- 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, antispyware, 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 del sistema operativo.
    - Sistemas basados en equipo (HIDS).
    - Sistemas basados en red (NIDS).
    - 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.

UNIDAD FORMATIVA 2

Denominación: COPIA DE SEGURIDAD Y RESTAURACIÓN DE LA INFORMACIÓN.

Código: UF1354

Duración: 30 horas

Referente de competencia: Esta unidad formativa se corresponde con la RP3 y RP4.

cve: BOE-A-2011-19503

Capacidades y criterios de evaluación

C1: 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.

CE1.1 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.

CE1.2 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.

CE1.3 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.

CE1.4 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.

CE1.5 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.

CE1.6 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.

cve: BOE-A-2011-19503

- Identificar las condiciones de seguridad y ambientales adecuadas y no adecuadas.
- Proponer acciones correctivas para asegurar los requisitos de seguridad y de condiciones ambientales.

Contenidos

1. **Copias de seguridad**
   - Tipos de copias de seguridad (total, incremental, diferencial).
   - Arquitectura del servicio 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 de 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.

cve: BOE-A-2011-19503