Actividades formativas

CÓDIGO	TÍTULO
FFP-AV-2022-01	Ciberseguridad en Entornos de las Tecnologías de la Información

Características de los cursos

FFP-AV-2022-01.- Ciberseguridad en Entornos de las Tecnologías de la Información

Nivel: Intermedio

Número de horas: 100

Plazas: 30

Período de realización Del 28 de septiembre de 2022 al 8 de noviembre de 2022

Localidad de impartición: Curso online

Profesorado preferente: Encargado de impartición del curso de especialización Ciberseguridad en Entornos de las Tecnologías de la Información;

Objetivos:

- Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización, aplicando la normativa vigente.
- Detectar e investigar incidentes de ciberseguridad, documentándolos e incluyéndolos en los planes de securización de la organización.
- Diseñar planes de securización contemplando las mejores prácticas para el bastionado de sistemas y redes.
- Configurar sistemas de control de acceso y autenticación en sistemas informáticos, cumpliendo los requisitos de seguridad y minimizando las posibilidades de exposición a ataques.
- Diseñar y administrar sistemas informáticos en red y aplicar las políticas de seguridad establecidas, garantizando la funcionalidad requerida con un nivel de riesgo controlado.
- Analizar el nivel de seguridad requerido por las aplicaciones y los vectores de ataque más habituales, evitando incidentes de ciberseguridad.
- Implantar sistemas seguros de desplegado de software con la adecuada coordinación entre los desarrolladores y los responsables de la operación del software.
- Realizar análisis forenses informáticos analizando y registrando la información relevante relacionada.
- Detectar vulnerabilidades en sistemas, redes y aplicaciones, evaluando los riesgos asociados.
- Definir y aplicar procedimientos para el cumplimiento normativo en materia de ciberseguridad y de protección de datos personales, implementándolos tanto internamente como en relación con terceros.
- Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente, respondiendo a los requisitos establecidos.

Competencias

Competencia científica	Competencia en innovación y mejora
Competencia didáctica	Competencia Digital (TIC)

Contenidos

1. Incidentes de ciberseguridad:
    - Desarrollo de planes de prevención y concienciación en ciberseguridad.
    - Auditoría de incidentes de ciberseguridad.
    - Investigación de los incidentes de ciberseguridad.
    - Implementación de medidas de ciberseguridad.
    - Detección y documentación de incidentes de ciberseguridad.

2. Bastionado de redes y sistemas.
    - Diseño de planes de securización.
    - Configuración de sistemas de control de acceso y autenticación de personas:
    - Administración de credenciales de acceso a sistemas informáticos.
    - Diseño de redes de computadores seguras.
    - Configuración de dispositivos y sistemas informáticos.
    - Configuración de dispositivos para la instalación de sistemas informáticos.
    - Configuración de los sistemas informáticos.
3. Puesta en producción segura.
    - Prueba de aplicaciones *web* y para dispositivos móviles.
    - Determinación del nivel de seguridad requerido por aplicaciones.
    - Detección y corrección de vulnerabilidades de aplicaciones *web*.
    - Detección de problemas de seguridad en aplicaciones para dispositivos móviles.
    - Implantación de sistemas seguros de desplegado de *software*.

4. Análisis forense informático.
    - Aplicación de metodologías de análisis forenses.
    - Realización de análisis forenses en dispositivos móviles.
    - Realización de análisis forenses en *Cloud*:
    - Realización de análisis forenses en *IoT*:
    - Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe.

5. *Hacking* ético.
    - Determinación de las herramientas de monitorización para detectar vulnerabilidades:
    - Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas.
    - Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros.
    - Consolidación y utilización de sistemas comprometidos.
    - Ataque y defensa en entorno de pruebas, a aplicaciones *web*.
6. Normativa de ciberseguridad.
    - Puntos principales de aplicación para un correcto cumplimiento normativo.
    - Diseño de sistemas de cumplimiento normativo.
    - Legislación para el cumplimiento de la responsabilidad penal.
    - Legislación y jurisprudencia en materia de protección de datos.
    - Normativa vigente de ciberseguridad de ámbito nacional e internacional:
    - Esquema Nacional de Seguridad (ENS).
    - Ley PIC (Protección de infraestructuras críticas).