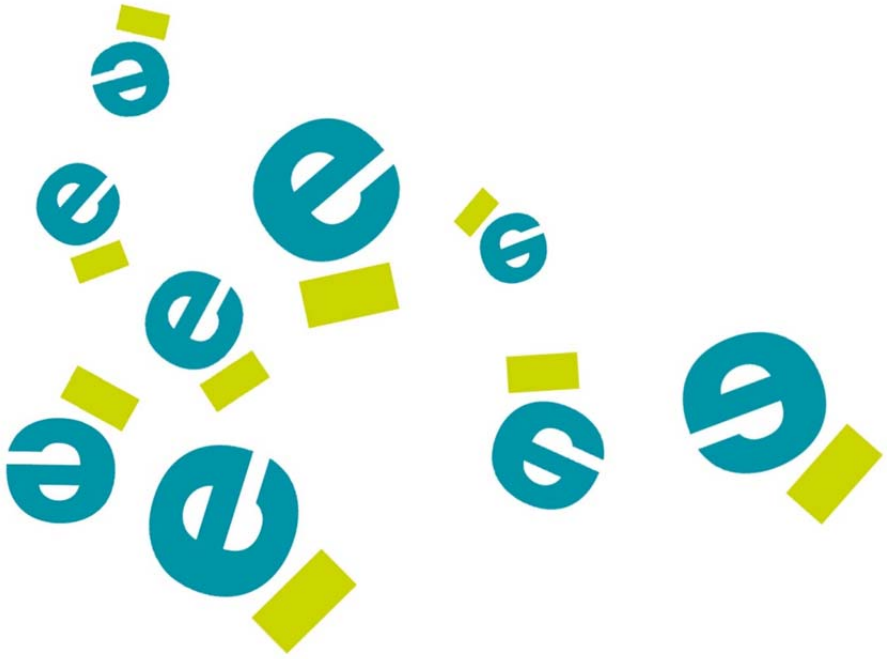

TÉCNICO EN GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

formación y aprendizaje

VNiVERSiDAD D SALAMANCA

Fundación Germán Sánchez Ruipérez

1. DESCRIPCIÓN

La Ley de Servicios de Sociedad de la Información y Comercio Electrónico (LSSICE) y la Ley Orgánica de Protección de Datos de carácter personal (LOPD) son dos leyes que garantizan fundamentalmente los derechos de los ciudadanos en relación con el uso de ellos (empresas y organizadores) en relación con el uso de estos datos y con la gestión de la información.

La información se ha convertido en uno de los principales activos de las empresas y por ello las nuevas tecnologías de la información y la comunicación se han convertido en una herramienta imprescindible para desarrollar cualquier actividad económica. Por ello, las organizaciones son responsables de la protección de la información que gestionan ante las amenazas de este entorno y deben, por todos los medios disponibles, garantizar su confidencialidad, integridad y disponibilidad.

Todo ello nos lleva a una percepción de creciente preocupación por todos los aspectos relacionados con la seguridad. Todas las organizaciones, públicas o privadas, grandes o pequeñas, se enfrentan día a día a amenazas contra sus recursos informáticos, con elevado riesgo de sufrir incidentes de alto impacto en su actividad.

Ante estas circunstancias, las organizaciones han de establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio, primando la protección de la información.

Para proteger la información de una manera coherente y eficaz es necesario implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema es una parte del sistema global de gestión de la organización, basado en una aproximación de los riesgos del negocio (actividad) para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.

La Norma ISO 27001 es la norma encargada de especificar los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica.

2. OBJETIVOS

El Objetivo es transmitir los fundamentos generales de la normativa reguladora de la protección de datos de carácter personal y de la normativa relativa a la prestación de servicios de la sociedad de la información, así como establecer las pautas de actuación para su implantación y adaptación en las organizaciones y empresas.

Con este curso el alumno como resultados del aprendizaje aprenderá a:

- conocer y comprender los requisitos legales exigibles, así como los derechos y obligaciones de las partes implicadas.
- identificar de forma práctica las exigencias que impone la ley a las organizaciones en su implantación: determinar obligaciones y responsabilidades.
- desempeñar buenas prácticas empresariales en la gestión de la seguridad de la información en relación con la adaptación e implantación de LOPD y la LSSICE en las organizaciones.

Otro objetivo es introducirse en los conceptos básicos de la gestión de la seguridad informática y de la seguridad de la información en las organizaciones, así como determinar las principales medidas de seguridad técnicas y buenas prácticas que garantizan la seguridad frente a las amenazas y riesgos, tanto de los sistemas informáticos como en Internet.

También:

- Aprender a diseñar un SGSI.
- Conocer los requisitos de la Norma ISO 27001.
- Conocer de forma práctica qué procedimientos hay que poner en marcha para implantar un SGSI conforme a las Normas ISO 27001.

3. PROFESORADO

Juan Adolfo Mogrovejo Espinosa

Diplomado en Relaciones Laborales. Técnico-consultor responsable del área de seguridad de la información y protección de datos en Grupo PM Consultores. Experiencia de 3 años, en implantación de la LOPD y auditorias, asesorando cartera de clientes de más de 200 empresas.

Marta Medina Palencia

Licenciada en Derecho. Técnico-consultor del área de seguridad de la información y protección de datos en Grupo PM Consultores. Experiencia en la implantación de LOPD a más de 50 empresas.

Oscar de la Cuesta

Ingeniero técnico Informático. Responsable del área de consultoría de Tecnologías de la Información en PM Consultores. Master IT, grupo SP en colaboración con el CEREM; Diplomado en Informática de Gestión (Analista programador), Escuela Universitaria de Sistemas Informáticos, Valladolid; C.I.N.T. (Cambridge Information Technology), Universidad de Cambridge. Técnico Programador de Sistemas. Centro de Estudios y Técnicas Informáticas. Técnico Superior en Sistemas de Telecomunicaciones e Informáticos. Asesoramiento a más de 50 empresas en diferentes áreas y tecnologías.

Raúl Cortijo Casado

Licenciado en Ciencias Económicas y Empresariales, sección Empresa, especialidad en Dirección Comercial. Especialista en Gestión por procesos y auditoria de sistemas de Gestión de la Calidad conforme a las Normas ISO 9001. Ha sido responsable de Calidad y Medioambiente en grupo de empresas del sector industrial. Desde el año 2004 es Consultor y auditor en PM Consultores, donde desempeña sus funciones de consultoría y formación para pymes en materia de sistemas de gestión de calidad, medio ambiente, I+D+i, LOPD y formación, con una experiencia acreditada de más de 50 empresas asesoradas y certificadas en diferentes sectores.

Todos son especialistas expertos en la asistencia técnica y asesoramiento para la implantación en las empresas y organizaciones de la Protección de datos y el cumplimiento de obligaciones legales en materia de protección de datos de carácter personal en el marco de la LOPD y la LSSICE en las áreas afectadas, tanto en aspectos organizativos, como tecnológicos y jurídicos.

4. FECHAS

INICIO	FIN
20/09/2011	23/12/2011

5. NÚMERO DE PLAZAS:

25 Plazas

6. DESTINATARIOS

Este curso se enmarca dentro del área profesional de Protección de Datos y Seguridad de la información. Esta disciplina afecta a un amplio espectro de diferentes profesionales y técnicos, con necesidades generales y específicas en conocer cuáles son los riesgos que afectan a la seguridad de la información y qué medidas se pueden poner en práctica.

Este curso está dirigido de forma general a:

- Cualquier persona interesada en la seguridad de la información, tanto a nivel personal como de empresa.

De forma particular:

- Responsables y gestores de la Seguridad de la Información en la empresa
- Gestores de la calidad en las organizaciones

7. PRECIO

El precio del técnico es de 450 €

8. DURACIÓN

120 Horas

9. PROGRAMA COMPLETO DEL CURSO

Protección de datos y servicios de la sociedad de la información

Módulo I. La Ley de Protección de Datos de carácter personal (LOPD) y su adaptación en las organizaciones

Unidad 1. Introducción: Datos de carácter personal y protección de datos
1.1. La protección de datos como derecho fundamental del ciudadano
1.2. Los datos personales
1.3. La adaptación del entorno empresarial a la protección de datos
1.4. ¿Qué es la protección de datos?: objeto y ámbito LOPD
1.5. Conceptos básicos
1.6. La Agencia Española de Protección de Datos (AEPD)

Unidad 2. Principios y obligaciones de la protección de datos.
2.1. Titularidad de los datos
- 2.1.1. Calidad de los datos
- 2.1.2. Informar en la recogida de datos
- 2.1.3. Solicitar el consentimiento de la persona afectada
- 2.1.4. Datos especialmente protegidos
- 2.1.5. Seguridad de los datos
- 2.1.6. Deber de secreto
- 2.1.7. Comunicación de datos
- 2.1.8. Acceso por cuenta de terceros

Unidad 3. Documento e Seguridad.
3.1. Introducción: la evaluación de la seguridad
3.2. El documento de seguridad

Unidad 4. Derechos de los afectados.
4.1. Introducción
4.2. Derecho de información en la recogida de datos
4.3. Derecho de impugnación
4.4. Derecho de consulta al Registro Central
4.5. Derecho de acceso
4.6. Derechos de rectificación y cancelación
4.7. Derecho de oposición

Unidad 5. Infracción y sanciones
5.1. Introducción
    5.1.1. Juego de asociación
5.2. Inmovilización de los ficheros

Unidad 6. Notificación e inscripción de ficheros
6.1. Notificación e inscripción de ficheros

Unidad 7. Auditorías periódicas
7.1. Auditorías periódicas

Unidad 8. Implantación de la LOPD en la empresa: resumen
8.1 Eliminar tópicos
8.2. Claves para la adaptación a la LOPD en las empresas
8.3. Entonces, ¿qué debemos hacer?
8.4. Legislación aplicable

Módulo II. La Ley de Servicios de Sociedad de la Información y Comercio electrónico (LSSICE) y su adaptación en las organizaciones

Unidad 1. ¿Qué es la LSSICE?
1.1. Introducción
1.2. Marco Normativo regulación de los servicios
1.3. Regulación de servicios prestados de la sociedad de la información
1.4. Ámbito de aplicación
1.5. Libertad de prestación de servicios de la sociedad de la información
1.6. Códigos de conducta

Unidad 2. Prestadores de servicios de la sociedad de la información
2.1. Introducción
2.2. Obligaciones
2.3. Responsabilidades
2.4. Comunicaciones comerciales por vía electrónica
2.5. Contratación electrónica
    2.5.1. Ejemplo práctico de venta electrónica: Tienda On Line de El Corte Inglés

Unidad 3. Solución extrajudicial de conflictos
3.1. Solución extrajudicial de conflictos

Unidad 4. Régimen sancionador
4.1. Régimen sancionador

Unidad 5. Como afecta la LOPD a la LSSICE
5.1. Introducción
5.2. Obtención de datos
5.3. Derechos del cliente
5.4. Comunicaciones electrónicas
5.5. Medidas de seguridad
5.6. Acceso a los datos por cuenta de terceros
5.7. Comunicaciones o cesiones de datos personales
5.8. Transferencias internacionales de datos
5.9. Actividades delictivas más comunes

Unidad 6. Adaptación de una página web a la LSSICE
6.1. Introducción
6.2. Adaptación de una web sin contratación electrónica
6.3. Adaptación de una web con contratación electrónica

Unidad 7. Casos Prácticos
Caso 1. Gestión de dominio
Caso 2. Gestión de mi web
Caso 3. Mi página web carece de política de privacidad y aviso legal
Caso 4. En mi página web se han detectado incidencias en los formularios
Caso 5. En mi página web se han detectado incidencias en links
Caso 6. En mi página web se han detectado incidencias en el uso de la imagen
Caso 7. Incidencia en la publicidad realizada por correo electrónico

Técnicas en seguridad informática y de la información

Módulo 1. Introducción a la Gestión de la Seguridad de la Información
1.1. Antecedentes: el porqué de la Seguridad
1.2. Concepto de seguridad informática
1.3. Amenazas informáticas y riesgos
    1.3.1. Amenazas
    1.3.2. Riesgos
1.4. Medidas y controles de seguridad ante las amenazas: salvaguardas
1.5. Seguridad en los Sistemas Informáticos: ¿qué debemos proteger?
    1.5.1. Ficheros de datos
    1.5.2. Programas
    1.5.3. Soportes
    1.5.4. Equipos
    1.5.5. Usuarios
    1.5.6. Accesos de redes
1.6. Política de seguridad

Módulo 2. Tecnologías básicas y buenas prácticas para garantizar la Seguridad en los sistemas informáticos

2.1. Introducción
2.2. Acceso a los sistemas: Usuarios y Contraseñas
2.3. Protección de la información: copias de seguridad (backup o copias de respaldo)
2.4. Mantenimiento del software: Parches
2.5. Protección eléctrica: Sistemas de alimentación ininterrumpida (SAI)
2.6. La Red local: Instalación y seguridad física
    2.6.1. Red local: rack y cableado
    2.6.2. Ordenadores portátiles
    2.6.3. Redes inalámbricas
2.7. Protección contra los virus

Módulo 3. Tecnologías básicas y buenas prácticas para garantizar la Seguridad en Internet

3.1. Introducción
3.2. Seguridad asociada a la conexión a Internet
    3.2.1. Protección contra virus informáticos
    3.2.2. Protección contra Spyware o programas espías
    3.2.3. Control de accesos: cortafuegos o firewall
3.3. Seguridad asociada a la navegación en Internet
    3.3.1. Cookies
    3.3.2. Protección contra Dialers
    3.3.3. Control de Pop-ups o elementos emergentes
    3.3.4. Protección contra contenido no recomendable: filtros
    3.3.5. Protección contra el Pharming
    3.3.6. Consejos generales de navegación
3.4. Seguridad asociada al uso del correo electrónico
    3.4.1. Protección contra el Spam
    3.4.2. Protección contra el Phising
    3.4.3. Protección contra el Carding
    3.4.4. Privacidad de la información y la firma digital
    3.4.5. Protección contra los virus transmitidos a través del correo.
    3.4.6. Consejos Generales de uso del correo electrónico
3.5. Seguridad asociada al uso de la banca y del comercio electrónico
    3.5.1. Páginas seguras (HTTPS): servidores seguros
    3.5.2. Autentificación en Internet: programas de firma y certificado digital
    3.5.3. Consejos generales de uso de la banca electrónica / comercio electrónico
3.6. Otras amenazas, fraudes y delitos en Internet

Módulo 4. Guía práctica. Resumen de amenazas, riesgos y soluciones

4.1. Guía práctica. Resumen de amenazas, riesgos y soluciones
4.2. Comprobación de la Seguridad: los programas de test
    4.2.1. Comprobación de la seguridad a través de programas
    4.2.2. Comprobaciones on line de seguridad

Diseño e implementación de un sistema de gestión de la seguridad de la información (SGSI) conforme a las normas ISO 27001

Introducción y objetivos

Módulo 1. Integración de la gestión de la seguridad de la información en el sistema de gestión de la organización

1.1. Marco normativo
1.2. La gestión de la seguridad en el sistema general de gestión de la organización

Módulo 2. Requisitos del sistema de Gestión de la seguridad de la información (SGSI) conforme a la norma ISO 27001: definición, estructura y gestión

2.1. Requisitos generales
2.2. Diseño y planificación del SGSI
2.3. Requisitos de documentación
    2.3.1. Control de documentos
    2.3.2. Control de registros
2.4. Compromiso de la dirección
2.5. Gestión de los recursos
2.6. Formación
2.7. Auditorías internas
2.8. Revisión por la dirección
    2.8.1. Entradas a la revisión
    2.8.2. Salidas de la revisión
2.9. Mejora continua
    2.9.1. Acción correctiva
    2.9.2. Acción preventiva
2.10. Glosarios de términos

Módulo 3. Implementación del SGSI conforme a la norma ISO 27001

3.1. Puesta en marcha
    3.1.1. Planificación
    3.1.2. Implantación
    3.1.3. Revisión y mejoras
3.2. Los controles de seguridad: la ISO 27002
    3.2.1. Política de seguridad
    3.2.2. Aspectos organizativos de la seguridad de la información
    3.2.3. Gestión de activos
    3.2.4. Seguridad ligada a los recursos humanos
    3.2.5. Seguridad física y ambiental
    3.2.6. Gestión de comunicaciones y operaciones
    3.2.7. Control de acceso
    3.2.8. Adquisición, desarrollo y mantenimiento de sistemas de información
    3.2.9. Gestión de incidencias

10. METODOLOGÍA

Todos nuestros cursos se basan en una metodología encaminada a favorecer un aprendizaje autónomo e interactivo, en la que nuestra máxima es conseguir que el alumno aprenda a través del estudio y la práctica ("Learning by doing"). Por ello, favorecemos el aprendizaje colaborativo, fomentando la interactividad entre los propios estudiantes y de estos con el equipo docente.

En nuestros programas formativos **el alumno es el verdadero protagonista** y el tutor le acompaña, a modo de guía o mentor, en su proceso de aprendizaje.

Nuestros estudiantes encuentran en sus aulas virtuales todo lo que necesitan para seguir de una forma óptima los cursos: tablón de anuncios, programa del curso, fichas de aprendizaje, material de apoyo, espacios para consultas y reflexión, etc.

Todos estos materiales educativos son desarrollados por un equipo de expertos y pedagogos de acuerdo a una planificación metodológica exhaustiva. Los usuarios disponen de fichas de contenido multimedia, simulaciones, demostraciones, visitas web guiadas, y un gran abanico de actividades que refuerzan su aprendizaje.

Para llevar a cabo esta tarea, nuestro campus, cuenta con una serie de **herramientas de comunicación** y colaboración que convierten las acciones formativas en, sencillas, amenas y, sobre todo, dinámicas. Estas herramientas son: los foros de debate, chats, wikis, mensajería interna, correo electrónico, etc.

11. EVALUACIÓN

La evaluación se llevará a cabo a través de ejercicios de evaluación de corrección automática, participación en actividades de comunicación (foros de debate, chats) y la redacción de breves trabajos.

12. CERTIFICACIÓN

A la finalización de este curso el alumno recibirá un certificado emitido por la Universidad de Salamanca y la Fundación Germán Sánchez Ruipérez, que garantiza que el mismo se ha desarrollado bajo principios de solidez metodológica, excelencia científica y reconocido prestigio de los expertos, tutores y autores de contenido.

13. CALIDAD

El Centro Internacional de Tecnologías Avanzadas de la Fundación Germán Sánchez Ruipérez es una entidad registrada en AENOR (ER.1052/2007) y certificada por la norma ISO 9001:2008.

14. INSCRIPCIÓN Y MATRÍCULA

Puede realizar la preinscripción en el curso a través del Campus Virtual de Formación y Aprendizaje.

Para ello haga clic en el siguiente enlace:

Formulario de preinscripción del curso

y, posteriormente, rellene el formulario al que será remitido. La preinscripción no le compromete a nada. Para confirmar su plaza deberá hacer efectivo el pago del curso.

15. CONTACTO

Para cualquier duda o cuestión relativa al curso, puede ponerse en contacto con nosotros a través del teléfono:

Formación y Aprendizaje Directo (España): **902 11 26 81**

International Calling: **(34) 923 19 73 30**

Fax: **923 54 14 12**

Mediante el correo electrónico: cursos@formacionyaprendizaje.com