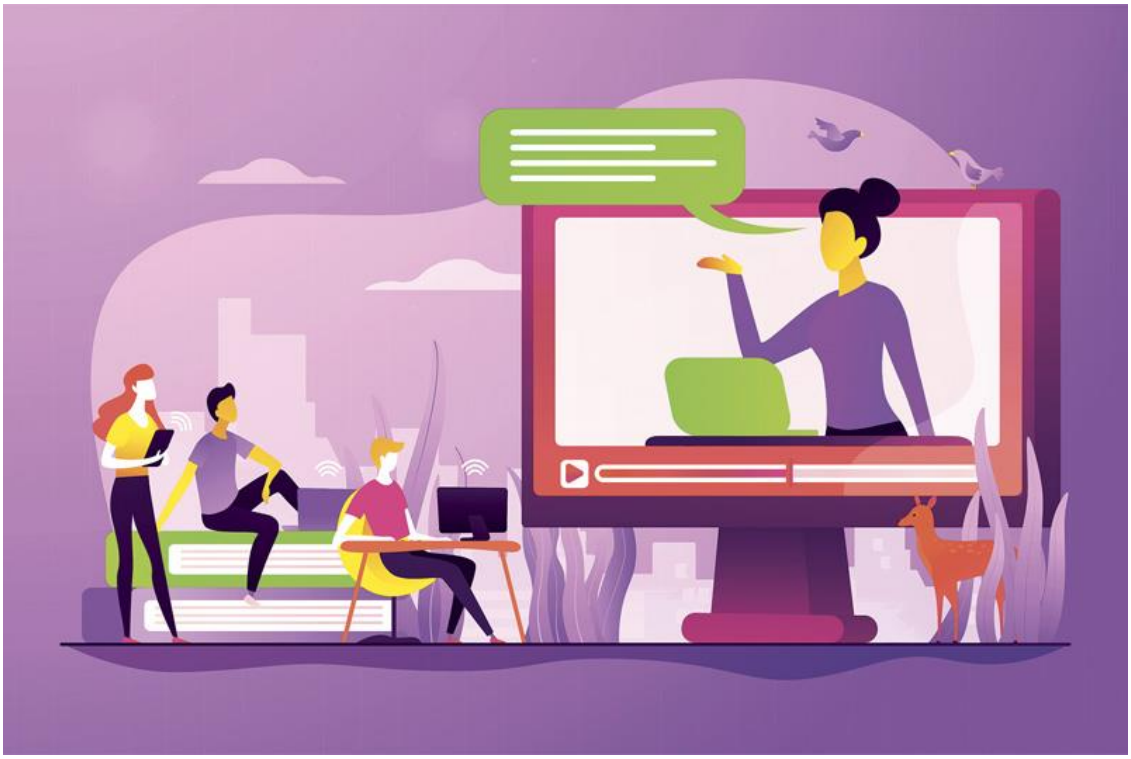

Aprendizaje Online

Otoniel Pérez Velarde | TSDSI

Índice

1.Introducción

A lo largo del informe realizado se realizará la explicación de un proyecto eLearning el cual consistirá en un curso de Seguridad Informática Online. La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con ésta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

2.Objetivos

Los objetivos del curso serán los siguientes:

- Conocer el concepto y modelos de seguridad, los tipos de control de acceso, autentificación de datos y posibles ataques a los que pueden estar sometidos los sistemas informáticos.
- Aprender las pautas y ámbitos de aplicación para el Reglamento de Seguridad y la aplicación de sus principales puntos del reglamento en Windows.
- Saber aplicar la ley de protección de datos aplicada en España: los principios de protección de datos y la forma en que se debe aplicar.
- Garantizar la continuidad de las operaciones de los elementos críticos que componen los sistemas de información, mediante acciones y procedimientos.
- Determinar si los planes de contingencia individuales son capaces de proporcionar el nivel deseado de apoyo a la sección o a los procesos críticos de la empresa, probando la efectividad de los procedimientos expuestos en el plan de contingencias.

3.Condiciones

Este curso va dirigido a todas aquellas personas que quieran formarse en el mundo de la seguridad informática, conociendo los sistemas de protección en los sistemas informáticos que garanticen desde la privacidad de los datos hasta la seguridad en las transacciones de información. Se realizará en un total de 300 horas. La metodología del curso es la siguiente:

- Aprendizaje 100% online: Plataforma web en la que se encuentra todo el contenido de la acción formativa. A través de ella podrá estudiar y comprender el temario mediante actividades prácticas. Autoevaluaciones y una evaluación final.
- Campus Virtual: Accede al campus virtual desde cualquier dispositivo, las 24 horas del día. Contando con acceso ilimitado a los contenidos del curso.

- Equipo docente especializado: El alumnado cuenta con un equipo de profesionales en esta área de formación, ofreciéndole un acompañamiento personalizado.
- Aprendizaje colaborativo: Método de enseñanza totalmente multidisciplinar. Lo que facilita el estudio y una mejor asimilación conceptual. Sumando esfuerzos, talentos y competencias.

4.Diseño del curso

4.1DISEÑO GENERAL

Este curso contará principalmente de 1 módulo de aprendizaje, el cual estará dividido en 12 UAs (Unidades de Aprendizaje) las cuales son las siguientes:

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS
2. ANÁLISIS DE IMPACTO DE NEGOCIO
3. GESTIÓN DE RIESGOS
4. PLAN DE IMPLANTACIÓN DE SEGURIDAD
5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS
7. IDENTIFICACIÓN DE SERVICIOS
8. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS
9. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN
10. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS
11. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS
12. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

4.2DISEÑOS DE CADA UA

En cada una de las Unidades de Aprendizajes se tendrán como recursos los siguientes: Temario en PDF, Campus Virtual, Profesores especializados, videos y ejemplos de ayuda. Así como para cada una de ellas el alumno podrá realizar actividades de autoevaluación para comprobar si ha adquirido los conocimientos de la unidad.

4.2.1 CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

Objetivos: Conocimiento acerca de los criterios generales sobre seguridad de los equipos informáticos.

Requisitos: Ninguno

Contenidos:

1. Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información

2. Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes

3. Salvaguardas y tecnologías de seguridad más habituales

4. La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

4.2.2 ANÁLISIS DE IMPACTO DE NEGOCIO

Objetivos: Conocimiento acerca del impacto de negocio causado por la seguridad informática

Requisitos: Superar la UA 1

Contenidos:

1. Identificación de procesos de negocio soportados por sistemas de información

2. Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio

3. Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

4.2.3 GESTIÓN DE RIESGOS

Objetivos: Conocimiento acerca de la gestión de riesgos informáticos en las organizaciones

Requisitos: Superar la UA 2

Contenidos:

1. Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes

2. Metodologías comúnmente aceptadas de identificación y análisis de riesgos

3. Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

4.2.4 PLAN DE IMPLANTACIÓN DE SEGURIDAD

Objetivos: Conocimiento acerca del desarrollo de un plan de implantación de seguridad

Requisitos: Superar la UA 3

Contenidos:

1. Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio

2. Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información

3. Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

4.2.5 PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Objetivos: Conocimiento acerca de la protección de datos de carácter personal

Requisitos: Superar la UA 4

Contenidos:

1. Principios generales de protección de datos de carácter personal

2. Infracciones y sanciones contempladas en la legislación vigente en materia de protección de datos de carácter personal

3. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización

4. Elaboración del documento de seguridad requerido por la legislación vigente en materia de protección de datos de carácter personal

4.2.6 SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

Objetivos: Conocimiento acerca de la seguridad física e industrial de los sistemas de seguridad

Requisitos: Superar la UA 5

Contenidos:

1. Determinación de los perímetros de seguridad física

2. Sistemas de control de acceso físico más frecuentes a las instalaciones de la organización y a las áreas en las que estén ubicados los sistemas informáticos

3. Criterios de seguridad para el emplazamiento físico de los sistemas informáticos

4. Exposición de elementos más frecuentes para garantizar la calidad y continuidad del suministro eléctrico a los sistemas informáticos

5. Requerimientos de climatización y protección contra incendios aplicables a los sistemas informáticos

6. Elaboración de la normativa de seguridad física e industrial para la organización

7. Sistemas de ficheros más frecuentemente utilizados

8. Establecimiento del control de accesos de los sistemas informáticos a la red de comunicaciones de la organización

9. Configuración de políticas y directivas del directorio de usuarios

10. Establecimiento de las listas de control de acceso (ACLs) a ficheros

11. Gestión de altas, bajas y modificaciones de usuarios y los privilegios que tienen asignados

12. Requerimientos de seguridad relacionados con el control de acceso de los usuarios al sistema operativo

13. Sistemas de autenticación de usuarios débiles, fuertes y biométricos

14. Relación de los registros de auditoría del sistema operativo necesarios para monitorizar y supervisar el control de accesos

15. Elaboración de la normativa de control de accesos a los sistemas informáticos

4.2.7 IDENTIFICACIÓN DE SERVICIOS

Objetivos: Conocimiento acerca de la identificación de servicios

Requisitos: Superar la UA 6

Contenidos:

1. Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información

2. Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios

3. Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

4.2.8 IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

Objetivos: Conocimiento acerca de la implantación y configuración de cortafuegos

Requisitos: Superar la UA 7

Contenidos:

1. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

2. Criterios de seguridad para la segregación de redes en el cortafuego mediante Zonas Desmilitarizadas / DMZ

3. Utilización de Redes Privadas Virtuales / VPN para establecer canales seguros de comunicaciones

4. Definición de reglas de corte en los cortafuegos

5. Relación de los registros de auditoría del cortafuego necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad

6. Establecimiento de la monitorización y pruebas de los cortafuegos

4.2.9 ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

Objetivos: Conocimiento acerca del análisis de riesgos de los sistemas de información

Requisitos: Superar la UA 8

Contenidos:

1. Introducción al análisis de riesgos

2. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura

3. Particularidades de los distintos tipos de código malicioso

4. Principales elementos del análisis de riesgos y sus modelos de relaciones

5. Metodologías cualitativas y cuantitativas de análisis de riesgos

6. Identificación de los activos involucrados en el análisis de riesgos y su valoración

7. Identificación de las amenazas que pueden afectar a los activos identificados previamente

8. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra

9. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría

10. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

11. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse

12. Determinación de la probabilidad e impacto de materialización de los escenarios

13. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza

14. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no

15. Relación de las distintas alternativas de gestión de riesgos

16. Guía para la elaboración del plan de gestión de riesgos

17. Exposición de la metodología NIST SP 800-30

18. Exposición de la metodología Magerit versión 2

4.2.10 USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

Objetivos: Conocimiento acerca del uso de herramientas para la auditoría de sistemas

Requisitos: Superar la UA 9

Contenidos:

1. Herramientas del sistema operativo tipo Ping, Traceroute, etc.

2. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc

3. Herramientas de análisis de vulnerabilidades tipo Nessus

4. Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc.

5. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc.

6. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc

4.2.11 DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

Objetivos: Conocimiento acerca de los aspectos sobre cortafuegos en auditorias de sistemas informáticos

Requisitos: Superar la UA 10

Contenidos:

1. Principios generales de cortafuegos

2. Componentes de un cortafuego de red

3. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad

4. Arquitecturas de cortafuegos de red

5. Otras arquitecturas de cortafuegos de red

4.2.12 GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Objetivos: Conocimiento acerca de la ejecución de las distintas fases de la auditoria de sistemas de información

Requisitos: Superar la UA 12

Contenidos:

1. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada

2. Guía para la elaboración del plan de auditoría

3. Guía para las pruebas de auditoría

4. Guía para la elaboración del informe de auditoría

5.Conclusiones

Tras la realización del informe de esta práctica podemos decir que esta ha sido de gran ayuda, ya que hemos podido ver todos los puntos y los pasos a seguir para implementar un proyecto de aprendizaje online.

6.Bibliografía

[1] S. R. M. Cáceres - Enseñanza online – Disponible en: https://aep22.ulpgc.es/pluginfile.php/275444/mod_resource/content/0/Servicios%20Electrónicos-Aprendizaje%20online.pdf