ANEXO I
TECNOLOGIAS DE LA INFORMACIÓN
DIRECCIÓN

CÓDIGO DEL PUESTO 9000252
DENOMINACIÓN DEL PUESTO ..... Técnico/a Analista de Ciberseguridad
NIVEL C.D..... 25
COMPL. ESPECÍFICO ANUAL..... 19.539,72€
JORNADA .....Mañana y dos tardes (M2)
SUBGRUPO ADSC. A1
CUERPO/ESCALA ....Escala Especial Superior de Sistemas y Tecnologías de la Información de la UAM/ Ex11

FUNCIONES JEFE/A DE SECCIÓN:

- Colaboración con los órganos superiores en la programación de actividades y definición de objetivos, así como en su ejecución y seguimiento.
- Diseñar y definir los objetivos y criterios de actuación de la Sección. Dirección, tramitación, impulso y supervisión de los procedimientos administrativos competencia de la Sección.
- Dirección de los medios humanos y técnicos a los efectos de coordinar, planificar y programar las tareas de la unidad para la consecución de los objetivos fijados.
- Cualquier otra tarea de carácter administrativo afín a la categoría del puesto y semejantes a las anteriormente descritas que pueda serle encomendada por razón de las competencias que tiene asignadas la Unidad.

FUNCIONES ESPECÍFICAS DEL PUESTO:

Detección, Análisis y Gestión de Amenazas y Vulnerabilidades.

- **Monitorización y Alerta** de las redes, sistemas y aplicaciones de la universidad para detección de incidentes de seguridad.
- **Análisis de Vulnerabilidades y Gestión de Riesgos** realizando evaluaciones de seguridad, escaneos de vulnerabilidades, análisis de riesgos y auditorías de seguridad.
- **Investigación Forense y Análisis de Malware** investigando ciberataques e incidentes de seguridad, realizando análisis forense digital de los sistemas comprometidos y análisis de malware para determinar la causa raíz, el alcance del impacto y los vectores de ataque utilizados.
- **Uso de Herramientas Avanzadas** empleando y configurando herramientas de Security Information and Event Management (SIEM) para la normalización y correlación de eventos, la gestión de alertas y la creación de cuadros de mando de seguridad que permitan una visión integral del estado de la ciberseguridad.

Respuesta a Incidentes de Seguridad y Recuperación.

- **Desarrollo de Planes** diseñando, implementando y manteniendo planes de respuesta a incidentes de seguridad (IRP) y planes de recuperación ante desastres (DRP) para garantizar la continuidad de los servicios críticos de la universidad ante cualquier eventualidad.
- **Gestión de Incidentes** ejecutando y coordinando acciones de contención, erradicación y recuperación ante ciberincidentes para minimizar el impacto y el tiempo de inactividad.

- **Informes y Mejora Continua** elaborando informes detallados post-incidente para la dirección, incluyendo un análisis de las lecciones aprendidas y recomendaciones concretas para la mejora continua de los procesos y sistemas de seguridad.

Implementación y Mantenimiento de Medidas de Seguridad.

- **Configuración de Herramientas de Seguridad** usando, configurando y gestionando software y hardware de protección, incluyendo cortafuegos (firewalls), programas de encriptación de datos, soluciones antivirus/antimalware, sistemas de detección y prevención de intrusiones (IDS/IPS), sistemas de prevención de pérdida de datos (DLP) y redes privadas virtuales (VPN).
- **Diseño de Arquitecturas Seguras** diseñando e implementando arquitecturas de redes seguras, así como gestionar eficazmente la identidad y el acceso a los sistemas y datos de la universidad.
- **Hardening de Sistemas** asegurando y "bastionando" sistemas operativos (Linux, Windows, macOS, dispositivos móviles) y aplicaciones, garantizando una puesta en producción segura y el cumplimiento de las mejores prácticas de seguridad.
- **Seguridad en Entornos Emergentes** con la gestión de la seguridad en entornos de computación en la nube (cloud security) y en la creciente red de dispositivos IoT (Internet of Things) dentro del campus universitario.

Auditoría, Cumplimiento Normativo y Gestión de Riesgos.

- **Cumplimiento Normativo** contribuyendo al cumplimiento de las leyes, reglamentos y normas internas y externas relacionadas con la seguridad de la información y la protección de datos.
- **Desarrollo de Políticas y Procedimientos** desarrollando, documentando y manteniendo políticas, procedimientos y flujos de trabajo de seguridad y cumplimiento, garantizando su alineación con los estándares y las mejores prácticas de la industria.
- **Análisis y Gestión de Riesgos** realizando análisis y gestión de riesgos de seguridad de la información, utilizando metodologías reconocidas como Magerit v3, para identificar, evaluar y tratar los riesgos de manera sistemática.
- **Auditorías de Seguridad** planificando y ejecutando auditorías de seguridad internas y externas para verificar la efectividad de los controles de seguridad implementados y el cumplimiento normativo.

Desarrollo Seguro y Hacking Ético.

- **Seguridad en el Desarrollo de Software** asesorando y colaborando en el diseño y desarrollo de aplicaciones que garanticen la privacidad y seguridad de la información desde las fases iniciales del ciclo de vida del software (Security by Design).
- **Pruebas de Penetración y Hacking Ético** realizando pruebas de penetración (pentesting) y ejercicios de hacking ético para descubrir proactivamente vulnerabilidades en sistemas, redes y aplicaciones, simulando ataques reales para fortalecer las defensas.
- **Automatización de Seguridad (DevSecOps)** Implementando y gestionando herramientas y procesos de automatización y orquestación de seguridad (DevSecOps) para integrar la seguridad en el ciclo de desarrollo y operaciones de TI.

Concienciación, Formación y Soporte a Usuarios

- **Concienciación y Capacitación** diseñando e impartiendo programas de capacitación y concienciación, promoviendo las mejores prácticas y una cultura de seguridad robusta.
- **Comunicación de Políticas** comunicando de manera efectiva las normas de cumplimiento, las políticas de seguridad y los procedimientos a seguir tanto al equipo de TI como a la comunidad universitaria en general.
- **Soporte Técnico en Seguridad** proporcionando soporte técnico especializado para resolver problemas relacionados con la seguridad en aplicaciones, sistemas y dispositivos de los usuarios.

MÉRITOS ESPECÍFICOS

	PUNTUACIÓN MÁXIMA
Título de Grado en Ingeniería Informática.	1
Nivel de inglés nivel C1 o superior. (0.5 puntos por nivel)	1
Experiencia en puesto similar (Técnico/a Analista de Ciberseguridad) en la UAM. (0.3 puntos por año)	9
Experiencia en puesto similar (Técnico/a Analista de Ciberseguridad) en otra Administración Pública Española o sector privado. (0.15 punto por año)	4

CURSOS

	PUNTUACIÓN MÁXIMA
Cursos de ciberseguridad. (0.75 puntos por curso)	9
Cursos de normativa, buenas prácticas y legislación. (0.5 puntos por curso)	2
Cursos de auditoría de seguridad informática. (0.5 puntos por curso)	1
Cursos de contenedores y orquestación con kubernetes. (0.5 puntos por curso)	2
Cursos de automatización. (0.5 puntos por curso)	1