

Seminario

INTENSIVO

Domine los principales aspectos legales, tecnológicos y organizativos asociados a la gestión efectiva de la seguridad de la información

Cómo diseñar e implantar el PLAN de SEGURIDAD de Sistemas de Información



¡Obtenga el máximo rendimiento a su inversión en seguridad y evite errores estratégicos!

7 MODULOS DE FORMACION INTENSIVA

- ▶ REQUERIMIENTOS LEGALES
- ▶ POLITICA DE SEGURIDAD
- ▶ ANALISIS Y TRATAMIENTO DE RIESGOS
- ▶ PLAN DIRECTOR DE SEGURIDAD
- ▶ SISTEMA DE GESTION DE SEGURIDAD
- ▶ AUDITORIAS DE CUMPLIMIENTO
- ▶ CERTIFICACION DEL SISTEMA DE GESTION DE LA INFORMACION

- **Obligaciones legales** en materia de seguridad de los Sistemas de Información: **LOPD, LSSI, Código Penal, LGT**
- Establecimiento de mecanismos para reducir el **riesgo residual** a **niveles asumibles** por la dirección
- Definición de las metas de seguridad a alcanzar mediante un **Plan Director de Seguridad** y medición del **cumplimiento de objetivos**
- Elaboración de una **Política de Seguridad** según leyes, reglamentos, normas y usos comúnmente aceptados
- Preparación para conseguir la certificación **UNE 71502/ 17799**

MADRID 22 y 23 de Mayo de 2007
Hotel NH Príncipe de Vergara

>>>> Inscríbese ahora
902 12 10 15

Madrid 22 y 23 de MAYO de 2007

Programa

MODULO 1

Requerimientos legales para la SEGURIDAD DE LA INFORMACION

En este módulo se analizarán las leyes, reglamentos y normas que regulan las actuaciones en materia de seguridad de la información. Se identificará el alcance legal y las consecuencias de su incumplimiento por parte de los distintos agentes que intervienen y el cambio de escenario de trabajo que suponen.

- Cuáles son los principios legales y normativos de la seguridad de la información: LOPD, Código Penal, LGT y LSSICE
- Cuál es el tratamiento de la confidencialidad y la seguridad por la legislación española
- Cómo hacer la auditoría previa de situación
- El Plan Director de Seguridad: autorregulación u obligación legal
- Diseño legal del Plan: seguridad interna y seguridad externa
- Aspectos a tener en cuenta en la elaboración y desarrollo del Plan: seguridad legal, comercio electrónico, propiedad intelectual, la salvaguarda de registros y la protección de pruebas
- Mantenimiento de la seguridad legal: auditoría como obligación legal (art. 17 del Real Decreto 994/1999)
- ISO /IEC 17799 y 71502: un sistema certificable de gestión de seguridad de la información con marco legal
- Cuáles son las consecuencias legales por falta de seguridad
- Quiénes son los agentes responsables legalmente en la gestión de seguridad

MODULO 2

Política de SEGURIDAD DE LA INFORMACION

Durante esta sesión se analizará el entorno en el que una organización debe definir su Política de Seguridad y los criterios que debe tener en cuenta a la hora de establecerla, analizando el marco de leyes, reglamentos y estándares con los que se puede encontrar a la hora de hacerlo y teniendo en cuenta la necesidad de alinear esta política con los objetivos de la organización.

- Análisis del entorno en el que se define la Política de Seguridad

Horario

- 9.15 h. Recepción de los asistentes
- 9.30 h. Apertura
- 11.30 - 12.00 h. Café
- 14.30 - 15.30 h. Almuerzo
- 18.00 h. Fin de la Jornada



- Marco de estándares y normas
 - Sistemas de Gestión
 - Códigos de buenas prácticas
 - Certificación de productos y servicios
 - Leyes y reglamentos
- Definición de conceptos clave
 - Definición de Seguridad
 - Activos de información y su valor
 - Normativas
 - Monitorización y Sistemas de Gestión en tiempo real
 - Otros
- Cómo se plasma la Política de Seguridad:
 - Normas internas de seguridad de la información
 - Dotación de recursos para implantar y hacer cumplir las normas
- Claves del éxito

MODULO 3

ANALISIS Y TRATAMIENTO DE RIESGOS

Durante esta sesión se proporcionarán las directrices para evaluar la seguridad de la información desde el punto de vista de los riesgos a que esta se ve sometida, marcando además pautas para aplicar metodologías y estrategias para llevar a la organización a niveles de riesgo asumibles por su Dirección.

- Estándares y referencias
 - MAGERIT
 - CRAMM
 - ISO 13335
 - NIST 800-30
- Identificación y agrupación de activos
 - Clasificación de los activos
 - Activos tangibles e intangibles
 - La información como un activo crítico
- Identificación y evaluación de amenazas
- Identificación y estimación de vulnerabilidades
- Identificación y valoración de impactos
- Evaluación del riesgo
 - Aproximaciones. Escenarios de siniestro
- Reducción del riesgo
 - Selección de salvaguardas
 - Control del riesgo residual

MODULO 4

PLAN DIRECTOR DE SEGURIDAD

El Plan Director de Seguridad define, en la práctica, la forma y el plazo en el que una organización pasa de un estado actual, desde el punto de vista de la seguridad de la información, a un estado objetivo marcado en su base por la Política de Seguridad. En este bloque se analizará la importancia de disponer de un Plan Director de Seguridad, cómo diseñarlo y como deben planificarse las actuaciones en base al resultado del análisis de riesgos.

- Definición del Plan Director de Seguridad
- Planificación de las actuaciones derivadas del Plan Director de Seguridad
- Matriz de riesgos
- Plan de formación y concienciación
- Métricas: medición del estado de seguridad en términos de negocio
- Cuadro de mando: gestión del plan de seguridad

MODULO 5

Sistema de Gestión de SEGURIDAD DE LA INFORMACION

En este módulo se definirán los ejes del Sistema de Gestión de Seguridad de la Información a implantar en la organización a partir de los objetivos marcados en el Plan Director de Seguridad, cubriendo los diferentes dominios de control identificados por la norma ISO 17799:2005.

- La norma ISO 17799:2005
- Dominios y objetivos de control
- Aspectos organizativos:
 - Recursos humanos
 - Organización de la seguridad
 - Funciones y responsabilidades
 - Gestión de incidentes de seguridad
- Aspectos lógicos:
 - Control de acceso
 - Gestión de redes y comunicaciones
 - Gestión de sistemas
 - Protección lógica
 - Monitorización y control lógico. Debilidades lógicas
 - Desarrollo y mantenimiento de sistemas de información
- Aspectos físicos:
 - Definición de seguridad física
 - Seguridad ambiental
 - Seguridad de los sistemas
 - Áreas seguras y públicas
- Aspectos legales: cumplimiento legal
- Continuidad del negocio

- Implantación de controles
 - Eficacia y eficiencia de los controles
 - Conformidad técnica
- Alineación con el negocio.
 - Objetivos estratégicos
 - Retorno de la inversión
 - Beneficios directos e indirectos

MODULO 6

AUDITORIAS DE CUMPLIMIENTO

En este módulo se definirán metodologías y procedimientos para llevar a cabo las auditorías de cumplimiento implicadas en un SGSI con el propósito de garantizar el cumplimiento de los objetivos propuestos en la planificación e implantados en el sistema de gestión.

- Normas generales de auditoría
- El equipo auditor: cualificación e independencia
- Auditoría ISO 17799:2005
 - Niveles de cumplimiento ISO 17799
 - Desviaciones con respecto al estándar
 - Acciones correctoras
- Auditoría bienal RMS

MODULO 7

Certificación del Sistema de Gestión de la Información (SGSI) INTEGRACION CON OTROS SISTEMAS DE GESTION

La Seguridad no es un producto, tampoco es un proyecto, es un proceso. En este módulo se revisará el proceso de certificación del SGSI según las normas ISO 27001/UNE 71502, una garantía continua de calidad de la seguridad en la organización que reporta enormes beneficios a la misma y la hace más competitiva en su sector de negocio.

- La seguridad como proceso
- La certificación del Sistema de Gestión de Seguridad de la Información
 - El proceso de certificación
 - Reconocimiento vs. objetivo
- Calidad de la seguridad
- El ciclo de mejora continua: PDCA
 - Auditoría y control del sistema de gestión
 - No conformidades y desviaciones
 - Acciones correctoras
- Beneficios para la organización
- Integración del SGSI con otros sistemas de gestión:
 - Sistemas de gestión TIC: ITIL
 - Otros sistemas de gestión: calidad, medioambiente

IIR Certified Technical Trainer



Todos los instructores que poseen la certificación CTT por IIR España han sido previamente seleccionados tanto por su experiencia y colaboración en proyectos tecnológicos y de comunicaciones, como por su capacidad didáctica y habilidades de comunicación.

Este distintivo reconoce la destacada labor desempeñada como formador experimentado con IIR España y así mismo la valoración excelente de los propios asistentes.

En los Seminarios IIR en los que encuentre instructores avalados por la certificación CTT, ya sabe que el interés del tema así como la forma de presentarla está garantizado.

Un seminario IIR con un instructor CTT, le garantiza:

- Formación teórico-práctica de alta calidad
- Metodología interactiva en función de sus necesidades formativas
- Máximo nivel de satisfacción

Planifica tu FORMACION PARA 2007

- **IT METRICS**
Madrid, 10 y 11 de Abril
- **Análisis de Riesgos para CPD**
Madrid, 11 y 12 de Abril
- **SLA**
Madrid, 24 y 25 de Abril
- **VAL IT**
Madrid, 25 y 26 de Abril
- **ITIL**
Madrid, 8 y 9 de Mayo
- **Acuerdos de Distribución de IT**
Madrid, 24 y 25 de Mayo
- **Archivo Digital**
Madrid, 29 y 30 de Mayo
- **Plan de Continuidad de Negocio**
Madrid, 29 y 30 de Mayo
- **Autenticación de Usuarios**
Madrid, 30 y 31 de Mayo
- **Tipos de replicación de CPDs**
Madrid, 5 y 6 de Junio

Más información www.iir.es/it



Nuestros instructores



Ana Marzo Portera

Abogado socio fundador de Equipo Marzo y Marzo&Abogados. Especialista en derecho de las nuevas tecnologías con amplia experiencia en seguridad legal en protección de datos y contratación informática.

Asesor Jurídico de la Asociación de Usuarios SAP España (AUSAPE) y colaborador con la Fundación Arte y Derecho para la defensa de los derechos de autoría derivados de la Ley de Propiedad Intelectual. Coautora de libros como "Claves legales de Internet para la empresa", "La gestión de datos personales dentro de la empresa", "La auditoría de medidas de seguridad de la ley de protección de datos", "Contratos informáticos y electrónicos". Además en materia de protección de datos ha colaborado con la Asociación Española de Empresas de Información Comercial (ASEICO), Asociación de Publicidad Directa y Bases de Datos (PDBD) para la elaboración del Código Ético de Protección de Datos y la Asociación de Prensa Profesional (APP).



José Miguel Rosell Tejada

Ingeniero Superior Industrial por la Escuela Técnica Superior de Ingenieros Industriales de la Universidad Politécnica de Valencia.

Especialista Universitario en transporte y negocio marítimo por la Universidad Pontificia de Comillas (Instituto Universitario de Administración y Dirección de Empresas. ICADE). Actualmente es Socio Director de S2 Grupo. Consultor especializado en Seguridad de los Sistemas de Información y en Sistemas de Gestión en Tiempo Real. Ha trabajado como Director de Tecnologías de la Información y Comunicaciones de Unión Naval de Levante y como Director de Explotación de Tissat, donde fue, entre otras, Director Gerente de la UTE Tissat-Fujitsu para la explotación de InfoCentre (Centro telemático de la Generalitat Valenciana), Responsable de explotación de la plataforma de Internet de Antena 3 Interactiva, Responsable de explotación de la plataforma tecnológica de los Centros de Emergencias de Valencia y Murcia, o Responsable de explotación de la plataforma tecnológica de la tarjeta sanitaria de Valencia. Especialista en el desarrollo de auditorías del Reglamento de Medidas de Seguridad de la LOPD y de la norma ISO 17799, en la implantación de sistemas de gestión por procesos de TIC (ITIL) y de gestión de la seguridad de la información (UNE 71502, ISO 27001), en la integración de sistemas de gestión (ISO 9000, ISO 14001, OSHAS 18001, UNE 7150), en la monitorización y control de procesos (BAM y BPM), en la explotación de grandes centros tecnológicos y de servicios y en sistemas de control interno.



Antonio Villalón Huerta

Ingeniero en Informática por la Universidad Politécnica de Valencia especializado en Sistemas Operativos y Redes de Computadores. Miembro de ISACA (Information Systems Audit & Control Association) y auditor CISA (Certified Information Systems Auditor), es responsable de las áreas de Estándares e Investigación del capítulo ISACA de la Comunidad Valenciana. Especialista en seguridad lógica y gestión de la seguridad. Especialista en entornos Unix, es autor del libro "Seguridad en Unix y Redes". Actualmente es Director Técnico de Explotación de S2 Grupo, donde como responsable técnico de la línea de negocio de Seguridad de la Información ha dirigido proyectos de auditoría, consultoría e implantación para empresas de diferentes sectores, destacando entre ellos la primera certificación de la norma UNE 71502 a nivel nacional. Ha trabajado como consultor de seguridad informática en TISSAT, participando en la seguridad TIC de proyectos como 112-CV (Teléfono de Emergencias), Antena 3 Interactiva (plataforma Internet), Infocentre (Generalitat Valenciana) o InfoMarket (B2B). Ponente habitual en conferencias relacionadas con la seguridad de la información, desde sus vertientes más técnicas a sus vertientes de gestión, imparte regularmente cursos relacionados con la materia en diferentes entidades y universidades españolas y es autor de diversos artículos relativos a la gestión normalizada de la seguridad.

Quién debe asistir

- >>> Director de Informática
- >>> Director de Sistemas de Información
- >>> Director de Seguridad Informática
- >>> Auditor de S.I.
- >>> Responsable de Tecnología
- >>> Responsable de Calidad de Sistemas
- >>> Responsable de Organización

Al término del Seminario podrá

- Identificar los **agentes** responsables legalmente de la falta de seguridad
- Establecer **criterios** para identificar y valorar los **riesgos potenciales**
- Implantar **salvaguardas** para gestionar el riesgo de la organización
- Planificar, implantar y monitorizar el **Plan Director de Seguridad**
- Aplicar **criterios**, generales y específicos, para definir la **Política de Seguridad**
- Identificar las **fases, tareas y resultados** del **Disaster Recovery Plan**
- Dominar los **controles y normas de auditoría** según la ISO/IEC 17799 y 71502 el MAP y prepararse para futuras certificaciones

Comentarios de los asistentes a anteriores convocatorias

“Interesante, me ha servido como punto de partida”

Juan Carlos Alonso. Responsable de Sistemas de Información. **AUTORIDAD PORTUARIA DE A CORUÑA**

“Los ponentes son de gran nivel profesional y conocimiento de la materia”

Mª Jesús Martínez Martínez. Jefa de Sistemas de Información. **AUTORIDAD PORTUARIA DE A CORUÑA**

“Está completo, es una buena forma de coger una visión global entre servicio fiable, seguridad de acceso y jurídica”

Pedro Noelle. Explotación I+D. **SECURITAS DIRECT**

“Muy bueno y completo”

Miguel Angel Neira Sánchez. Jefe de Area Oficina de Seguridad. **DIRECCIÓN GENERAL DE LA GUARDIA CIVIL**

IIR España (Institute for International Research) es una compañía del **Grupo Informa plc**, el mayor especialista mundial en contenidos académicos, científicos, profesionales y comerciales. Cotizado en la Bolsa de Londres, Informa plc cuenta con **7.400 empleados** y está presente en **43 países** a través de **150 unidades operativas**.

- ▶ **120 líneas de negocio** distintas
- ▶ **10.000 eventos** de formación e información a través de compañías como **IIR, IBC o Euroforum**
- ▶ **2.000 productos de suscripción** que incluyen: diarios académicos, noticias en tiempo real, revistas y boletines de noticias
- ▶ **40.000 títulos académicos** en catálogo a través de marcas tan prestigiosas como **Taylor & Francis o Routledge**

Además, a través de marcas tan reconocidas como **ESI Internacional, Achieve Global, Forum o Huthwaite**, Informa es el referente mundial en soluciones estratégicas de mejora del desarrollo o **performance improvement**.

En España, IIR es líder desde hace **20 años** en el desarrollo y gestión de contenidos y eventos para empresas. Con un **equipo de 120 personas**, IIR España ofrece a sus clientes un servicio de formación e información integral con productos innovadores como los **Written Courses** (programas modulares de formación a distancia) además de:

- ▶ 500 Conferencias, Congresos y Seminarios de producción propia anuales
- ▶ 200 cursos de Formación In Company

Cómo diseñar e implantar el

PLAN de SEGURIDAD de Sistemas de Información

Fecha y lugar de celebración

Madrid • 22 y 23 de Mayo de 2007 • Hotel NH Príncipe de Vergara
Príncipe de Vergara, 92. 28006 Madrid. Tel. 91 563 26 95

Precio 1.399 € + 16% IVA

El precio incluye almuerzo, cafés y documentación

Precio Especial para Grupos

IIR ofrece precios especiales a las empresas que inscriban a 3 o más personas al mismo evento.

Para informarse, contacte con **Diana Mayo**, en el teléfono: 91 700 48 70

Cancelación

Deberá ser comunicada por escrito. Si se comunica hasta 2 días laborables antes del inicio del encuentro, se devolverá el importe menos un 10% en concepto de gastos administrativos. Pasado este periodo no se reembolsará el importe de la inscripción pero se admite la sustitución de su plaza, que deberá ser notificada por escrito hasta un día antes de la celebración del encuentro.

IIR le recuerda que la entrada a este acto únicamente estará garantizada si el pago del seminario es realizado antes de la fecha de su celebración.



Institute for International Research
Líder mundial en formación e información para empresas

902 12 10 15
91 700 48 70

91 319 62 18

www.iir.es

Príncipe de Vergara, 109
28002 Madrid

inscrip@iir.es

Boletín de Inscripción

Sí, deseo inscribirme a **PLAN DE SEGURIDAD**

Madrid • 22 y 23 de Mayo de 2007 CS0043

IIR le recuerda que la inscripción a nuestras jornadas es personal

DATOS DE LOS ASISTENTES ¡Gracias por su inscripción!

1º NOMBRE:

CARGO:

E-MAIL:

FAX DIRECTO:

TEL. DIRECTO:

MOVIL:

2º NOMBRE:

CARGO:

E-MAIL:

FAX DIRECTO:

TEL. DIRECTO:

MOVIL:

EMPRESA:

SECTOR:

CIF:

NUMERO DE EMPLEADOS EN SU OFICINA: 1-10 11-50 51-100 101-200 201-500 501-1.000 >1.000

DIRECCION DEL ASISTENTE:

POBLACION:

C.P.:

TELEFONO:

FAX:

QUIEN AUTORIZA SU ASISTENCIA:

CARGO:

RESPONSABLE DE FORMACION:

DATOS DE FACTURACION *(Rellenar sólo si la dirección de facturación es distinta a la del asistente)*

EMPRESA:

CIF:

DEPARTAMENTO:

JEFE DE CONTABILIDAD:

DIRECCION:

POBLACION:

C.P.:

TELEFONO:

FAX:

FORMA DE PAGO **IMPORTANTE** Al realizar el pago indiquen la referencia CS0043

Transferencia bancaria a la cta. 0065-0120-60-0001011755 (Barclays)

Visa Mastercard American Express Diners Club

Titular de la tarjeta

Número de la tarjeta

Caduca

Fecha y firma

Cheque a nombre de IIR España

PDF

Información

Alojamiento en Hotel

Para beneficiarse de un precio especial en el hotel correspondiente haga su reserva directamente por teléfono, indicando que está Vd. inscrito en el evento de IIR España.

Certificado de Asistencia

A todos los asistentes que lo deseen se les expedirá un Certificado Acreditativo de Asistencia a este evento.

Transportista Oficial **IBERIA**

Los asistentes a los eventos que IIR España celebre en 2007, obtendrán un descuento del 30% sobre tarifas completas en Business y un 40% sobre tarifas completas en Turista en los vuelos con Iberia (excepto para vuelos Nacionales por AIR NOSTRUM para los cuales obtendrán un 25% de descuento sobre tarifas completas Business y Turista). Para más información contacte con **Serviberia**, Tel. 902 400 500 o en cualquier delegación de Iberia y/o Agencia de Viajes Iberia, indicándole el Tour Code BT7IB21MPE0017.

Datos Personales

En cumplimiento con el artículo 5 de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, le informamos de que los datos personales que aporte en el presente formulario serán incorporados a los ficheros de "Institute for International Research España, S.L.", debidamente inscritos ante la Agencia Española de Protección de Datos, y cuyas finalidades son la gestión y cumplimiento de la relación establecida como consecuencia de la inscripción en el evento a que hace referencia, así como la gestión por parte de IIR de la selección de los asistentes al mismo, así como la realización de envíos publicitarios acerca de las actividades, servicios, ofertas, promociones especiales y de documentación de diversa naturaleza y por diferentes medios de información comercial, además de la gestión de la información de la que se disponga para la promoción de eventos, seminarios, cursos o conferencias que pudieran resultar de interés para los inscritos, de acuerdo con las labores de segmentación y obtención de perfiles relativa a los mismos, todo ello al objeto de personalizar el trato conforme a sus características y/o necesidades.

Mediante la presente, usted queda informado y consiente que sus datos puedan ser cedidos a patrocinadores, publicaciones, expositores en ferias u otros sujetos en base a la relación que IIR mantiene con los mismos para procurar una mayor eficiencia de la gestión de sus actividades.

Para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de sus datos por parte de IIR, deberá remitir un escrito identificado con la referencia "Protección de Datos" a "Institute for International Research España, S.L.", con domicilio social en la calle Príncipe de Vergara nº 109, 28002 Madrid, en el que se concrete la solicitud y al que acompañe fotocopia de su Documento Nacional de Identidad.

IIR Doc

No puedo asistir a estas Jornadas

Estoy interesado en su documentación

Busque la información estratégica más relevante de su sector en www.iir.es/doc
Más de 700 documentaciones inéditas de eventos celebrados por IIR disponibles para Vd.