

Curso totalmente gratuito conducente a la obtención de un Certificado de Profesionalidad dirigido prioritariamente a trabajadores/as ocupados/as

MF0959_2 MANTENIMIENTO DE LA SEGURIDAD EN SISTEMAS INFORMATICOS



Gestión de la seguridad informática



Monitorización de accesos



Copias de seguridad y su restauración



985 26 91 29
622 20 60 95



acalug@academialugones.com

1.	COMPETENCIA GENERAL.....	3
2.	REALIZACIONES PROFESIONALES Y CRITERIOS DE REALIZACIÓN.....	3
3.	UNIDAD FORMATIVA: MONITORIZACIÓN DE LOS ACCESOS AL SISTEMA INFORMÁTICO.....	5
	3.1 UNIDAD FORMATIVA: MONITORIZACIÓN DE LOS ACCESOS AL SISTEMA INFORMÁTICO	5
4.	CONTENDOS.....	¡Error! Marcador no definido.

1. COMPETENCIA GENERAL

Mantener la seguridad de los subsistemas físicos y lógicos en sistemas informáticos.

2. REALIZACIONES PROFESIONALES Y CRITERIOS DE REALIZACIÓN

RP1: Revisar los accesos al sistema informático, para asegurar la aplicación de los procedimientos establecidos y el plan de seguridad, informando de las anomalías detectadas.

CR1.1 Las herramientas de monitorización, para trazar los accesos y la actividad del sistema se comprueban para asegurar su funcionamiento, según el plan de seguridad del sistema.

CR1.2 Los ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema se recopilan para localizar la existencia de accesos o actividades no deseados.

CR1.3 Las incidencias detectadas en el acceso al sistema son comprobadas para establecer si están registradas, en otro caso se documentan y se registran para su uso posterior según procedimientos establecidos.

CR1.4 Los cambios detectados en la configuración de control de acceso de usuarios al sistema se documentan, para mantener el inventario actualizado, según procedimientos establecidos.

RP2: Comprobar el funcionamiento de los mecanismos de seguridad establecidos informando de las anomalías detectadas a personas de responsabilidad superior.

CR2.1 Los permisos de acceso de los usuarios al sistema se comprueban, para asegurar su validez, según el plan de seguridad del sistema.

CR2.2 Las políticas de seguridad de usuario se comprueban, para cerciorar su validez, según el plan de seguridad del sistema.

CR2.3 Los sistemas de protección antivirus y de programas maliciosos se revisan, en lo que respecta a su actualización y configuración funcional, para garantizar la seguridad del equipo, según los procedimientos establecidos por la organización.

CR2.4 Las incidencias detectadas son comprobadas para establecer si están registradas, en otro caso se documentan y se registran para su uso posterior, siguiendo procedimientos establecidos e informando al inmediato superior.

CR2.5 Los procesos de diagnóstico se realizan en los equipos en los que se han detectado incidencias utilizando herramientas específicas y de gestión remota con el fin de solucionarlas o escalarlas siguiendo los procedimientos establecidos.

RP3: Realizar la copia de seguridad, para garantizar la integridad de los datos, según los procedimientos establecidos y el plan de seguridad.

CR3.1 Las copias de seguridad se realizan, para proteger los datos del sistema, según la periodicidad, soporte y procedimiento establecidos en el plan de seguridad del sistema.

CR3.2 Las copias de seguridad se verifican, para asegurar la utilización de las mismas, según los procedimientos establecidos en el plan de seguridad del sistema.

CR3.3 El almacenaje de las copias de seguridad, para evitar pérdidas de la información, se realiza en las condiciones y según el procedimiento indicado en el plan de seguridad del sistema y las recomendaciones del fabricante del soporte.

CR3.4 Las incidencias detectadas son comprobadas, para establecer si están registradas, de otro modo se documentan y registran para su uso posterior, según procedimientos establecidos.

RP4: Verificar que las condiciones ambientales y de seguridad se mantienen según los planes establecidos, informando de posibles anomalías.

CR4.1 Las especificaciones técnicas de los dispositivos se comprueban para asegurar que se cumplen las recomendaciones de los fabricantes en cuanto a condiciones ambientales y de seguridad.

CR4.2 La ubicación de los equipos y dispositivos físicos se revisa para asegurar que se cumplen los requisitos en cuanto a seguridad, espacio y ergonomía establecidos por la organización.

CR4.3 Las incidencias detectadas son comprobadas para establecer si están registradas, en otro caso se documentan y se registran para su uso posterior siguiendo procedimientos establecidos e informando al inmediato superior.

CR4.4 Las acciones correctivas establecidas para solucionar determinadas incidencias detectadas se realizan según procedimientos establecidos.

3. UNIDAD FORMATIVA: MONITORIZACIÓN DE LOS ACCESOS AL SISTEMA INFORMÁTICO

3.1 CAPACIDADES Y CRITERIOS DE EVALUACIÓN

C1: Identificar los tipos de acceso al sistema informático así como los mecanismos de seguridad del mismo describiendo sus características principales y herramientas asociadas más comunes para garantizar el uso de los recursos del sistema.

CEI.1 Describir los mecanismos del sistema de control de acceso detallando la organización de usuarios y grupos para garantizar la seguridad de la información y funcionalidades soportadas por el equipo informático, según las especificaciones técnicas.

CEI.2 Explicar los procedimientos de los sistemas para establecer permisos y derechos de usuarios, detallando su organización y herramientas administrativas asociadas para organizar políticas de seguridad, según los procedimientos establecidos en el software base.

CEI.3 Clasificar los mecanismos de seguridad comunes en sistemas detallando sus objetivos, características y herramientas asociadas para garantizar la seguridad de la información y funcionalidades soportadas por el equipo informático.

CEI.4 Identificar los mecanismos de protección del sistema contra virus y programas maliciosos para asegurar su actualización.

CEI.5 Identificar los mecanismos de seguridad del sistema para mantener la protección del mismo, según unos procedimientos de operación especificados:

- Identificar los usuarios y grupos definidos en el sistema operando con las herramientas administrativas indicadas en los procedimientos dados.
- Localizar, para cada usuario, los permisos de acceso y las políticas de seguridad asociadas, operando con las herramientas administrativas indicadas en los procedimientos dados.
- Verificar que las aplicaciones antivirus y de protección contra programas maliciosos están actualizadas.
- Comprobar el registro de los usuarios y grupos en el inventario, registrando los cambios detectados.

C2: Interpretar las trazas de monitorización de los accesos y actividad del sistema identificando situaciones anómalas, siguiendo unas especificaciones dadas.

CE2.1 Enumerar los mecanismos del sistema de trazas de acceso y de actividad para su monitorización detallando su ámbito de acción, características principales y herramientas asociadas.

CE2.2 Describir las incidencias producidas en el acceso de usuarios y de actividad del sistema clasificándolas por niveles de seguridad para detectar situaciones anómalas en dichos procesos.

CE2.3 Identificar las herramientas para extraer los ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema para facilitar su consulta y manipulación, de acuerdo a sus especificaciones técnicas.

CE2.4 Interpretar el contenido de ficheros de traza de conexión de usuarios y los ficheros de actividad del sistema para localizar accesos y actividades no deseadas siguiendo el procedimiento indicado por el administrador.

CE2.5 En supuestos prácticos, donde se cuenta con ficheros de traza de conexión de usuarios y ficheros de actividad del sistema, realizar el análisis y la evaluación de los mismos para detectar posibles accesos y actividades no deseadas, según unas especificaciones dadas:

- Identificar las características de un conjunto de registros de usuarios siguiendo las indicaciones del administrador.
- Localizar un registro de un usuario dado y explicar sus características.
- Extraer y registrar las situaciones anómalas relativas a un usuario siguiendo las indicaciones del administrador.
- Documentar las acciones realizadas.

CE2.6 Distinguir las herramientas utilizadas para el diagnóstico y detección de incidencias tanto en aplicación local como remota, para su gestión, solución o escalado de las mismas, según unas especificaciones dadas.

3.2 CONTENIDOS

1. Gestión de la seguridad informática

- ✓ Objetivo de la seguridad.
- ✓ Términos relacionados con la seguridad informática.
- ✓ Procesos de gestión de la seguridad.

- Objetivos de la gestión de la seguridad.
- Beneficios y dificultades.
- Política de seguridad. La Ley Orgánica de Protección de Datos de carácter personal.
- Análisis del riesgo.
 - Identificación de recursos.
 - Identificación de vulnerabilidades y amenazas: atacante externo e interno.
 - Medidas de protección.
- Plan de seguridad.
- ✓ Interrelación con otros procesos de las tecnologías de la información.
- ✓ Seguridad física y seguridad lógica.

2. Seguridad lógica del sistema

- ✓ Acceso al sistema y al software de aplicación.
 - Concepto de usuario, cuenta, grupo de usuario, permisos, lista de control de accesos (ACL).
 - Políticas de seguridad respecto de los usuarios.
- ✓ Autenticación de usuarios:
 - Definición y conceptos básicos.
 - Sistemas de autenticación débiles y fuertes.
 - Sistemas de autenticación biométricos y otros sistemas.
 - Acceso local, remote y Single Sing-On.
- ✓ Herramientas para la gestión de usuarios.
 - El servicio de directorio: conceptos básicos, protocolos e implementaciones.
 - Directorios: LDAP, X500, Active Directory.
 - Herramientas de administración de usuarios y equipos.
 - Administración básica del servicio de directorio.
- ✓ Confidencialidad y Disponibilidad de la información en el puesto de usuario final.
 - Sistemas de ficheros y control de acceso a los mismos.
 - Permisos y derechos sobre los ficheros.
- ✓ Seguridad en el puesto de usuario.
 - Tipología de software malicioso.
 - Software de detección de virus y programas maliciosos.
 - Antivirus, antispymware, firewall, filtros antispam, etc.
 - Técnicas de recuperación y desinfección de datos afectados.

- ✓ Herramientas de gestión remota de incidencias.

3. Procedimientos de monitorización de los accesos y la actividad del sistema

- ✓ Objetivos de la monitorización y de la gestión de incidentes de seguridad.
- ✓ Procedimientos de monitorización de trazas.
 - Identificación y caracterización de aspectos monitorizables o auditables.
 - Clasificación de eventos e incidencias: de sistema, de aplicación, de seguridad.
 - Mecanismos de monitorización de trazas: logs del sistema, consolas de monitorización de usuarios.
 - Información de los registros de trazas.
- ✓ Técnicas y herramientas de monitorización.
 - Técnicas: correlación de logs, de eventos.
 - Herramientas de monitorización.
 - Herramientas propias de sistema operativo.
 - Sistemas basados en equipos (HIDS).
 - Sistemas basados en red (NDIS).
 - Sistemas de prevención de intrusiones (IPS).
 - Informes de monitorización.
 - Recolección de información.
 - Análisis y correlación de eventos.
 - Verificación de la intrusión.
 - Alarmas y acciones correctivas.
 - Organismos de gestión de incidentes:
 - Nacionales. IRIS-CERT, esCERT.
 - Internacionales. CERT, FIRST.

4. UNIDAD FORMATIVA: COPIA DE SEGURIDAD Y RESTAURACIÓN DE LA INFORMACIÓN

4.1 CAPACIDADES Y CRITERIOS DE EVALUACIÓN

CI: Aplicar procedimientos de copia de seguridad y restauración, verificar su realización y manipular los medios de almacenamiento para garantizar la integridad de la información del sistema informático, siguiendo unas especificaciones dadas.

CEI.1 Clasificar los distintos medios de almacenamiento y seguridad de datos del sistema informático para utilizarlos en los procesos de copia en función de especificaciones técnicas establecidas.

CEI.2 Explicar los procedimientos y herramientas para la realización de copias de seguridad y almacenamiento de datos del sistema informático para garantizar la integridad de la información del sistema.

CEI.3 Explicar los procedimientos y herramientas para la restauración de datos de un sistema informático para la recuperación de la información del sistema, según las especificaciones dadas.

CEI.4 Explicar los procedimientos y herramientas para la verificación de la copia de seguridad y de la restauración de datos para asegurar la fiabilidad del proceso según las especificaciones dadas.

CEI.5 En un sistema de almacenamiento de datos con varios dispositivos, realizar copias de seguridad para garantizar la integridad de datos, dados unos procedimientos a seguir:

- Seleccionar el dispositivo de almacenamiento y herramienta para realizar la copia.
- Realizar la copia de seguridad según la periodicidad y el procedimiento especificado, o bien a indicación del administrador.
- Verificar la realización de la copia.
- Etiquetar la copia realizada y proceder a su almacenaje según las condiciones ambientales, de ubicación y de seguridad especificadas.
- Comprobar y registrar las incidencias detectadas.
- Documentar los procesos realizados.

CEI.6 Realizar la restauración de copias de seguridad para recuperar la información almacenada, dados unos procedimientos a seguir:

- Seleccionar la herramienta para realizar la restauración de acuerdo al tipo y soporte de copia de seguridad realizada.

- Realizar el proceso de restauración según las indicaciones recibidas.
- Verificar el proceso de restauración comprobando el destino de la misma.
- Comprobar y registrar las incidencias detectadas.
- Documentar los procesos realizados.

C2: Describir las condiciones ambientales y de seguridad para el funcionamiento de los equipos y dispositivos físicos que garanticen los parámetros de explotación dados.

CE2.1 Describir los factores ambientales que influyen en la ubicación y acondicionamiento de espacios de dispositivos físicos, material fungible y soportes de información para cumplimentar los requisitos de instalación de dispositivos, según las especificaciones técnicas de los mismos.

CE2.2 Identificar los factores de seguridad y ergonomía a tener en cuenta en la ubicación de equipos y dispositivos físicos para garantizar los condicionantes de implantación de los dispositivos, según las especificaciones técnicas de los mismos.

CE2.3 Comprobar las condiciones ambientales para asegurar la situación de equipos y dispositivos físicos, de acuerdo a las normas especificadas:

- Comprobar que la ubicación de los dispositivos físicos, material fungible y soportes de información cumplen las normas establecidas y las especificaciones técnicas.
- Comprobar el registro de ubicación de dispositivos físicos y material fungible en el inventario, registrando los cambios detectados.
- Identificar las condiciones de seguridad y ambientales adecuadas y no adecuadas.
- Proponer acciones correctivas para asegurar los requisitos de seguridad y de condiciones ambientales.

4.2 CONTENIDOS

1. Copias de seguridad

- ✓ Tipos de copias de seguridad (total, incremental, diferencial).
- ✓ Arquitectura de servicios de copias de respaldo.

- ✓ Medios de almacenamiento para copias de seguridad.
- ✓ Herramientas para la realización de copias de seguridad.
 - Funciones básicas.
 - Configuración de opciones de restauración y copias de seguridad.
 - Realización de copias de seguridad.
 - Restauración de copias y verificación de la integridad de la información.
- ✓ Realización de copias de seguridad y restauración en sistemas remotos.

2. Entorno físico de un sistema informático

- ✓ Los equipos y el entorno: adecuación del espacio físico.
 - Ubicación y acondicionamiento de espacios de dispositivos físicos.
 - Factores ambientales.
 - Factores de seguridad y ergonomía.
 - Ubicación y acondicionamiento de material fungible y soportes de información.
- ✓ Agentes externos y su influencia en el sistema.
- ✓ Efectos negativos sobre el sistema.
- ✓ Creación del entorno adecuado.
 - Condiciones ambientales: humedad, temperatura.
 - Factores industriales: polvo, humo, interferencias, ruidos y vibraciones.
 - Factores humanos: funcionalidad, ergonomía y calidad de la instalación.
 - Otros factores.
- ✓ Factores de riesgo.
 - Conceptos de seguridad eléctrica.
 - Requisitos eléctricos de la instalación.
 - Perturbaciones eléctricas y electromagnéticas.
 - Electricidad estática.
 - Otros factores de riesgo.
- ✓ Los aparatos de medición.
- ✓ Acciones correctivas para asegurar requisitos de seguridad y ambientales.
- ✓ El Centro del Proceso de datos (CPD).
 - Requisitos y ubicación de un CPD.
 - Condiciones del medio ambiente externo.
 - Factores que afectan a la seguridad física de un CPD.

- Acondicionamiento.
- Sistemas de seguridad física.
- ✓ Plan de Emergencia y Evacuación.

3. Reglamentos y normativas

- ✓ El estándar ANSI/TIA-942-2005.
- ✓ Medidas de seguridad en el tratamiento de datos de carácter personal (RD 1720/2007).
- ✓ La guía de seguridad.