

Máster en Protección de Información y Comunicaciones



ÍNDICE

1 | Somos Educa
Business School

2 | Rankings

3 | Alianzas y
acreditaciones

4 | By EDUCA
EDTECH
Group

5 | Metodología
LXP

6 | Razones por las
que elegir Educa
Business School

7 | Programa
Formativo

8 | Temario

9 | Contacto

SOMOS EDUCA BUSINESS SCHOOL

EDUCA Business School es una institución de formación online especializada en negocios. Como miembro de la Comisión Internacional de Educación a Distancia y con el prestigioso Certificado de Calidad AENOR (normativa ISO 9001) nuestra institución se distingue por su compromiso con la excelencia educativa.

Nuestra **oferta formativa**, además de **satisfacer las demandas del mercado laboral** actual, puede bonificarse como formación continua para el personal trabajador, así como ser homologados en Oposiciones dentro de la Administración Pública. Las titulaciones de EDUCA Business School se pueden certificar con la Apostilla de La Haya dotándolos de validez internacional en más de 160 países.

Más de

18

años de
experiencia

Más de

300k

estudiantes
formados

Hasta un

98%

tasa
empleabilidad

Hasta un

100%

de financiación

Hasta un

50%

de los estudiantes
repite

Hasta un

25%

de estudiantes
internacionales

RANKINGS DE EDUCA BUSINESS SCHOOL

Educa Business School se engloba en el conjunto de EDUCA EDTECH Group, que ha sido reconocido por su trabajo en el campo de la formación online.

Todas las entidades bajo el sello EDUCA EDTECH comparten la misión de democratizar el acceso a la educación y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación. Gracias a ello ha conseguido el reconocimiento de diferentes rankings a nivel nacional e internacional.



ALIANZAS Y ACREDITACIONES



FONDO
SOCIAL
EUROPEO



BY EDUCA EDTECH

Educa Business School es una marca avalada por **EDUCA EDTECH Group**, que está compuesto por un conjunto de experimentadas y reconocidas instituciones educativas de formación online. Todas las entidades que lo forman comparten la misión de democratizar el acceso a la educación y apuestan por la transferencia de conocimiento, por el desarrollo tecnológico y por la investigación.



ONLINE EDUCATION



METODOLOGÍA LXP

La metodología **EDUCA LXP** permite una experiencia mejorada de aprendizaje integrando la AI en los procesos de e-learning, a través de modelos predictivos altamente personalizados, derivados del estudio de necesidades detectadas en la interacción del alumnado con sus entornos virtuales.

EDUCA LXP es fruto de la **Transferencia de Resultados de Investigación** de varios proyectos multidisciplinares de I+D+i, con participación de distintas Universidades Internacionales que apuestan por la transferencia de conocimientos, desarrollo tecnológico e investigación.



1. Flexibilidad

Aprendizaje 100% online y flexible, que permite al alumnado estudiar donde, cuando y como quiera.



2. Accesibilidad

Cercanía y comprensión. Democratizando el acceso a la educación trabajando para que todas las personas tengan la oportunidad de seguir formándose.



3. Personalización

Itinerarios formativos individualizados y adaptados a las necesidades de cada estudiante.



4. Acompañamiento / Seguimiento docente

Orientación académica por parte de un equipo docente especialista en su área de conocimiento, que aboga por la calidad educativa adaptando los procesos a las necesidades del mercado laboral.



5. Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.



6. Excelencia educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo, garantizando el desarrollo profesional.

RAZONES POR LAS QUE ELEGIR EDUCA BUSINESS SCHOOL

1. FORMACIÓN ONLINE ESPECIALIZADA

Nuestros alumnos acceden a un modelo pedagógico innovador **de más de 20 años de experiencia educativa con Calidad Europea.**



2. METODOLOGÍA DE EDUCACIÓN FLEXIBLE

Con nuestra metodología estudiarán **100% online** y nuestros alumnos/as tendrán acceso los 365 días del año a la plataforma educativa.



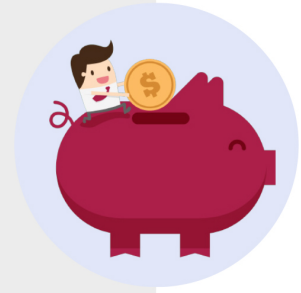
3. CAMPUS VIRTUAL DE ÚLTIMA TECNOLOGÍA



Contamos con una **plataforma avanzada** con material adaptado a la realidad empresarial, que fomenta la participación, interacción y comunicación con alumnos de distintos países.

4. DOCENTES DE PRIMER NIVEL

Nuestros docentes están acreditados y formados en **Universidades de alto prestigio en Europa**, todos en activo y con una amplia experiencia profesional.



5. TUTORÍA PERMANENTE



Contamos con un **Centro de Atención al Estudiante CAE**, que brinda atención personalizada y acompañamiento durante todo el proceso formativo.

6. DOBLE MATRICULACIÓN

Algunas de nuestras acciones formativas cuentan con la llamada **Doble matriculación**, que te permite obtener dos formaciones, ya sean de masters o curso, al precio de una.



Máster en Protección de Información y Comunicaciones



**MODALIDAD
ONLINE**



**ACOMPañAMIENTO
PERSONALIZADO**

Titulación

Titulación de Máster en Protección de Información y Comunicaciones con 1500 horas expedida por EDUCA BUSINESS SCHOOL como Escuela de Negocios Acreditada para la Impartición de Formación Superior de Postgrado, con Validez Profesional a Nivel Internacional





EDUCA BUSINESS SCHOOL
como centro acreditado para la impartición de acciones formativas
expide el presente título propio

NOMBRE DEL ALUMNO/A
con número de documento XXXXXXXX ha superado los estudios correspondientes de

Nombre del curso
con una duración de XXX horas, perteneciente al Plan de Formación de Educa Business School.
Y para que surta los efectos pertinentes queda registrado con número de expediente XXXX/XXXX-XXXX-XXXXXX.
Con una calificación XXXXXXXXXXXXXXXX.
Y para que conste expido la presente titulación en Granada, a (día) de (mes) del (año).

Firma del Alumno/a
NOMBRE ALUMNO/A

La Dirección Académica
NOMBRE DE AREA MANAGER





Con Examen Convulsivo, Categoría Especial del Consejo Examinador y Solicitud de la UNED03 (Item: Pruebas de 0000)

Descripción

En un mundo donde la información es el recurso más valioso, protegerla se ha convertido en una necesidad esencial. El Máster en Protección de Información y Comunicaciones te ofrece una formación integral y actualizada en un sector en auge y con alta demanda laboral. Aprenderás desde la implementación de sistemas de seguridad basados en la norma ISO/IEC 27002 hasta la gestión de

ciberataques y auditorías informáticas. El programa se centra en desarrollar habilidades críticas para administrar incidentes de seguridad, optimizar el rendimiento de sistemas y establecer políticas robustas de protección de datos. Además, adquirirás conocimientos en criptografía y seguridad en redes de datos, preparándote para enfrentar los desafíos actuales y futuros del entorno digital. Este máster online te brinda la flexibilidad de estudiar a tu ritmo, combinando teoría y práctica para convertirte en un experto en seguridad de la información y comunicaciones.

Objetivos

'- Describir la seguridad de la información y su impacto en las organizaciones actuales. - Aplicar la norma ISO/IEC 27002 para implantar sistemas de seguridad efectivos. - Gestionar políticas de seguridad y manejo de activos en entornos corporativos. - Controlar el acceso a sistemas de información mediante estrategias avanzadas. - Administrar incidentes y asegurar la continuidad del negocio con eficacia. - Implantar sistemas de detección y prevención de intrusiones en redes. - Realizar análisis forense informático para identificar y mitigar amenazas.

Para qué te prepara

El Máster en Protección de Información y Comunicaciones está diseñado para profesionales y graduados del sector tecnológico que busquen profundizar en la seguridad de la información. Aborda temas avanzados como la gestión de políticas de seguridad, auditoría informática, prevención de ciberataques y criptografía, ideal para quienes deseen actualizar o ampliar sus competencias en un entorno digital seguro.

A quién va dirigido

Este máster te capacita para diseñar, implementar y gestionar sistemas de seguridad en la información y comunicaciones, aplicando normativas como ISO/IEC 27001 y 27002. Aprenderás a proteger datos y gestionar riesgos, asegurar la continuidad del negocio y responder eficazmente a incidentes de seguridad. Además, desarrollarás habilidades para realizar auditorías, implementar IDS/IPS y aplicar criptografía, lo que te permitirá garantizar la integridad y confidencialidad de la información en cualquier organización.

Salidas laborales

'- Consultor en ciberseguridad - Auditor de seguridad informática - Especialista en protección de datos - Responsable de políticas de seguridad - Analista de riesgos informáticos - Gestor de incidentes de seguridad - Administrador de sistemas de seguridad - Experto en criptografía y PKI - Coordinador de

respuesta ante ciberataques - Asesor en cumplimiento normativo de seguridad informática

TEMARIO

MÓDULO 1. INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. DESCRIPCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. La sociedad de la información
2. ¿Qué se entiende por seguridad de la información?
3. ¿Por qué tener en cuenta la seguridad de la información?
4. Fundamentos de la seguridad de la información: confidencialidad, integridad y disponibilidad
5. Fuentes de los riesgos de la seguridad
6. Controles para garantizar la seguridad de la información
7. Cómo conseguir la seguridad de la información

UNIDAD DIDÁCTICA 2. NORMATIVA BÁSICA SOBRE SEGURIDAD DE LA INFORMACIÓN

1. Marco legal y jurídico de la seguridad de la información
2. Normativa comunitaria sobre seguridad de la información
3. Normativa de calidad sobre la gestión de la seguridad de la información: Norma ISO 27000
4. La seguridad de la información en la legislación española

UNIDAD DIDÁCTICA 3. DESCRIPCIÓN DE LA NORMA ISO/IEC 27002 PARA LA IMPLANTACIÓN DE UN SISTEMA DE SEGURIDAD

1. ¿Qué es la norma ISO/IEC 27002?
2. Ámbito de aplicación de la Norma ISO/IEC 27002
3. Detalle de la Norma ISO/IEC 27002
4. Controles de los riesgos de seguridad

UNIDAD DIDÁCTICA 4. LA GESTIÓN DE POLÍTICAS DE SEGURIDAD Y DE LOS ACTIVOS QUE INTERVIENEN EN LAS MISMAS

1. Qué son las políticas de seguridad de la información
2. Cómo organizar la seguridad de la información
3. Cómo implantar la seguridad de la información
4. Agentes externos: el control de acceso a terceros
5. Medidas de control a los agentes de seguridad de la información
6. Adjudicación de funciones a los activos de seguridad de la información
7. Clasificación de la información

UNIDAD DIDÁCTICA 5. SEGURIDAD DE LA INFORMACIÓN DE LOS RECURSOS HUMANOS

1. Seguridad de la información propia de los recursos humanos
2. Precauciones de seguridad antes de la contratación
3. Precauciones de seguridad durante el periodo de contratación
4. Precauciones de seguridad en la finalización de la relación laboral o cambio de puesto de trabajo
5. Precauciones de seguridad de la información con respecto a la seguridad física y ambiental o del

entorno

6. Las zonas seguras
7. Los sistemas de protección y seguridad

UNIDAD DIDÁCTICA 6. GESTIÓN DE LOS SISTEMAS DE COMUNICACIONES

1. Introducción a la gestión de las comunicaciones y operaciones
2. Procedimientos y responsabilidades operacionales
3. Prestación externa de los servicios
4. Creación de una metodología para la gestión del sistema
5. Gestión de la seguridad frente a códigos maliciosos y móviles
6. Planificación de las copias de seguridad de la información
7. Planificación y control de la seguridad de la red
8. Gestión de medios
9. Controles en el intercambio de información
10. La seguridad en organizaciones con comercio electrónico
11. Controles para la detección de actividades no autorizadas

UNIDAD DIDÁCTICA 7. EL CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN

1. Qué persigue el control de accesos
2. Objetivos de los sistemas de control de accesos
3. Administración de acceso de usuario
4. Obligaciones del usuario
5. Controles de seguridad de acceso a la red
6. Controles a nivel de sistema operativo
7. Controles a nivel de aplicación
8. Seguridad en dispositivos móviles y teletrabajo

UNIDAD DIDÁCTICA 8. IMPLANTACIÓN DE SISTEMAS DE INFORMACIÓN

1. Justificación de los de sistemas de información
2. Especificaciones de seguridad de los sistemas de información
3. Normas para la gestión de información en las aplicaciones
4. Protecciones a través de controles criptográficos
5. Protección de los archivos del sistema
6. Protección y control de los procesos de desarrollo y soporte
7. Administración y control de la vulnerabilidad técnica

UNIDAD DIDÁCTICA 9. ADMINISTRACIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Y DE LA CONTINUIDAD DEL NEGOCIO

1. Administración de incidentes en la seguridad de la información
2. Revisión y comunicación de eventos y puntos débiles en la seguridad de la información
3. Control de incidentes y optimizaciones en la seguridad de la información
4. Ajustes para la mejora de la continuidad del negocio
5. Controles de la seguridad de la información

UNIDAD DIDÁCTICA 10. EJECUCIÓN DE LOS REQUERIMIENTOS LEGALES Y TÉCNICOS

1. Observancia de los requerimientos legales
2. Ejecución de las políticas y estándares de seguridad
3. Cuestiones a observar en la auditoría de los sistemas de información

MÓDULO 2. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD DIDÁCTICA 1. LA NORMA UNE-ISO/IEC 27001:2014

1. Estándares y Normas Internacionales sobre los SGSI: Familia de Normas ISO 27000
2. La Norma UNE-ISO/IEC 27001:2014. Objeto y ámbito de aplicación
3. Análisis Diferencial de la Norma UNE-ISO/IEC 27001:2014
4. Términos de referencia
5. Importancia de implantar un sistema de seguridad de la información

UNIDAD DIDÁCTICA 2. LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. La seguridad de la información
2. Implantación de sistemas de seguridad de la información
3. Cómo documentar un sistema de seguridad de información

UNIDAD DIDÁCTICA 3. COMETIDO DE LA DIRECCIÓN EN LOS PLANES DE SEGURIDAD

1. Implicación de la dirección
2. Administración de los recursos
3. Estudio e implantación de una política de gestión de la seguridad

UNIDAD DIDÁCTICA 4. CONTROL Y SUPERVISIÓN DE LOS SISTEMAS DE GESTIÓN DE LA INFORMACIÓN POR PARTE DE LA DIRECCIÓN

1. Supervisión del sistema de gestión de la información
2. Perfeccionamiento del sistema de gestión de la seguridad de la información

MÓDULO 3. AUDITORIA DE SEGURIDAD INFORMÁTICA

UNIDAD DIDÁCTICA 1. CRITERIOS SOBRE AUDITORÍA INFORMÁTICA

1. Código deontológico aplicado a la auditoría informática
2. Tipos de auditoría aplicables a los sistemas de información
3. Orientaciones para construir un equipo auditor
4. Controles a realizar para llevar a cabo una auditoría
5. Muestras a tomar para llevar el control de la auditoría
6. Herramientas informáticas para la auditoría (Computer Assisted Audit Tools)
7. Requerimientos que deben cumplir los hallazgos de auditoría
8. Implantación de criterios para agrupar los hallazgos como observaciones o no conformidades
9. Normativas y metodologías a aplicar en la auditoría de sistemas de información

UNIDAD DIDÁCTICA 2. LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. Disposiciones generales de protección de datos de carácter personal
2. Normativa europea, la directiva 95/46/CE

3. Normativa nacional, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley Orgánica de Protección de Datos (LOPD) y Reglamento de Desarrollo de La Ley Orgánica de Protección de Datos (RD 1720/2007)
4. Registro y control de los ficheros con datos de carácter personal pertenecientes a organizaciones
5. Detalle de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007
6. Normas para el desarrollo de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

UNIDAD DIDÁCTICA 3. RIESGOS PROPIOS DE LOS SISTEMAS DE INFORMACIÓN

1. El análisis de riesgos en los sistemas de información
2. Identificación de las vulnerabilidades y amenazas a los sistemas de información.
3. Tipos de código malicioso
4. Elementos del análisis de riesgos y sus relaciones
5. Métodos de control de análisis de riesgos
6. Los activos involucrados en el análisis de riesgos y su valoración
7. Las amenazas que pueden afectar a los activos identificados
8. Detalle de las vulnerabilidades existentes en los sistemas de información
9. Control y mejora del proceso de auditoría y comparación de vulnerabilidades
10. Identificación de los sistemas de prevención en el análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas
11. Creación de escenarios de riesgo para el estudio de los pares activo-amenaza
12. Estudio de la probabilidad e impacto de materialización de los escenarios
13. Determinación del nivel de riesgo para los distintos pares de activo y amenaza
14. Establecimiento de los criterios de evaluación del riesgo para determinar el nivel de aceptación de un riesgo
15. Alternativas de gestión de riesgos
16. Normas para la creación del plan de gestión de riesgos
17. Introducción a la metodología NIST SP 800-30
18. Introducción a la metodología Magerit versión 2

UNIDAD DIDÁCTICA 4. HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

1. Herramientas del sistema operativo
2. Herramientas de redes y sus dispositivos
3. Herramientas de testeo de vulnerabilidades
4. Herramientas para análisis de protocolos
5. Analizadores de páginas web
6. Ataques de diccionario y fuerza bruta

UNIDAD DIDÁCTICA 5. PARTICIPACIÓN DE LOS CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

1. Introducción a los cortafuegos
2. Partes de un cortafuegos de red
3. Clasificación de los cortafuegos por funcionalidad y ubicación
4. Diseños de cortafuegos de red

5. Diseños avanzados de cortafuegos de red

UNIDAD DIDÁCTICA 6. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1. Normas para la implantación de la auditoría de la documentación
2. Instrucciones para la elaboración del plan de auditoría
3. Pruebas de auditoría
4. Instrucciones para la elaboración del informe de auditoría

MÓDULO 4. PREVENCIÓN Y GESTIÓN DE CIBERATAQUES

UNIDAD DIDÁCTICA 1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
2. Identificación y caracterización de los datos de funcionamiento del sistema
3. Arquitecturas más frecuentes de los IDS
4. Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
5. Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

UNIDAD DIDÁCTICA 2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. Análisis previo
2. Definición de políticas de corte de intentos de intrusión en los IDS/IPS
3. Análisis de los eventos registrados por el IDS/IPS
4. Relación de los registros de auditoría del IDS/IPS
5. Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

UNIDAD DIDÁCTICA 3. CONTROL MALWARE

1. Sistemas de detección y contención de Malware
2. Herramientas de control de Malware
3. Criterios de seguridad para la configuración de las herramientas de protección frente a Malware
4. Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a Malware
5. Relación de los registros de auditoría de las herramientas de protección frente a Malware
6. Establecimiento de la monitorización y pruebas de las herramientas de protección frente a Malware
7. Análisis de Malware mediante desensambladores y entornos de ejecución controlada

UNIDAD DIDÁCTICA 4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. Procedimiento de recolección de información relacionada con incidentes de seguridad
2. Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
3. Proceso de verificación de la intrusión
4. Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

UNIDAD DIDÁCTICA 5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1. Establecimiento de las responsabilidades
2. Categorización de los incidentes derivados de intentos de intrusión
3. Establecimiento del proceso de detección y herramientas de registro de incidentes
4. Establecimiento del nivel de intervención requerido en función del impacto previsible
5. Establecimiento del proceso de resolución y recuperación de los sistemas
6. Proceso para la comunicación del incidente a terceros

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE INFORMÁTICO

1. Conceptos generales y objetivos del análisis forense
2. Exposición del Principio de Lockard
3. Guía para la recogida de evidencias electrónicas
4. Guía para el análisis de las evidencias electrónicas recogidas
5. Guía para la selección de las herramientas de análisis forense

MÓDULO 5. SEGURIDAD EN LAS REDES DE DATOS

UNIDAD DIDÁCTICA 1. CRIPTOGRAFÍA

1. Perspectiva histórica y objetivos de la criptografía
2. Teoría de la información
3. Propiedades de la seguridad que se pueden controlar mediante la aplicación de la criptografía
4. Criptografía de clave privada o simétrica
5. Criptografía de clave pública o asimétrica
6. Algoritmos criptográficos más utilizados
7. Funciones hash y los criterios para su utilización
8. Protocolos de intercambio de claves
9. Herramientas de cifrado

UNIDAD DIDÁCTICA 2. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. Identificación de los componentes de una PKI y sus modelos de relaciones
2. Autoridad de certificación y sus elementos
3. Política de certificado y declaración de prácticas de certificación (CPS)
4. Lista de certificados revocados (CRL)
5. Funcionamiento de las solicitudes de firma de certificados (CSR)
6. Infraestructuras de gestión de privilegios (PMI)
7. Campos de certificados de atributos
8. Aplicaciones que se apoyan en la existencia de una PKI

UNIDAD DIDÁCTICA 3. SEGURIDAD EN LAS COMUNICACIONES

1. Las redes privadas virtuales
2. Protocolo IPSec
3. Protocolos SSL y SSH
4. Sistemas SSL VPN
5. Túneles cifrados
6. Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN

MÓDULO 6. ADMINISTRACIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UNIDAD DIDÁCTICA 1. INTRODUCCIÓN Y CONCEPTOS BÁSICOS

1. La sociedad de la información
2. Diseño, desarrollo e implantación
3. Factores de éxito en la seguridad de la información

UNIDAD DIDÁCTICA 2. NORMATIVA ESENCIAL SOBRE EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Estándares y Normas Internacionales sobre los SGSI. ISO 27001:2017
2. Legislación: Leyes aplicables a los SGSI (RGPD)

UNIDAD DIDÁCTICA 3. POLÍTICA DE SEGURIDAD: ANÁLISIS Y GESTIÓN DE RIESGOS

1. Plan de implantación del SGSI
2. Análisis de riesgos
3. Gestión de riesgos

UNIDAD DIDÁCTICA 4. MÉTRICAS PARA CONTROLAR Y OPTIMIZAR EL RENDIMIENTO DE SISTEMAS

1. Marco para el uso de métricas e indicadores
2. Identificación de los elementos a controlar
3. Normas para seleccionar correctamente los indicadores
4. Definir los límites de rendimiento en los sistemas
5. Recolección y análisis de los datos aportados por los indicadores

UNIDAD DIDÁCTICA 5. IMPLANTACIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

1. Los dispositivos usados en las comunicaciones
2. Estudio de los protocolos y servicios de comunicaciones
3. Configuración de los equipos de comunicaciones
4. Procesos y herramientas de control
5. Herramientas de monitorización de sistemas
6. Administración de la información y eventos de seguridad (SIM/SEM)
7. Gestión de eventos de elementos de red y filtrado

UNIDAD DIDÁCTICA 6. SELECCIÓN DEL SISTEMA DE REGISTRO EN FUNCIÓN DE LOS REQUERIMIENTOS DE LA ORGANIZACIÓN

1. 1. Determinación del periodo de almacenamiento
2. Los requerimientos legales en cuanto al registro
3. Medidas de control para cubrir las exigencias de seguridad
4. Identificación de responsables en los sistemas de registro
5. Sistemas de almacenamiento
6. Factores para seleccionar el sistema de almacenamiento

UNIDAD DIDÁCTICA 7. GESTIÓN DEL CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN

1. Mecanismos para validación de usuarios
2. Sistemas usados para el control de accesos, tanto físicos como remotos
3. Legislación aplicable al control de accesos y asignación de privilegios
4. Roles en la organización de acuerdo a las funciones
5. Active Directory y servidores LDAP
6. Sistemas de gestión de identidades y autorizaciones (IAM)
7. Sistemas Single Sign On (SSO)

