ANEXO III

I. IDENTIFICACIÓN DEL CERTIFICADO DE PROFESIONALIDAD

Denominación: Seguridad informática

Código: IFCT0109

Familia Profesional: Informática y Comunicaciones

Área profesional: Sistemas y telemática

Nivel de cualificación profesional: 3

Cualificación profesional de referencia:

IFC153_3 Seguridad informática (RD 1087/05 de 16 de septiembre)

Relación de unidades de competencia que configuran el certificado de profesionalidad:

UC0486_3: Asegurar equipos informáticos.
UC0487_3: Auditar redes de comunicación y sistemas informáticos.
UC0488_3: Detectar y responder ante incidentes de seguridad.
UC0489_3: Diseñar e implementar sistemas seguros de acceso y transmisión de datos.
UC0490_3: Gestionar servicios en el sistema informático.

Competencia general:

Garantizar la seguridad de los accesos y usos de la información registrada en equipos informáticos, así como del propio sistema, protegiéndose de los posibles ataques, identificando vulnerabilidades y aplicando sistemas de cifrado a las comunicaciones que se realicen hacia el exterior y en el interior de la organización.

Entorno Profesional:

Ámbito Profesional:

Desarrolla su actividad profesional en el área de sistemas del departamento de informática de empresas públicas o privadas que utilizan equipamiento informático, desempeñando tareas de auditoría, configuración y temas relacionados con la seguridad informática, tanto por cuenta ajena como por cuenta propia.

Sectores Productivos:

Está presente en múltiples sectores productivos, sobre todo en el sector servicios, aunque se percibe una marcada característica de transectorialidad. También está presente en los siguientes tipos de empresas:

- Empresas de cualquier sector y tamaño que utilizan equipamiento informático en sus procesos de gestión.
- Empresas que prestan servicios de asistencia técnica informática.
- Empresas de externalización (outsourcing) de servicios.

cve: BOE-A-2011-10055

Ocupaciones o puestos de trabajo relacionados:

3820.1017 Programador de Aplicaciones Informáticas
3812.1014 Técnico en Informática de Gestión
Técnico en seguridad informática.
Técnico en auditoría informática.

Duración de la formación asociada: 500 horas

Relación de módulos formativos y de unidades formativas:

MF0486_3: Seguridad en equipos informáticos. (90 horas)
MF0487_3: Auditoría de seguridad informática. (90 horas)
MF0488_3: Gestión de incidentes de seguridad informática. (90 horas)
MF0489_3: Sistemas seguros de acceso y transmisión de datos. (60 horas)
MF0490_3: (Transversal) Gestión de servicios en el sistema informático. (90 horas)
MP0175: Modulo de prácticas profesionales no laborales de Seguridad informática. (80 horas)

II. PERFIL PROFESIONAL DEL CERTIFICADO DE PROFESIONALIDAD

Unidad de competencia 1

Denominación: ASEGURAR EQUIPOS INFORMÁTICOS

Nivel: 3

Código: UC0486_3

Realizaciones profesionales y criterios de realización

RP1: Aplicar políticas de seguridad para la mejora de la protección de servidores y equipos de usuario final según las necesidades de uso y condiciones de seguridad.

CR1.1 El plan de implantación del sistema informático de la organización se analiza comprobando que incorpora la información necesaria referida a procedimientos de instalación y actualización de equipos, copias de respaldo y detección de intrusiones entre otros, así como referencias de posibilidades de utilización de los equipos y restricciones de los mismos y protecciones contra agresiones de virus y otros elementos no deseados.

CR1.2 Los permisos de acceso, por parte de los usuarios, a los distintos recursos del sistema son determinados por medio de las herramientas correspondientes según el Plan de Implantación y el de seguridad del sistema informático.

CR1.3 EL acceso a los servidores se realiza garantizando la confidencialidad e integridad de la conexión según las normas de seguridad de la organización.

CR1.4 Las políticas de usuario se analizan verificando que quedan reflejadas circunstancias tales como usos y restricciones asignadas a equipos y usuarios, servicios de red permitidos y restringidos y ámbitos de responsabilidades debidas a la utilización de los equipos informáticos.

CR1.5 La política de seguridad es transmitida a los usuarios, asegurándose de su correcta y completa comprensión.

CR1.6 Las tareas realizadas se documentan convenientemente según los procedimientos de la organización.

CR1.7 Las informaciones afectadas por la legislación de protección de datos se tratan verificando que los usuarios autorizados cumplan los requisitos indicados por la normativa y los cauces de distribución de dicha información están documentados y autorizados según el plan de seguridad.

cve: BOE-A-2011-10055

MÓDULO DE PRÁCTICAS PROFESIONALES NO LABORALES DE SEGURIDAD INFORMÁTICA

Código: MP0175

Duración: 80 horas

Capacidades y criterios de evaluación

C1: Proporcionar soporte técnico en materia de seguridad.

CE1.1. Proporcionar asistencia técnica en el diseño y configuración de soluciones de seguridad.

CE1.2. Dar soporte a otras áreas en las tareas de diseño y reingeniería de procesos para aportar la visión de seguridad.

CE1.3. Actuar como enlace entre las distintas áreas de la compañía para coordinar medidas de seguridad multidepartamentales.

CE1.4. Analizar las reglas específicas desarrolladas por las áreas técnicas específicas para las herramientas de seguridad corporativas.

CE1.5. Coordinar el uso de las herramientas de cifrado y la gestión de las claves

CE1.6. Dar soporte técnico a los comités de dirección que proceda.

CE1.7. Evaluar y mantenerse permanentemente informado de los errores, informes, noticias, boletines, etc. de seguridad recibidos y dar el primer nivel de soporte y distribución.

CE1.8. Desarrollar las políticas y procedimientos operativos en materia de seguridad de la información y dar soporte a las distintas áreas de la organización para su puesta en producción.

C2: Verificar la correcta aplicación de las medidas de seguridad.

CE2.1. Realizar las verificaciones necesarias para determinar el grado de vulnerabilidad de las distintas plataformas tecnológicas, así como el resto de revisiones periódicas de seguridad de los sistemas de información.

CE2.2. Mantener actualizado el análisis de riesgos de la organización

CE2.3. Coordinar las auditorías técnicas de seguridad.

C3: Participar en los procesos de trabajo de la empresa, siguiendo las normas e instrucciones establecidas en el centro de trabajo.

CE3.1 Comportarse responsablemente tanto en las relaciones humanas como en los trabajos a realizar.

CE3.2 Respetar los procedimientos y normas del centro de trabajo.

CE3.3 Emprender con diligencia las tareas según las instrucciones recibidas, tratando de que se adecuen al ritmo de trabajo de la empresa.

CE3.4 Integrarse en los procesos de producción del centro de trabajo.

CE3.5 Utilizar los canales de comunicación establecidos.

CE3.6 Respetar en todo momento las medidas de prevención de riesgos, salud laboral y protección del medio ambiente.

Contenidos

1. Revisión de la situación de la seguridad de la información

- Revisión de las normas internas de seguridad
- Revisión de la gestión de usuarios, privilegios y política de contraseñas
- Revisión de las copias de seguridad
- Revisión de las incidencias que se han producido

cve: BOE-A-2011-10055

- Revisión de la situación con respecto a la protección frente a código malicioso
- Revisión de la seguridad de las redes de datos
- Revisión de la seguridad de servidores y puestos de trabajo
- Revisión de la seguridad física, suministro eléctrico, climatización y protección de incendios según proceda

2. Configuración de reglas de relacionadas con la seguridad
- Configuración de la seguridad de el/los router
- Configuración de la seguridad de el/los switch
- Configuración de la seguridad de el/los cortafuegos
- Configuración de la seguridad de el/los sistema de detección de intrusos
- Configuración de la seguridad de el/los antivirus

3. Comunicación de los aspectos relacionados con la seguridad
- Establecimiento de canales para mantener a la organización actualizada en materia de seguridad
- Establecimiento de los canales internos para coordinar la seguridad entre los departamentos de la organización

4. Monitorización de la seguridad
- Monitorización de las comunicaciones
- Monitorización del rendimiento de sistemas

5. Aplicación de la normativa y metodología de seguridad
- Aplicación de códigos de buenas practicas de seguridad a la gestión diaria de los sistemas de información
- Integración de los requerimientos de seguridad en los procesos de negocio de la organización

6. Integración y comunicación en el centro de trabajo
- Comportamiento responsable en el centro de trabajo.
- Respeto a los procedimientos y normas del centro de trabajo.
- Interpretación y ejecución con diligencia las instrucciones recibidas.
- Reconocimiento del proceso productivo de la organización.
- Utilización de los canales de comunicación establecidos en el centro de trabajo.
- Adecuación al ritmo de trabajo de la empresa.
- Seguimiento de las normativas de prevención de riesgos, salud laboral y protección del medio ambiente.

IV. PRESCRIPCIONES DE LOS FORMADORES

Módulos Formativos	Acreditación requerida	*Experiencia profesional en el ámbito de la unidad de competencia	
		Si se cuenta con acreditación	Si no se cuenta con acreditación
MF0486_3: Asegurar equipos informáticos	• Licenciado, Ingeniero, Arquitecto o el título de grado correspondiente u otros títulos equivalentes. • Diplomado, Ingeniero Técnico, Arquitecto Técnico o el título de grado correspondiente u otros títulos equivalentes.	1 año	3 años

cve: BOE-A-2011-10055