

MÁSTER Y EXPERTO UNIVERSITARIO EN EL DESARROLLO DE SISTEMAS PARA EL COMERCIO ELECTRÓNICO

Avances en Seguridad Aplicada al Comercio Electrónico

Auditoria Informática y Aspectos Legales

Juan Manuel Corchado Rodríguez
Javier Bajo Pérez
Sara Rodríguez González
Juan Francisco de Paz Santana
Fernando de la Prieta Pintado
Oscar Gil Gonzalo
Davinia Carolina Zato Domínguez

<http://master-ecom.usal.es>



UNIVERSIDAD
DE SALAMANCA

Telefónica

TELEFÓNICA
INVESTIGACIÓN Y DESARROLLO

Telefónica

Móviles

Matchmind[↑]

Ideas & Technology for Business

EXPERTO UNIVERSITARIO EN EL DESARROLLO DE SISTEMAS PARA EL COMERCIO ELECTRÓNICO

Avances en Seguridad Aplicada al Comercio Electrónico

Seguridad en Redes y Desarrollo Seguro de Aplicaciones Seguras

<http://master-ecom.usal.es>

Juan Manuel Corchado Rodríguez

Javier Bajo Pérez

Sara Rodríguez González

Juan Francisco de Paz Santana

Fernando de la Prieta Pintado

Oscar Gil Gonzalo

Davinia Carolina Zato Domínguez



UNIVERSIDAD
DE SALAMANCA

BISITE

Biomedicina, Sistemas Inteligentes, Tecnología Educativa
Grupo de Investigación

Patrocinadores y Colaboradores:

Telefónica

TELEFÓNICA
INVESTIGACIÓN Y DESARROLLO

Telefónica
Móviles

Matchmind[↑]
Ideas & Technology for Business

centro
de innovación
en movilidad
Microsoft

dycec
sólo soluciones

cedetel
TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

flag
solutions

oxxigeno

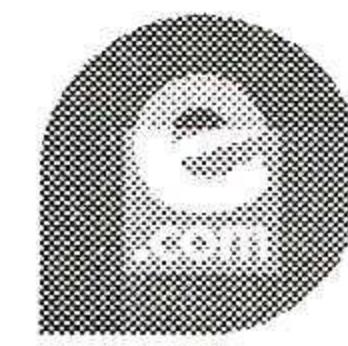
CERTYRED
CERTIFICACIÓN PROFESIONAL
Seguridad en Internet



Unkasoft®

Panda
Software

GPM
INNOVACIÓN
Y DESARROLLO



Contenido

1	Introducción a la auditoría informática	7
1.1	El concepto de auditoría	7
1.2	Auditoría contra consultoría	8
1.3	Auditoría informática.....	10
1.4	Metodologías de evaluación de sistemas	11
1.5	Metodologías más comunes	12
1.6	Auditoría de seguridad	14
2	ISO 27001	14
2.1	Podemos certificar una ISO 27001	15
2.2	Historia.....	15
2.3	Términos y definiciones	15
2.3.1	Seguridad de la información.....	15
2.3.2	Evaluación del Riesgo.....	16
2.3.3	Gestión del Riesgo	16
2.4	Dominios de Control ISO 27002.....	16
2.4.1	Política de seguridad	17
2.4.2	Aspectos organizativos para la seguridad	17
2.4.3	Clasificación y control de activos	18
2.4.4	Seguridad ligada al personal	18
2.4.5	Seguridad física y del entorno	19
2.4.6	Gestión de comunicaciones y operaciones	19
2.4.7	Control de accesos.....	20
2.4.8	Desarrollo y mantenimiento de sistemas	20
2.4.9	Respuesta a incidentes	21
2.4.10	Gestión de continuidad de negocio.....	21
2.4.11	Conformidad con la legislación	21
2.5	Objetivos de control	22
2.5.1	Política de seguridad	22
2.5.2	Aspectos organizativos para la seguridad	22
2.5.3	Clasificación y control de activos	22
2.5.4	Seguridad ligada al personal	22
2.5.5	Seguridad física y del entorno	23
2.5.6	Gestión de comunicaciones y operaciones	23
2.5.7	Control de accesos.....	23
2.5.8	Desarrollo y mantenimiento de sistemas	23
2.5.9	Gestión de incidentes	24
2.5.10	Gestión de continuidad del negocio.....	24
2.5.11	Conformidad con la legislación	24
2.6	Esquema de la ISO 27001.....	25

2.6.1	Política de seguridad	25
2.6.2	Aspectos organizativos para la seguridad	25
2.6.3	Clasificación y control de activos	27
2.6.4	Seguridad ligada al personal	28
2.6.5	Seguridad física y del entorno	30
2.6.6	Gestión de comunicaciones y operaciones	32
2.6.7	Control de accesos.....	36
2.6.8	Desarrollo y mantenimiento de sistemas	41
2.6.9	Gestión de continuidad del negocio	45
2.6.10	Conformidad con la legislación	47
3	OSSTMM	49
3.1	Introducción	49
3.2	Mapa de seguridad.....	49
3.3	Metodología	50
3.4	Sección A – Seguridad de la información	50
3.4.1	Revisión de la Inteligencia Competitiva	51
3.4.2	Revisión de provacidad.....	51
3.4.3	Recolección de documentos.....	52
3.5	Sección B – Seguridad de los Procesos	52
3.5.1	Testeo de Solicitud	52
3.5.2	Testeo de Sugerencia Dirigida	53
3.5.3	Testeo de las Personas Confiables	53
3.6	Sección C – Seguridad en las Tecnologías de Internet	54
3.6.1	Logística y Controles	54
3.6.2	Sondeo de Red.....	55
3.6.3	Identificación de los Servicios de Sistema.....	55
3.6.4	Búsqueda de Información Competitiva.....	56
3.6.5	Revisión de Privacidad.....	56
3.6.6	Obtención de Documentos	57
3.6.7	Búsqueda y Verificación de Vulnerabilidades	57
3.6.8	Testeo de Aplicaciones en Internet	58
3.6.9	Enrutamiento	58
3.6.10	Testeo de Sistemas Confiados.....	59
3.6.11	Testeo de Control de Acceso	59
3.6.12	Testeo de Sistema de Detección de Intrusos	59
3.6.13	Testeo de Medidas de Contingencia	60
3.6.14	Desifrado de Contraseñas	60
3.6.15	Testeo de Denegación de Servicios	61
3.6.16	Evaluación de Políticas de Seguridad.....	62
3.7	Sección D – Seguridad en las Comunicaciones.....	62
3.7.1	Testeo de PBX.....	63
3.7.2	Testeo del Correo de Voz	63
3.7.3	Revisión del Fax	63



3.7.4 Testeo del Modem	64
3.8 Sección E – Seguridad Inalámbrica.....	64
3.8.1 Verificación de Radiación Electromagnética (EMR)	65
3.8.2 Verificación de Redes Inalámbricas [802.11]	65
3.8.3 Verificación de Redes Bluetooth	66
3.8.4 Verificación de Dispositivos de Entrada Inalámbricos.....	67
3.8.5 Verificación de Dispositivos de Mano Inalámbricos	67
3.8.6 Verificación de Comunicaciones sin Cable	68
3.8.7 Verificación de Dispositivos de Vigilancia Inalámbricos	68
3.8.8 Verificación de Dispositivos de Transacción Inalámbricos	69
3.8.9 Verificación de RFID.....	69
3.8.10 Verificación de Sistemas Infrarrojos.....	70
3.8.11 Revisión de Privacidad	71
3.9 Sección F – Seguridad Física.....	71
3.9.1 Revisión de Perímetro	72
3.9.2 Revisión de Monitoreo	72
3.9.3 Evaluación de Controles de Acceso	72
3.9.4 Revisión de Respuesta de Alarmas	73
3.9.5 Revisión de Ubicación.....	73
3.9.6 Revisión de Entorno	74