Curso de Especialización de formación profesional en ciberseguridad en entornos de las tecnologías de la información

Incidentes de ciberseguridad

Desarrollo de planes de prevención y concienciación en ciberseguridad (Incidentes de ciberseguridad)

- Principios generales en materia de ciberseguridad
- Normativa de protección del puesto del trabajo
- Plan de formación y concienciación en materia de ciberseguridad
- Materiales de formación y concienciación
- Auditorías internas de cumplimiento en materia de prevención

Auditoría de incidentes de ciberseguridad (Incidentes de ciberseguridad)

- Taxonomía de incidentes de ciberseguridad
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes: tipos y fuentes
- Controles, herramientas y mecanismos de detección e identificación de incidentes de seguridad física
- Controles, herramientas y mecanismos de monitorización, identificación, detección y alerta de incidentes a

través de la investigación en fuentes abiertas (OSINT)
- Clasificación, valoración, documentación, seguimiento inicial de incidentes de ciberseguridad

Investigación de los incidentes de ciberseguridad (Incidentes de ciberseguridad)

- Recopilación de evidencias
- Análisis de evidencias
- Investigación del incidente
- Intercambio de información del incidente con proveedores u organismos competentes
- Medidas de contención de incidentes

Implementación de medidas de ciberseguridad (Incidentes de ciberseguridad)

- Desarrollar procedimientos de actuación detallados para dar respuesta, mitigar, eliminar o contener los tipos de incidentes
- Implantar capacidades de ciberresiliencia
- Establecer flujos de toma de decisiones y escalado interno y/o externo adecuados
- Tareas para reestablecer los servicios afectados por incidentes
- Documentación
- Seguimiento de incidentes para evitar una situación similar

Detección y documentación de incidentes de ciberseguridad (Incidentes de

ciberseguridad)

- Desarrollar procedimientos de actuación para la notificación de incidentes
- Notificación interna de incidentes
- Notificación de incidentes a quienes corresponda

Bastionado de redes y sistemas

Diseño de planes de securización (Bastionado de redes y sistemas)

- Análisis de riesgos
- Principios de la Economía Circular en la Industria 4.0
- Plan de medidas técnicas de seguridad
- Políticas de securización más habituales
- Guías de buenas prácticas para la securización de sistemas y redes
- Estándares de securización de sistemas y redes
- Caracterización de procedimientos, instrucciones y recomendaciones
- Niveles, escalados y protocolos de atención a incidencias

Configuración de sistemas de control de acceso y autenticación de personas (Bastionado de redes y sistemas)

- Mecanismos de autenticación. Tipos de factores
- Autenticación basada en distintas técnicas

Administración de credenciales de acceso a sistemas informáticos (Bastionado de

redes y sistemas)

- Gestión de credenciales
- Infraestructuras de Clave Pública (PKI)
- Acceso por medio de Firma electrónica
- Gestión de accesos. Sistemas NAC (Network Access Control, Sistemas de Gestión de Acceso a la Red)
- Gestión de cuentas privilegiadas
- Protocolos RADIUS y TACACS, servicio KERBEROS, entre otros

Diseño de redes de computadores seguras (Bastionado de redes y sistemas)

- Segmentación de redes
- Subnetting
- Redes virtuales (VLANs)
- Zona desmilitarizada (DMZ)
- Seguridad en redes inalámbricas (WPA2, WPA3, etc.)
- Protocolos de red seguros (IPSec, etc.)

Configuración de dispositivos y sistemas informáticos (Bastionado de redes y sistemas)

- Seguridad perimetral. Firewalls de Próxima Generación
- Seguridad de portales y aplicativos web. Soluciones WAF (Web Aplication Firewall)
- Seguridad del puesto de trabajo y endpoint fijo y móvil. AntiAPT, antimalware
- Seguridad de entornos cloud. Soluciones CASB
- Seguridad del correo electrónico
- Soluciones DLP (Data Loss Prevention)
- Herramientas de almacenamiento de logs
- Protección ante ataques de denegación de servicio distribuido (DDoS)

- Configuración segura de cortafuegos, enrutadores y proxies
- Redes privadas virtuales (VPNs), y túneles (protocolo IPSec)
- Monitorización de sistemas y dispositivos
- Herramientas de monitorización (IDS, IPS)
- SIEMs (Gestores de Eventos e Información de Seguridad)
- Soluciones de Centros de Operación de Red, y Centros de Seguridad de Red: NOCs y SOCs

Configuración de dispositivos para la instalación de sistemas informáticos (Bastionado de redes y sistemas)

- Precauciones previas a la instalación de un sistema informático: aislamiento, configuración del control de acceso a la BIOS, bloqueo del orden de arranque de los dispositivos, entre otros
- Seguridad en el arranque del sistema informático, configuración del arranque seguro
- Seguridad de los sistemas de ficheros, cifrado, particionado, entre otros

Configuración de los sistemas informáticos (Bastionado de redes y sistemas)

- Reducción del número de servicios, Telnet, RSSH, TFTP, entre otros
- Hardening de procesos (eliminación de información de depuración en caso de errores, aleatorización de la memoria virtual para evitar exploits, etc.)
- Eliminación de protocolos de red innecesarios (ICMP, entre otros)
- Securización de los sistemas de administración remota
- Sistemas de prevención y protección frente a virus e

intrusiones (antivirus, HIDS, etc.)
- Configuración de actualizaciones y parches automáticos
- Sistemas de copias de seguridad
- Shadow IT y políticas de seguridad en entornos SaaS

Puesta en producción segura

Prueba de aplicaciones web y para dispositivos móviles (Puesta en producción segura)

- Fundamentos de la programación
- Lenguajes de programación interpretados y compilados
- Código fuente y entornos de desarrollo
- Ejecución de software
- Elementos principales de los programas
- Pruebas. Tipos
- Seguridad en los lenguajes de programación y sus entornos de ejecución («sandboxes»)

Determinación del nivel de seguridad requerido por aplicaciones (Puesta en producción segura)

- Fuentes abiertas para el desarrollo seguro
- Listas de riesgos de seguridad habituales: OWASP Top Ten (web y móvil)
- Requisitos de verificación necesarios asociados al nivel de seguridad establecido
- Comprobaciones de seguridad a nivel de aplicación: ASVS (Application Security Verification Standard)

Detección y corrección de

vulnerabilidades de aplicaciones web (Puesta en producción segura)

- Desarrollo seguro de aplicaciones web
- Listas públicas de vulnerabilidades de aplicaciones web. OWASP Top Ten
- Entrada basada en formularios. Inyección. Validación de la entrada
- Estándares de autenticación y autorización
- Robo de sesión
- Vulnerabilidades web
- Almacenamiento seguro de contraseñas
- Contramedidas. HSTS, CSP, CAPTCHAs, entre otros
- Seguridad de portales y aplicativos web. Soluciones WAF(Web Application Firewall)

Detección de problemas de seguridad en aplicaciones para dispositivos móviles (Puesta en producción segura)

- Modelos de permisos en plataformas móviles. Llamadas al sistema protegidas
- Firma y verificación de aplicaciones
- Almacenamiento seguro de datos
- Validación de compras integradas en la aplicación
- Fuga de información en los ejecutables
- Soluciones CASB

Implantación de sistemas seguros de desplegado de software (Puesta en producción segura)

- Puesta segura en producción
- Prácticas unificadas para el desarrollo y operación del software (DevOps)
- Sistemas de control de versiones

- Sistemas de automatización de construcción (build)
- Integración continua y automatización de pruebas
- Escalado de servidores. Virtualización. Contenedores
- Gestión automatizada de configuración de sistemas
- Herramientas de simulación de fallos
- Orquestación de contenedores

Análisis forense informático

Aplicación de metodologías de análisis forenses (Análisis forense informático)

- Identificación de los dispositivos a analizar
- Recolección de evidencias (trabajar un escenario)
- Análisis de la línea de tiempo (TimeStamp)
- Análisis de volatilidad – Extracción de información (Volatility)
- Análisis de Logs, herramientas más usadas

Realización de análisis forenses en dispositivos móviles (Análisis forense informático)

- Métodos para la extracción de evidencias
- Herramientas de mercado más comunes

Realización de análisis forenses en IoT (Análisis forense informático)

- Identificar los dispositivos a analizar
- Adquirir y extraer las evidencias
- Analizar las evidencias de manera manual y automática
- Documentar el proceso realizado
- Establecer la línea temporal
- Mantener la cadena de custodia
- Elaborar las conclusiones

- Presentar y exponer las conclusiones

Documentación y elaboración de informes de análisis forenses. Apartados de los que se compone el informe (Análisis forense informático)

- Hoja de identificación (título, razón social, nombre y apellidos, firma)
- Índice de la memoria
- Objeto (objetivo del informe pericial y su justificación)
- Alcance (ámbito de aplicación del informe pericial – resumen ejecutivo para una supervisión rápida del contenido y resultados)
- Antecedentes (aspectos necesarios para la comprensión de las alternativas estudiadas y las conclusiones finales)
- Normas y referencias (documentos y normas legales y reglamentos citados en los distintos apartados)
- Definiciones y abreviaturas (definiciones, abreviaturas y expresiones técnicas que se han utilizado a lo largo del informe)
- Requisitos (bases y datos de partida establecidos por el cliente, la legislación, reglamentación y normativa aplicables)
- Análisis de soluciones – resumen de conclusiones del informe pericial (alternativas estudiadas, qué caminos se han seguido para llegar a ellas, ventajas e inconvenientes de cada una y cuál es la solución finalmente elegida y su justificación)
- Anexos

Hacking ético

Determinación de las herramientas de monitorización para detectar vulnerabilidades (Hacking ético)

- Elementos esenciales del hacking ético
- Diferencias entre hacking, hacking ético, tests de penetración y hacktivismo
- Recolección de permisos y autorizaciones previos a un test de intrusión
- Fases del hacking
- Auditorías de caja negra y de caja blanca
- Documentación de vulnerabilidades
- Clasificación de herramientas de seguridad y hacking
- ClearNet, Deep Web, Dark Web, Darknets. Conocimiento, diferencias y herramientas de acceso: Tor. ZeroNet, FreeNet

Ataque y defensa en entorno de pruebas, de las comunicaciones inalámbricas (Hacking ético)

- Comunicación inalámbrica
- Modo infraestructura, ad-hoc y monitor
- Análisis y recolección de datos en redes inalámbricas
- Técnicas de ataques y exploración de redes inalámbricas
- Ataques a otros sistemas inalámbricos
- Realización de informes de auditoría y presentación de resultados

Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros (Hacking ético)

- Fase de reconocimiento (footprinting)
- Fase de escaneo (fingerprinting)

- Monitorización de tráfico
- Interceptación de comunicaciones utilizando distintas técnicas
- Manipulación e inyección de tráfico
- Herramientas de búsqueda y explotación de vulnerabilidades
- Ingeniería social. Phising
- Escalada de privilegios

Consolidación y utilización de sistemas comprometidos (Hacking ético)

- Administración de sistemas de manera remota
- Ataques y auditorías de contraseñas
- Pivotaje en la red
- Instalación de puertas traseras con troyanos (RAT, Remote Access Trojan)

Ataque y defensa en entorno de pruebas, a aplicaciones web (Hacking ético)

- Negación de credenciales en aplicaciones web
- Recolección de información
- Automatización de conexiones a servidores web (ejemplo: Selenium)
- Análisis de tráfico a través de proxies de intercepción
- Búsqueda de vulnerabilidades habituales en aplicaciones web
- Herramientas para la explotación de vulnerabilidades web

Normativa de ciberseguridad

Puntos principales de aplicación para un correcto cumplimiento normativo

(Normativa de ciberseguridad)

- Introducción al cumplimiento normativo (Compliance: objetivo, definición y conceptos principales)
- Principios del buen gobierno y ética empresarial
- Compliance Officer: funciones y responsabilidades
- Relaciones con terceras partes dentro del Compliance

Diseño de sistemas de cumplimiento normativo (Normativa de ciberseguridad)

- Sistemas de Gestión de Compliance
- Entorno regulatorio de aplicación
- Análisis y gestión de riesgos, mapas de riesgos
- Documentación del sistema de cumplimiento normativo diseñado

Legislación para el cumplimiento de la responsabilidad penal (Normativa de ciberseguridad)

- Riesgos penales que afectan a la organización
- Sistemas de gestión de Compliance penal
- Sistemas de gestión anticorrupción

Legislación y jurisprudencia en materia de protección de datos (Normativa de ciberseguridad)

- Principios de protección de datos
- Novedades del RGPD de la Unión Europea
- Privacidad por Diseño y por Defecto
- Análisis de Impacto en Privacidad (PIA), y medidas de seguridad
- Delegado de Protección de Datos (DPO)

Normativa vigente de ciberseguridad de ámbito nacional e internacional (Normativa de ciberseguridad)

- Normas nacionales e internacionales
- Sistema de Gestión de Seguridad de la Información (estándares internacionales) (ISO 27.001)
- Acceso electrónico de los ciudadanos a los Servicios Públicos

Esquema Nacional de Seguridad (ENS) (Normativa de ciberseguridad)

- Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301)
- Directiva NIS
- Legislación sobre la protección de infraestructuras críticas

Ley PIC (Protección de infraestructuras críticas) (Normativa de ciberseguridad)

- Ley PIC (Protección de infraestructuras críticas)