminamiento de red

Control de acceso al sistema operativo
- Procedimientos seguros de inicio de sesión
- Identificación y autentificación del usuario
- El sistema de gestión de contraseñas
- El uso de los recursos del sistema
- La desconexión automática de sesión
- Limitación del tiempo de conexión

Control de acceso a las aplicaciones y a la información
- Restricciones del acceso a la información
- Aislamiento de sistemas sensibles

Informática móvil y teletrabajo
- Los ordenadores portátiles y las comunicaciones móviles
- El teletrabajo

UNIDAD DIDÁCTICA 8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Objetivos del desarrollo y mantenimiento de sistemas de información
Requisitos de seguridad de los sistemas de información
Tratamiento correcto de la información en las aplicaciones
- Validación de los datos de entrada
- El control de procesamiento interno
- La integridad de los mensajes
- Validación de los datos de salida

Controles criptográficos

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com

- Política de uso de los controles criptográficos
- Gestión de claves

Seguridad de los archivos del sistema

- Control del software en explotación
- Protección de los datos de prueba en el sistema
- El control de acceso al código fuente de los programas

Seguridad de los procesos de desarrollo y soporte

- Procedimientos para el control de cambios
- Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo
- Restricciones a los cambios en los paquetes de software
- Entorno de desarrollo seguro
- Externalización de software por terceros

Gestión de la vulnerabilidad técnica

UNIDAD DIDÁCTICA 9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Y DE LA CONTINUIDAD DEL NEGOCIO

La gestión de incidentes en la seguridad de la información

Notificación de eventos y puntos débiles en la seguridad de la información

- Notificación de los eventos en la seguridad de la información
- Notificación de puntos débiles de la seguridad

Gestión de incidentes y mejoras en la seguridad de la información

- Responsabilidades y procedimientos
- Aprendizaje de los incidentes de seguridad de la información
- Recopilación de evidencias

Gestión de la continuidad del negocio

Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

- Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
- Continuidad del negocio y evaluación de riesgos
- Desarrollo e implantación de planes de continuidad del negocio que incluyan la seguridad de la información
- Marco de referencia para la planificación de la continuidad del negocio
- Pruebas, mantenimiento y reevaluación de los planes de continuidad

UNIDAD DIDÁCTICA 10. CUMPLIMIENTO DE LAS PREVISIONES LEGALES Y TÉCNICAS

Cumplimiento de los requisitos legales

- Normativa aplicable
- Derechos de propiedad intelectual

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com

- Protección de registros organizacionales
- Privacidad de la información personal
- Prevención del mal uso de los medios de procesamiento de la información
- Regulación de los controles criptográficos

Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico
- Cumplimiento de las políticas y estándares de seguridad
- Verificación del cumplimiento técnico

Consideraciones de la auditoría de los sistemas de información
- Controles de auditoría de los sistemas de información
- Protección de las herramientas de auditoría de los sistemas de información

MÓDULO 2. EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 11. LA NORMA UNE-EN-ISO/IEC 27001:2017

Objeto y ámbito de aplicación
Relación con la Norma ISO/IEC 27002:2009
Definiciones y términos de referencia
Beneficios aportados por un sistema de seguridad de la información
Introducción a los sistemas de gestión de seguridad de la información

UNIDAD DIDÁCTICA 12. IMPLANTACIÓN DEL SISTEMA DE SEGURIDAD EN LA ORGANIZACIÓN

Contexto
Liderazgo
Planificación
- Acciones para tratar los riesgos y oportunidades
- Objetivos de seguridad de la información y planificación para su consecución

Soporte

UNIDAD DIDÁCTICA 13. SEGUIMIENTO DE LA IMPLANTACIÓN DEL SISTEMA

Operación
Evaluación del desempeño
- Seguimiento, medición, análisis y evaluación
- Auditoría interna
- Revisión por la dirección

Mejora

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com

- No conformidad y acciones correctivas
- Mejora continua

CL. Laguna del Marquesado Nº 10
28021 - Madrid
910 382 879
cursos@ceinla.com
www.ceinla.com