EUROPEAN UNION AGENCY FOR CYBERSECURITY

ECSF

MARCO EUROPEO DE COMPETENCIAS EN CIBERSEGURIDAD

SEPTIEMBRE 2022

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

aniversario 50 1973 - 2023

SOBRE ENISA

La Agencia de Ciberseguridad de la Unión Europea, ENISA, es la agencia de la Unión dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Creada en 2004 y reforzada por la Ley de Ciberseguridad de la UE, la Agencia de Ciberseguridad de la Unión Europea contribuye a la ciberpolítica de la UE, mejora la fiabilidad de los productos, servicios y procesos de las TIC con sistemas de certificación de la ciberseguridad, coopera con los Estados miembros y los organismos de la UE y ayuda a Europa a prepararse para los retos cibernéticos del mañana. Mediante el intercambio de conocimientos, el desarrollo de capacidades y la sensibilización, la Agencia colabora con sus principales interesados para reforzar la confianza en la economía conectada, aumentar la resiliencia de la infraestructura de la Unión y, en última instancia, mantener la seguridad digital de la sociedad y los ciudadanos europeos. Puede encontrar más información sobre ENISA y su trabajo aquí: www.enisa.europa.eu

CONTACTO

Para contactar con el editor, por favor use euskills@enisa.europa.eu

AGRADECIMIENTOS

Este marco es el resultado de la opinión y el acuerdo de los expertos del Grupo de trabajo ad hoc sobre el marco de competencias, compuesto por Agata BEKIER, Vladlena BENSON, Jutta BREYER, Fabio DI FRANCO, Sara GARCIA, Athanasios GRAMMATOPOULOS, Markku KORKIAKOSKI, Csaba KRASZNAY, Haralambos MOURATIDIS, Christina GEORGHIADOU, Erwin ORYE, Edmundas PIESARSKAS, Nineta POLEMI, Paresh RATHOD, Antonio SANNINO, Fred VAN NOORD, Richard WIDH, Nina OLESEN y Jan HAJNY.

Fabio DI FRANCO y Athanasios GRAMMATOPOULOS dirigieron esta actividad para ENISA.

NOTA LEGAL

ENISA mantiene sus derechos de propiedad intelectual en relación con esta publicación.

NOTA SOBRE COPYRIGHT

ISBN: 978-92-9204-584-5 - DOI: 10.2824/859537

TRADUCCIÓN

Esta versión ha sido traducida del inglés al español por AMETIC.

TABLA DE CONTENIDOS

1. VISIÓN GENERAL

- Director de seguridad de la información (CISO)
- Especialista en inteligencia sobre ciberamenazas
- Gestor de incidencias ciebernéticas
- Arquitecto de ciberseguridad
- Responsable de ciberlegislación, política y cumplimiento
- Auditor de ciberseguridad
- Educador en ciberseguridad
- Implementador de ciberseguridad
- Investigador en ciberseguridad
- Gestor de riesgos de ciberseguridad
- Investigador forense digital
- Eamen de penetración

2. PERFILES

2.1. DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN (CISO)

Título(s) alternativo(s)

Director del Programa de Ciberseguridad

Responsable de seguridad de la información (ISO)

Responsable de seguridad de la información

Jefe de seguridad de la información

Responsable de seguridad de TI/TIC

Resumen

Gestiona la estrategia de ciberseguridad de una organización y su aplicación para garantizar que los sistemas, servicios y activos digitales estén adecuadamente seguros y protegidos.

Misión

Define, mantiene y comunica la visión, la estrategia, las políticas y los procedimientos de ciberseguridad. Gestiona la aplicación de la política de ciberseguridad en toda la organización. Garantiza el intercambio de información con autoridades externas y organismos profesionales.

Producto(s)

-Estrategia de ciberseguridad

-Política de ciberseguridad

Tarea(s) principal(es)

-Definir, aplicar, comunicar y mantener los objetivos, requisitos, estrategias y políticas de ciberseguridad, en consonancia con la estrategia empresarial, para apoyar los objetivos de la organización.

-Preparar y presentar la visión, las estrategias y las políticas de ciberseguridad para su aprobación por la alta dirección de la organización y garantizar su ejecución.

-Supervisar la aplicación y mejora del Sistema de Gestión de la Seguridad de la Información (SGSI).

-Informar a la alta dirección sobre los riesgos y amenazas para la ciberseguridad y su impacto en la organización.

-Garantizar que la alta dirección aprueba los riesgos de ciberseguridad de la organización.

-Desarrollar planes de ciberseguridad

-Desarrollar relaciones con las autoridades y comunidades relacionadas con la ciberseguridad

-Informar a la alta dirección de los incidentes, riesgos y conclusiones en materia de ciberseguridad.

-Supervisar los avances en ciberseguridad

-Conseguir recursos para aplicar la estrategia de ciberseguridad

-Negociar el presupuesto de ciberseguridad con la alta dirección.

-Garantizar la resistencia de la organización a los incidentes cibernéticos.

-Gestionar el desarrollo continuo de capacidades dentro de la organización

-Revisar, planificar y asignar los recursos de ciberseguridad adecuados.

Competencia(s) fundamental(es)

-Evaluar y mejorar la postura de ciberseguridad de una organización

-Analizar y aplicar políticas, certificaciones y normas de ciberseguridad, metodologías y marcos

-Analizar y cumplir las leyes, normativas y reglamentos relacionados con la ciberseguridad

-Aplicar recomendaciones y buenas prácticas de ciberseguridad

-Gestionar los recursos de ciberseguridad

-Desarrollar, defender y dirigir la ejecución de una estrategia de ciberseguridad

-Influir en la cultura de ciberseguridad de una organización

-Diseñar, aplicar, supervisar y revisar el Sistema de Gestión de la Seguridad de la Información (SGSI) ya sea directamente o dirigiendo su externalización

-Revisar y mejorar los documentos de seguridad, los informes y los acuerdos de nivel de servicio (SLA), y garantizar la consecución de los objetivos de seguridad.

-Identificar y resolver los problemas relacionados con la ciberseguridad

-Establecer un plan de ciberseguridad

-Comunicarse, coordinarse y cooperar con las partes interesadas internas y externas

-Anticipar los cambios necesarios en la estrategia de seguridad de la información de la organización y formular nuevos planes

-Definir y aplicar modelos de madurez para la gestión de la ciberseguridad

-Anticipar las amenazas a la ciberseguridad, las necesidades y los retos futuros

-Motivar y animar a las personas

Conocimiento(s) fundamental(es)

-Políticas de ciberseguridad

-Normas, metodologías y marcos de ciberseguridad

-Recomendaciones y buenas prácticas en materia de ciberseguridad

-Leyes, reglamentos y legislaciones relacionados con la ciberseguridad

-Certificaciones relacionadas con la ciberseguridad

-Requisitos éticos de organización en materia de ciberseguridad

-Modelos de madurez en ciberseguridad

-Procedimientos de ciberseguridad

-Gestión de recursos

-Prácticas de gestión

-Normas, metodologías y marcos de gestión de riesgos

e-competencias (de e-CF)

A.7. Vigilancia de la tendencia tecnológica	Nivel 4
D.1. Desarrollo de estrategia de seguridad de la información	Nivel 5
E.3. Gestión de riesgos	Nivel 4
E.8.Gestión de seguridad de la información	Nivel 4
E.9. Gobierno de los sistemas de información	Nivel 5

2.2. GESTOR DE INCIDENCIAS CIEBERNETICAS

Título(s) alternativo(s)

Gestor de incidentes cibernéticos

Experto en cibercrisis

Ingeniero de respuesta a incidentes

Analista del Centro de Operaciones de Seguridad (SOC)

Ciberdefensa

Analista de operaciones de seguridad (Analista SOC)

Responsable de SIEM de ciberseguridad

Resumen

Supervisar el estado de la ciberseguridad de la organización, gestionar los incidentes durante los ciberataques y garantizar el funcionamiento continuo de los sistemas TIC.

Misión

Supervisa y evalúa el estado de ciberseguridad de los sistemas. Analiza, evalúa y mitiga el impacto de los incidentes de ciberseguridad. Identifica las causas profundas de los incidentes cibernéticos y los actores maliciosos. De acuerdo con el Plan de Respuesta a Incidentes de la organización, restaura las funcionalidades de los sistemas y procesos a un estado operativo, recopilando pruebas y documentando las medidas adoptadas.

Producto(s) final(es)

- Plan de respuesta a incidentes

- Informe sobre incidentes cibernéticos

Tarea(s) principal(es)

- Contribuir al desarrollo, mantenimiento y evaluación del Plan de Respuesta a Incidentes.

- Desarrollar, aplicar y evaluar procedimientos relacionados con la gestión de incidentes

- Identificar, analizar, mitigar y comunicar incidentes de ciberseguridad

- Evaluar y gestionar las vulnerabilidades técnicas

- Medir la eficacia de la detección y respuesta a incidentes de ciberseguridad

- Evaluar la resistencia de los controles de ciberseguridad y las medidas de mitigación adoptadas tras un incidente de ciberseguridad o de violación de datos.

- Adoptar y desarrollar técnicas de prueba de gestión de incidentes

- Establecer procedimientos para el análisis de los resultados de los incidentes y la presentación de informes sobre su gestión

- Documentar el análisis de los resultados de los incidentes y las acciones de gestión de los mismos

- Cooperar con los Centros de Operaciones Seguras (SOC) y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT).

- Cooperar con el personal clave para la notificación de incidentes de seguridad con arreglo al marco jurídico aplicable.

Competencia(s) fundamental(es)

- Practicar todos los aspectos técnicos, funcionales y operativos de los incidentes de ciberseguridad de tratamiento y respuesta

- Recopilar, analizar y correlacionar información sobre ciberamenazas procedente de múltiples fuentes

- Trabajo en sistemas operativos, servidores, nubes e infraestructuras pertinentes

- Trabajar bajo presión

- Comunicar, presentar e informar a las partes interesadas

- Gestionar y analizar archivos de registro

Conocimiento(s) fundamental(es)

- Normas, metodologías y marcos de gestión de incidentes

- Recomendaciones y buenas prácticas para la gestión de incidentes

- Herramientas de gestión de incidentes

- Procedimientos de comunicación para la gestión de incidentes

- Seguridad de los sistemas operativos

- Seguridad de las redes informáticas

- Ciberamenazas

- Procedimientos de ataque a la ciberseguridad

- Vulnerabilidades de los sistemas informáticos

- Certificaciones relacionadas con la ciberseguridad

- Leyes, reglamentos y legislaciones relacionados con la ciberseguridad

- Funcionamiento de los Centros de Operaciones Seguros (SOC)

- Funcionamiento de los equipos de respuesta a incidentes de seguridad informática (CSIRT)

e-Competencias (de e-CF)

A.7. Vigilancia de las tendencias tecnológicas	Nivel 3
B.2. Integración de componentes	Nivel 2
B.3. Pruebas	Nivel 3
B.5. Producción de documentación	Nivel 3
C.4. Gestión de problemas	Nivel 4

2.3. RESPONSABLE JURÍDICO, POLÍTICO Y DE CUMPLIMIENTO DE LA CIBERSEGURIDAD

Título(s) alternativo(s)

Responsable de Protección de Datos (RPD)

Responsable de protección de datos

Consultor en Derecho Cibernético

Asesor jurídico cibernético

Responsable de Gobernanza de la Información

Responsable de cumplimiento de datos

Responsable jurídico de ciberseguridad

Responsable de Cumplimiento de TI/TIC

Consultor de Gobernanza, Riesgo y Cumplimiento (GRC)

Resumen

Gestiona el cumplimiento de las normas relacionadas con la ciberseguridad, legales y reglamentarias.

Marcos basados en la estrategia de la organización y los requisitos legales.

Misión

Supervisar y garantizar el cumplimiento de la legislación en materia de ciberseguridad y datos, marcos normativos y políticas acordes con la estrategia y la legislación de la organización.

Contribuye a las acciones de la organización relacionadas con la protección de datos.

Proporciona asesoramiento jurídico en el desarrollo de la gobernanza de ciberseguridad de la organización y las estrategias/soluciones de corrección recomendadas para garantizar el cumplimiento.

Entrega(s)

- Manual de cumplimiento

- Informe de conformidad

Tarea(s) principal(es)

- Garantizar el cumplimiento de las normas de protección de datos y proporcionar asesoramiento jurídico y orientación al respecto de normas, leyes y reglamentos sobre protección de datos

- Identificar y documentar las lagunas de cumplimiento

- Realizar evaluaciones de impacto sobre la privacidad y desarrollar, mantener, comunicar y formar sobre las políticas de privacidad, los procedimientos

- Aplicar y defender el programa de privacidad y protección de datos de la organización.

- Garantizar que los propietarios, titulares, responsables, encargados del tratamiento, sujetos, internos o se informe a los socios y entidades externas sobre sus derechos en materia de protección de datos, obligaciones y responsabilidades

- Actuar como punto de contacto clave para gestionar las consultas y reclamaciones relativas al procesamiento datos.

- Asistir en el diseño, la aplicación, la auditoría y las actividades de comprobación de la conformidad para garantizar el cumplimiento de las normas de ciberseguridad y privacidad

- Supervisar las auditorías y las actividades de formación relacionadas con la protección de datos

- Cooperar y compartir información con autoridades y grupos profesionales

- Contribuir al desarrollo de la estrategia y la política de ciberseguridad de la organización y procedimientos

- Desarrollar y proponer formación de concienciación del personal para lograr el cumplimiento y fomentar una cultura de protección de datos en la organización

- Gestionar los aspectos jurídicos de las responsabilidades de seguridad de la información y las relaciones con terceros.

Competencia(s) fundamental(es)

- Conocimiento exhaus tivo de la estrategia empresarial, los modelos y los productos y capacidad para tener en cuenta los requisitos legales, reglamentarios y normativos

- Llevar a cabo prácticas de la vida laboral de las cuestiones de protección de datos y privacidad implicadas en la aplicación de los procesos organizativos, las finanzas y la estrategia empresarial

- Dirigir el desarrollo de políticas adecuadas de ciberseguridad y privacidad y procedimientos que complementen las necesidades de la empresa y los requisitos legales; además garantizar su aceptación, comprensión y aplicación, y comunicarla entre las partes implicadas

- Realizar, supervisar y revisar las evaluaciones de impacto sobre la privacidad utilizando normas, marcos, metodologías y herramientas reconocidas

- Explicar y comunicar temas de protección de datos y privacidad a las partes interesadas y usuarios

- Comprender, practicar y cumplir las exigencias y normas éticas.

- Comprender las implicaciones de las modificaciones del marco jurídico para la organización de estrategias y políticas de ciberseguridad y protección de datos

- Colaborar con otros miembros del equipo y colegas

Conocimiento(s) fundamental(es)

- Normas, metodologías y marcos de ciberseguridad

- Políticas de ciberseguridad

- Requisitos legales, reglamentarios y de cumplimiento de la legislación, recomendaciones y mejores prácticas.

- Normas, metodologías y marcos de evaluación del impacto sobre la intimidad

e-competencias (de e-CF)

A.1. Alineación de los sistemas de información y la estrategia empresarial	Nivel 4
D.1. Desarrollo de la estrategia de seguridad de la información	Nivel 4
E.8.	Nivel 3
E.9.SI-Gobernanza	Nivel 4

2.4. ESPECIALISTA EN INTELIGENCIA SOBRE CIBERAMENAZAS

Título(s) alternativo(s)

Analista de ciberinteligencia

Modelador de ciberamenazas

Declaración sumaria

Recopilar, procesar y analizar datos e información para elaborar informes de inteligencia procesables y difundirlos a las partes interesadas.

Misión

Gestiona el ciclo de vida de la inteligencia sobre ciberamenazas, incluida la información sobre ciberamenazas, recopilación, análisis y producción de información útil y su difusión a los ciudadanos. Así como, la seguridad y la comunidad CTI, a nivel táctico, operativo y estratégico. Identifica y supervisa las Tácticas, Técnicas y Procedimientos (TTP) utilizados por los actores de las ciberamenazas y sus tendencias, rastrear las actividades de los actores de las amenazas y observar cómo los acontecimientos no cibernéticos pueden influir en las acciones relacionadas con la cibernética.

Producto(s) final(es)

- Manual de inteligencia sobre ciberamenazas

- Informe sobre ciberamenazas

Tarea(s) principal(es)

- Desarrollar, aplicar y gestionar la información sobre ciberamenazas de la estrategia organización.

- Desarrollar planes y procedimientos para gestionar la información sobre amenazas

- Traducir los requisitos empresariales en requisitos de inteligencia

- Implementar la recopilación, el análisis y la producción de inteligencia sobre amenazas.

inteligencia y difusión a las partes interesadas en la seguridad

- Identificar y evaluar las ciberamenazas dirigidas a la organización

- Identificar, supervisar y evaluar las Tácticas, Técnicas y Procedimientos (TTP) utilizados en las ciberamenazas mediante el análisis de datos de fuentes públicas y privadas, información e inteligencia

- Elaborar informes procesables basados en datos de inteligencia sobre amenazas

- Elaborar y asesorar sobre planes de mitigación a nivel táctico, operativo y estratégico.

- Coordinarse con las partes interesadas para compartir y consumir información sobre ciberamenazas relevantes.

- Aprovechar los datos de inteligencia para apoyar y ayudar en la elaboración de modelos de amenazas, recomendaciones para la mitigación de riesgos y la caza de ciberamenazas

- Articular y comunicar la inteligencia abierta y públicamente a todos los niveles.

- Transmitir la gravedad de seguridad adecuada explicando la exposición al riesgo y sus consecuencias para las partes interesadas no técnicas

Competencia(s) fundamental(es)

- Colaborar con otros miembros del equipo y colegas

- Recopilar, analizar y correlacionar información sobre ciberamenazas procedente de múltiples fuentes

- Identificar las TTP y las campañas de los actores de la amenaza

- Automatizar los procedimientos de gestión de la información sobre amenazas

- Realizar análisis técnicos e informes

- Identificar los acontecimientos no cibernéticos con implicaciones en las actividades relacionadas con la cibernética.

- Modelo de amenazas, actores y TTP

- Comunicarse, coordinarse y cooperar con las partes interesadas internas y externas

- Comunicar, presentar e informar a las partes interesadas

- Utilizar y aplicar plataformas y herramientas CTI

Conocimiento(s) fundamental(es)

- Seguridad de los sistemas operativos

- Seguridad de las redes informáticas

- Controles y soluciones de ciberseguridad

- Programación informática

- Normas, metodologías y marcos de intercambio de información sobre ciberamenazas (CTI)

- Procedimientos responsables de divulgación de la información

- Conocimientos interdisciplinarios y transfronterizos relacionados con la ciberseguridad

- Ciberamenazas

- Actores de ciberamenazas

- Procedimientos de ataque a la ciberseguridad

- Ciberamenazas avanzadas y persistentes (APT)

- Tácticas, técnicas y procedimientos (TTP) de los actores de la amenaza

- Certificaciones relacionadas con la ciberseguridad

e-competencias (de e-CF)

B.5. Producción de documentación	Nivel 3
D.7. Ciencia y análisis de datos	Nivel 4
D.10. Gestión de la información y el conocimiento	Nivel 4
E.4. Gestión de las relaciones	Nivel 3
E.8. Gestión de la seguridad de la información	Nivel 4

2.5. ARQUITECTO DE CIBERSEGURIDAD

Título(s) alternativo(s)

Arquitecto de soluciones de ciberseguridad

Diseñador de ciberseguridad

Arquitecto de seguridad de datos

Resumen

Planifica y diseña soluciones de seguridad por diseño (infraestructuras, sistemas, activos, software, hardware y servicios) y controles de ciberseguridad.

Misión

Diseña soluciones basadas en los principios de seguridad por diseño y privacidad por diseño.

Crea y mejora continuamente modelos arquitectónicos y desarrolla documentación y especificaciones arquitectónicas. Coordinar el desarrollo seguro, integración y mantenimiento de los componentes de ciberseguridad conforme a las normas y otros requisitos conexos.

Producto(s) final(es)

- Diagrama de arquitectura de ciberseguridad

- Informe sobre requisitos de ciberseguridad

Tarea(s) principal(es)

- Diseñar y proponer una arquitectura segura para aplicar la estrategia de la organización.

- Desarrollar la arquitectura de ciberseguridad de la organización para abordar la seguridad y la privacidad.

- Elaborar documentación y especificaciones arquitectónicas

- Presentar el diseño de la arquitectura de seguridad de alto nivel a las partes interesadas

- Establecer un entorno seguro durante el ciclo de vida de desarrollo de los sistemas, servicios y productos

- Coordinar el desarrollo, la integración y el mantenimiento de la ciberseguridad.

componentes que garantizan las especificaciones de ciberseguridad

- Analizar y evaluar la ciberseguridad de la arquitectura de la organización.

- Garantizar la seguridad de las arquitecturas de las soluciones mediante revisiones de seguridad y certificación

- Colaborar con otros equipos y colegas

- Evaluar el impacto de las soluciones de ciberseguridad en el diseño y el rendimiento de la arquitectura de la organización

- Adaptar la arquitectura de la organización a las amenazas emergentes

- Evaluar la arquitectura implantada para mantener un nivel de seguridad adecuado.

Competencia(s) fundamental(es)

- Realizar análisis de los requisitos de seguridad de usuarios y empresas

- Elaborar especificaciones arquitectónicas y funcionales de ciberseguridad

- Descomponer y analizar sistemas para desarrollar requisitos de seguridad y privacidad e identificar soluciones eficaces

- Diseñar sistemas y arquitecturas basados en la seguridad y la privacidad por diseño y por principios de ciberseguridad por defecto

- Orientar y comunicarse con los responsables de la aplicación y el personal de TI/OT.

- Comunicar, presentar e informar a las partes interesadas

- Proponer arquitecturas de ciberseguridad basadas en las necesidades y el presupuesto de las partes interesadas.

- Seleccionar especificaciones, procedimientos y controles adecuados

- Aumentar la resistencia frente a puntos de fallo en toda la arquitectura

- Coordinar la integración de soluciones de seguridad

Conocimiento(s) fundamental(es) - Certificaciones relacionadas con la ciberseguridad

- Recomendaciones y buenas prácticas en materia de ciberseguridad

- Normas, metodologías y marcos de ciberseguridad

- Análisis de requisitos relacionados con la ciberseguridad

- Ciclo de desarrollo seguro

- Modelos de referencia de arquitectura de seguridad

- Tecnologías relacionadas con la ciberseguridad

- Controles y soluciones de ciberseguridad

- Riesgos de ciberseguridad

- Ciberamenazas

- Tendencias en ciberseguridad

- Requisitos legales, reglamentarios y de cumplimiento legislativo, recomendaciones y buenas prácticas

- Procedimientos de ciberseguridad heredados

- Tecnologías de protección de la intimidad (PET)

-Normas, metodologías y marcos de protección de la intimidad mediante el diseño

e-competencias

A.5. Diseño arquitectónico	Nivel 5
A.6. Diseño de aplicaciones	Nivel 3
B.1. Desarrollo de aplicaciones	Nivel 3
B.3. Pruebas	Nivel 3
B.6. Ingeniería de sistemas TIC	Nivel 4

2.6. AUDITOR DE CIBERSEGURIDAD

Título(s) alternativo(s)

Auditor de seguridad de la información (auditor informático o jurídico)

Auditor de Gobernanza, Riesgo y Cumplimiento (GRC)

Director de Auditoría de Ciberseguridad

Auditor de procedimientos y procesos de ciberseguridad

Auditor de Riesgos de Seguridad de la Información y Cumplimiento Normativo

Analista de evaluación de protección de datos

Resumen

Realizar auditorías de ciberseguridad en el ecosistema de la organización. Garantizar el cumplimiento con información estatutaria, reglamentaria, política, requisitos de seguridad, normas del sector y las mejores prácticas.

Misión

Realiza revisiones independientes para evaluar la eficacia de los procesos y controles y el cumplimiento general de los marcos jurídicos y reglamentarios de la organización.

Evalúa, prueba y verifica los productos relacionados con la ciberseguridad (sistemas, hardware, software y servicios), funciones y políticas que garanticen, el cumplimiento de directrices, normas y reglamentos.

Entrega(s)

- Plan de auditoría de ciberseguridad

- Informe de auditoría de ciberseguridad

Tarea(s) principal(es)

- Desarrollar la política, los procedimientos, las normas y las directrices de auditoría de la organización.

- Establecer las metodologías y prácticas utilizadas para la auditoría de sistemas.

- Establecer el entorno objetivo y gestionar las actividades de auditoría

- Definir el alcance, los objetivos y los criterios de la auditoría

- Elaborar un plan de auditoría que describa los marcos, las normas y la metodología, procedimientos y pruebas de auditoría

- Revisar el objetivo de la evaluación, los objetivos de seguridad y los requisitos en función del riesgo del perfil.

- Auditoría del cumplimiento de las leyes y reglamentos aplicables en materia de ciberseguridad.

- Auditoría de conformidad con las normas aplicables en materia de ciberseguridad.

- Ejecutar el plan de auditoría y recopilar pruebas y mediciones.

- Mantener y proteger la integridad de los registros de auditoría.

- Desarrollar y comunicar la evaluación de la conformidad, la garantía, la auditoría, la certificación e informes de mantenimiento.

- Supervisar las actividades de corrección de riesgos.

Capacidad(es) clave(s)

- Organizar y trabajar de forma sistemática y determinista basándose en pruebas

- Seguir y practicar marcos, normas y metodologías de auditoría.

- Aplicar herramientas y técnicas de auditoría

- Analizar los procesos empresariales, evaluar y revisar la seguridad del software o hardware, así como controles técnicos y organizativos

- Descomponer y analizar los sistemas para detectar puntos débiles y controles ineficaces.

- Comunicar, explicar y adaptar los requisitos legales y reglamentarios y las necesidades de la empresa.

- Recopilar, evaluar, mantener y proteger la información de auditoría

- Auditar con integridad, imparcialidad e independencia

Conocimiento(s) fundamental(es)

- Controles y soluciones de ciberseguridad

- Requisitos legales, reglamentarios y de cumplimiento legislativo, recomendaciones y buenas prácticas

- Supervisión, comprobación y evaluación de la eficacia de los controles de ciberseguridad

- Normas, metodologías y marcos de evaluación de la conformidad

- Normas, metodologías y marcos de auditoría

- Normas, metodologías y marcos de ciberseguridad

- Certificación relacionada con la auditoría

- Certificaciones relacionadas con la ciberseguridad

e-Competencias (de e-CF)

B.3. Pruebas	Nivel 4
B.5. Producción de documentación	Nivel 3
E.3. E.3. Gestión de riesgos	Nivel 4
E.6 Gestión de la calidad de las TIC	Nivel 4
E.8. Gestión de la seguridad de la información	Nivel 4

2.7. EDUCADOR EN CIBERSEGURIDAD

Título(s) alternativo(s)

Especialista en ciberseguridad

Formador en ciberseguridad

Profesorado en Ciberseguridad (Catedrático, Conferenciante)

Resumen

Mejora los conocimientos, habilidades y competencias de los seres humanos en materia de ciberseguridad.

Misión

Diseña, desarrolla y lleva a cabo programas de sensibilización, formación y educación en temas relacionados con la ciberseguridad y la protección de datos. Utiliza métodos didácticos y métodos, técnicas e instrumentos de formación para comunicar y mejorar la cultura de ciberseguridad, capacidades, conocimientos y aptitudes de los recursos humanos.

Promueve la importancia de la ciberseguridad y la consolida en la organización.

Producto(s) final(es)

- Programa de concienciación sobre ciberseguridad

- Material de formación sobre ciberseguridad

Tarea(s) principal(es)

- Elaborar, actualizar e impartir planes de estudios sobre ciberseguridad y protección de datos y material educativo de formación y sensibilización basado en contenidos, métodos y herramientas, de las necesidades de los alumnos

- Organizar, diseñar e impartir actividades, seminarios, cursos, formación práctica de sensibilización sobre ciberseguridad y protección de datos.

- Supervisar, evaluar e informar sobre la eficacia de la formación

- Evaluar e informar sobre el rendimiento de los becarios

- Encontrar nuevos enfoques de educación, formación y sensibilización

- Diseñar, desarrollar e impartir simulaciones de ciberseguridad, laboratorios virtuales o ciberespacios.

- Orientar sobre programas de certificación de ciberseguridad para particulares

- Mantener y mejorar continuamente los conocimientos especializados; fomentar y potenciar la formación continua.

- Mejora de las capacidades de ciberseguridad y creación de capacidades

Competencia(s) fundamental(es)

- Determinar las necesidades en materia de sensibilización, formación y educación sobre ciberseguridad

- Diseñar, desarrollar e impartir programas de aprendizaje para cubrir las necesidades de ciberseguridad.

- Desarrollar ejercicios de ciberseguridad que incluyan simulaciones con ciberescala

- Impartir formación para la obtención de certificaciones profesionales en ciberseguridad y protección de datos.

- Utilizar los recursos de formación existentes en materia de ciberseguridad

- Desarrollar programas de evaluación de las actividades de sensibilización, formación y educación.

- Comunicar, presentar e informar a las partes interesadas

- Identificar y seleccionar los enfoques pedagógicos apropiados para el público destinatario.

- Motivar y animar a la gente

Conocimiento(s) fundamental(es) - Normas, metodologías y marcos pedagógicos

- Desarrollo de programas de sensibilización, educación y formación en ciberseguridad

- Certificaciones relacionadas con la ciberseguridad

- Normas, metodologías y marcos de educación y formación en ciberseguridad

- Leyes, normativas y legislaciones relacionadas con la ciberseguridad

- Recomendaciones y buenas prácticas en materia de ciberseguridad

- Normas, metodologías y marcos de ciberseguridad

- Controles y soluciones de ciberseguridad

e-Competencias (de e-CF)

D.3. Educación y formación	Nivel 3
D.9. Desarrollo del personal	Nivel 3
E.8. Gestión de la seguridad de la información	Nivel 3

2.8. IMPLEMENTADOR DE CIBERSEGURIDAD

Título(s) alternativo(s)

Implementador de seguridad de la información

Experto en soluciones de ciberseguridad

Desarrollador de ciberseguridad Ingeniero de ciberseguridad

Ingeniero de desarrollo, seguridad y operaciones (DevSecOps)

Resumen

Desarrollar, desplegar y explotar soluciones de ciberseguridad (sistemas, activos, software, controles y servicios) en infraestructuras y productos.

Misión

Proporciona desarrollo técnico relacionado con la ciberseguridad, integración, pruebas, aplicación, funcionamiento, mantenimiento, supervisión y apoyo de soluciones de ciberseguridad. Garantiza el cumplimiento de las especificaciones y los requisitos de conformidad, asegura un rendimiento sólido y resuelve los problemas técnicos necesarios en las soluciones relacionadas con la ciberseguridad de la organización (sistemas, activos, software, controles y servicios), las infraestructuras y los productos.

Producto(s)

- Soluciones de ciberseguridad

Tarea(s) principal(es)

- Desarrollar, implantar, mantener, actualizar y probar productos de ciberseguridad.

- Proporcionar apoyo relacionado con la ciberseguridad a usuarios y clientes

- Integrar las soluciones de ciberseguridad y garantizar su buen funcionamiento

- Configurar de forma segura sistemas, servicios y productos

- Mantener y mejorar la seguridad de los sistemas, servicios y productos

- Implantar procedimientos y controles de ciberseguridad

- Supervisar y garantizar el funcionamiento de los controles de ciberseguridad implantados.

- Documentar e informar sobre la seguridad de los sistemas, servicios y productos.

- Colaborar estrechamente con el personal de TI/OT en las acciones relacionadas con la ciberseguridad.

- Implantar, aplicar y gestionar parches en los productos para solucionar vulnerabilidades técnicas.

Competencia(s) fundamental(es)

- Comunicar, presentar e informar a las partes interesadas

- Integrar las soluciones de ciberseguridad en la infraestructura de la organización

- Configurar las soluciones de acuerdo con la política de seguridad de la organización.

- Evaluar la seguridad y el rendimiento de las soluciones

- Desarrollar código, scripts y programas

- Identificar y resolver problemas relacionados con la ciberseguridad

- Colaborar con otros miembros del equipo y colegas

Conocimiento(s) fundamental(es)

- Ciclo de vida del desarrollo seguro

- Programación informática

- Seguridad de los sistemas operativos

- Seguridad de las redes informáticas

- Controles y soluciones de ciberseguridad

- Prácticas de seguridad ofensivas y defensivas

- Recomendaciones y mejores prácticas de codificación segura

- Recomendaciones y buenas prácticas en materia de ciberseguridad

- Normas, metodologías y marcos de pruebas

- Procedimientos de ensayo

- Tecnologías relacionadas con la ciberseguridad

e-competencias (de e-CF)

A.5.	Nivel 3
A.6.	Nivel 3
B.1. Desarrollo de aplicaciones	Nivel 3
B.3. Pruebas	Nivel 3
B.6. Ingeniería de sistemas TIC	Nivel 4

2.9. INVESTIGADOR EN CIBERSEGURIDAD

Título(s) alternativo(s)

Ingeniero de investigación en ciberseguridad

Director de Investigación (CRO) en ciberseguridad

Director de Investigación en ciberseguridad

Oficial de Investigación y Desarrollo (I+D) en ciberseguridad

Personal científico en ciberseguridad

Responsable de investigación e innovación/Experto en ciberseguridad

Becario de investigación en ciberseguridad

Resumen

Investigar el ámbito de la ciberseguridad e incorporar los resultados a las soluciones de ciberseguridad.

Misión

Realiza investigación fundamental/básica y aplicada y facilita la innovación en el ámbito de la ciberseguridad mediante la cooperación con otras partes interesadas. Analiza las tendencias y los descubrimientos científicos en ciberseguridad.

Producto(s)

- Publicación en Ciberseguridad

Tarea(s) principal(es)

- Analizar y evaluar tecnologías, soluciones, desarrollos y procesos de ciberseguridad.

- Realizar trabajos de investigación, innovación y desarrollo en temas relacionados con la ciberseguridad- Manifestar y generar ideas de investigación e innovación

- Avanzar en el estado actual de los temas relacionados con la ciberseguridad.

- Colaborar en el desarrollo de soluciones innovadoras relacionadas con la ciberseguridad.

- Realizar experimentos y desarrollar pruebas de concepto, pilotos y prototipos de soluciones de ciberseguridad.

- Seleccionar y aplicar marcos, métodos, normas, herramientas y protocolos, incluida la creación y comprobación de una prueba de concepto para apoyar los proyectos.

- Contribuir a ideas, servicios y soluciones empresariales de ciberseguridad de vanguardia.

- Ayudar en la creación de capacidades relacionadas con la ciberseguridad, incluida la concienciación, la formación teórica, la formación práctica, las pruebas, la tutoría, la supervisión y el intercambio.

- Identificar logros intersectoriales en materia de ciberseguridad y aplicarlos en un contexto diferente o proponer enfoques y soluciones innovadores.

- Dirigir o participar en los procesos y proyectos de innovación, incluida la gestión de proyectos y la elaboración de presupuestos.

- Publicar y presentar trabajos científicos y resultados de investigación y desarrollo

Competencia(s) fundamental(es)

- Generar nuevas ideas y trasladar la teoría a la práctica

- Descomponer y analizar los sistemas para identificar los puntos débiles y los controles ineficaces.

- Descomponer y analizar sistemas para desarrollar requisitos de seguridad y privacidad e identificar soluciones eficaces.

-Seguimiento de los nuevos avances en tecnologías relacionadas con la ciberseguridad.

- Comunicar, presentar e informar a las partes interesadas

- Identificar y resolver problemas relacionados con la ciberseguridad

- Colaborar con otros miembros del equipo y colegas

Conocimiento(s) fundamental(es)

- Investigación, desarrollo e innovación (I+D+i) relacionados con la ciberseguridad

- Normas, metodologías y marcos de ciberseguridad

-Requisitos legales, reglamentarios y legislativos sobre la liberación o el uso de tecnologías relacionadas con la ciberseguridad.

- Aspecto multidisciplinar de la ciberseguridad

- Procedimientos responsables de divulgación de la información

e-competencias (de e-CF)

A.7. Vigilancia de las tendencias tecnológicas	Nivel 5
A.9. Innovar	Nivel 5
D.7. Ciencia y análisis de datos	Nivel 4
C.4. Gestión de problemas	Nivel 3
D.10. Gestión de la información y el conocimiento	Nivel 3

2.10. GESTOR DE RIESGOS DE CIBERSEGURIDAD

Título(s) alternativo(s)

Analista de riesgos de seguridad de la información

Consultor de garantía de riesgos de ciberseguridad

Evaluador de riesgos de ciberseguridad

Analista del impacto de la ciberseguridad

Responsable de Ciberriesgos

Resumen

Gestionar los riesgos relacionados con la ciberseguridad de la organización en consonancia con los objetivos de la organización.

Desarrollar, mantener y comunicar los procesos de gestión de riesgos e informes.

Misión

Gestiona continuamente (identifica, analiza, evalúa, estima, mitiga) los riesgos relacionados con la ciberseguridad de las infraestructuras, sistemas y servicios de TIC mediante la planificación, aplicar, informar y comunicar el análisis, la evaluación y el tratamiento de los riesgos.

Establece una estrategia de gestión de riesgos para la organización y garantiza que los riesgos permanecer en un nivel aceptable para la organización mediante la selección de acciones de mitigación y controles.

Producto(s) final(es)

- Informe de evaluación de riesgos de ciberseguridad

- Plan de acción para remediar los riesgos de ciberseguridad

Tarea(s) principal(es)

- Desarrollar la estrategia de gestión de riesgos de ciberseguridad de una organización

- Gestionar un inventario de los activos de la organización

- Identificar y evaluar las amenazas y vulnerabilidades de los sistemas TIC relacionadas con la ciberseguridad.

- Identificación del panorama de amenazas, incluidos los perfiles de los atacantes y la estimación de potenciales ataques

- Evaluar los riesgos de ciberseguridad y proponer las opciones de tratamiento de riesgos más adecuadas, incluidos los controles de seguridad y la mitigación y evitación de riesgos que mejor aborden la estrategia de la organización.

- Supervisar la eficacia de los controles de ciberseguridad y los niveles de riesgo.

- Garantizar que todos los riesgos de ciberseguridad se mantienen en un nivel aceptable para los activos de la organización.

- Desarrollar, mantener, informar y comunicar el ciclo completo de gestión de riesgos

Competencia(s) fundamental(es)

- Implantar marcos, metodologías y sistemas de gestión de riesgos de ciberseguridad y garantizar el cumplimiento de los reglamentos y normas

- Analizar y consolidar las prácticas de gestión de la calidad y los riesgos de la organización.

- Permitir a los propietarios de activos empresariales, ejecutivos y otras partes interesadas tomar decisiones informadas sobre riesgos para gestionar y mitigar los riesgos.

- Crear un entorno de ciberseguridad consciente de los riesgos

- Comunicar, presentar e informar a las partes interesadas

- Proponer y gestionar opciones de riesgo compartido

Conocimiento(s) fundamental(es)

- Normas, metodologías y marcos de gestión de riesgos

- Herramientas de gestión de riesgos

- Recomendaciones y buenas prácticas para la gestión de riesgos

- Ciberamenazas

- Vulnerabilidades de los sistemas informáticos

- Controles y soluciones de ciberseguridad

- Riesgos de ciberseguridad

- Supervisión, comprobación y evaluación de la eficacia de los controles de ciberseguridad

- Certificaciones relacionadas con la ciberseguridad

- Tecnologías relacionadas con la ciberseguridad

e-Competencias(de e-CF)

E.3. Gestión de riesgos	Nivel 4
E.5. Mejora de los procesos	Nivel 3
E.7. Gestión del cambio empresarial	Nivel 4
E.9. SI-Gobernanza	Nivel 4

2.11. INVESTIGADOR FORENSE DIGITAL

Título(s) alternativo(s)

Analista forense digital

Especialista en ciberseguridad y análisis forense

Consultor informático forense

Resumen

Asegúrese de que la investigación del ciberdelincuente revele todas las pruebas digitales que demuestren la actividad maliciosa.

Misión

Conecta artefactos con personas físicas, capta, recupera, identifica y conservar los datos, incluidas las manifestaciones, entradas, salidas y procesos de los sistemas digitales bajo investigación.

Proporciona análisis, reconstrucción e interpretación de las pruebas basadas en una opinión cualitativa.

Presenta una opinión cualitativa imparcial sin interpretar los resultados obtenidos.

Producto(s) final(es)

- Resultados del análisis forense digital

- Pruebas electrónicas

Tarea(s) principal(es)

- Desarrollar políticas, planes y procedimientos de investigación forense digital

- Identificar, recuperar, extraer, documentar y analizar pruebas digitales

- Preservar y proteger las pruebas digitales y ponerlas a disposición de las personas autorizadas.

- Inspeccionar los entornos en busca de pruebas de acciones no autorizadas e ilegales

- Documentación, elaboración de informes y presentación de informes forenses digitales de forma sistemática y determinista.

- Seleccionar y personalizar las técnicas de prueba, análisis y elaboración de informes forenses.

Competencia(s) fundamental(es)

- Trabajar de forma ética e independiente, sin influencias ni prejuicios internos o externos.
- Recopilar información preservando su integridad
- Identificar, analizar y correlacionar eventos de ciberseguridad
- Explicar y presentar las pruebas digitales de forma sencilla, directa y fácil de entender la forma
- Elaborar y comunicar informes de investigación detallados y razonados.

Conocimiento(s) fundamental(es)

- Recomendaciones y buenas prácticas en materia de análisis forense digital
- Normas, metodologías y marcos forenses digitales
- Procedimientos de análisis forense digital
- Procedimientos de ensayo
- Procedimientos, normas, metodologías y marcos de investigación criminal
- Leyes, reglamentos y legislaciones relacionados con la ciberseguridad
- Herramientas de análisis de malware
- Ciberamenazas
- Vulnerabilidades de los sistemas informáticos
- Procedimientos de ataque a la ciberseguridad
- Seguridad de los sistemas operativos
- Seguridad de las redes informáticas
- Certificaciones relacionadas con la ciberseguridad

e-Competencias (de e-CF)

A.7. Vigilancia de las tendencias tecnológicas	Nivel 3
B.3. Pruebas	Nivel 4
B.5. Producción de documentación	Nivel 3
E.3. Gestión de riesgos	Nivel 3

2.12. EXAMEN DE PENETRACIÓN

Título(s) alternativo(s)

Pentester

Hacker ético

Analista de vulnerabilidades

Comprobador de ciberseguridad

Experto en ciberseguridad ofensiva

Experto en ciberseguridad defensiva

Experto del Equipo Rojo

Equipo Rojo

Resumen

Evaluar la eficacia de los controles de seguridad, revelar y utilizar las vulnerabilidades de ciberseguridad, evaluando su criticidad si son explotadas por actores de amenazas.

Misión

Planifica, diseña, implementa y ejecuta actividades de pruebas de penetración y ataque para evaluar la eficacia de las medidas de seguridad desplegadas o previstas.

Identifica vulnerabilidades o fallos en los controles técnicos y organizativos que afectan a la confidencialidad, integridad y disponibilidad de los productos TIC (por ejemplo, sistemas, hardware, software y servicios).

Producto(s) final(es)

- Informe de resultados de la evaluación de la vulnerabilidad

- Informe de pruebas de penetración

Tarea(s) principal(es)

- Identificar, analizar y evaluar las vulnerabilidades de ciberseguridad técnica y organizativa.

- Identificar vectores de ataque, descubrir y demostrar la explotación de técnicas de vulnerabilidad de ciberseguridad

- Pruebas de conformidad de los sistemas y operaciones con las normas reglamentarias

- Seleccionar y desarrollar técnicas adecuadas de pruebas de penetración
- Organizar planes de pruebas y procedimientos para pruebas de penetración
- Establecer procedimientos para el análisis de los resultados de las pruebas de penetración y la elaboración de informes al respecto.
- Documentar e informar de los resultados de las pruebas de penetración a las partes interesadas
- Despliegue de herramientas y programas de pruebas de penetración

Competencia(s) fundamental(es)

- Desarrollar códigos, guiones y programas
- Realizar ingeniería social
- Identificar y explotar vulnerabilidades
- Realizar hacking ético
- Pensar de forma creativa y original
- Identificar y resolver problemas relacionados con la ciberseguridad
- Comunicar, presentar e informar a las partes interesadas
- Utilizar eficazmente las herramientas de pruebas de penetración
- Realizar análisis técnicos e informes
- Descomponer y analizar los sistemas para detectar puntos débiles y controles ineficaces.
- Los códigos de revisión evalúan su seguridad

Conocimiento(s) fundamental(es)

- Procedimientos de ataque a la ciberseguridad
- Aparatos de tecnología de la información (TI) y tecnología operativa (TO)
- Procedimientos de seguridad ofensivos y defensivos
- Seguridad de los sistemas operativos
- Seguridad de las redes informáticas
- Procedimientos de pruebas de penetración
- Normas, metodologías y marcos de pruebas de penetración
- Herramientas de pruebas de penetración
- Programación informática
- Vulnerabilidades de los sistemas informáticos

- Recomendaciones y buenas prácticas en materia de ciberseguridad
- Certificaciones relacionadas con la ciberseguridad

e-Competencias (de e-CF)

B.2. Integración de componentes	Nivel 4
B.3. Pruebas	Nivel 4
B.4. Despliegue de la solución	Nivel 2
B.5. Producción de documentación	Nivel 3
E.3. Gestión de riesgos	Nivel 4

3. BIBLIOTECA DE ENTREGABLES

La lista de entregables ofrece algunos ejemplos indicativos y prácticos de los entregables/resultados de cada perfil de funciones. La lista no es exhaustiva, por lo que no cubre todos los aspectos de cada perfil. El texto sigue el siguiente orden:Título del perfil, Entregable y Descripción

Director de Seguridad de la Información (CISO)

Estrategia de ciberseguridad

La estrategia de ciberseguridad es un plan de acciones diseñado para mejorar la seguridad y resistencia de las infraestructuras y servicios de una organización.

Director de Seguridad de la Información (CISO)

Política de ciberseguridad

Una política que enumera las normas para garantizar la ciberseguridad de la organización.

Respuesta a incidentes cibernéticos

Plan de Respuesta a Incidentes

Conjunto de procedimientos documentados que detallan los pasos que deben darse en cada fase de la respuesta a un incidente (Preparación, Detección y Análisis, Contención, Erradicación y Recuperación, Actividad Post-Incidente).

Respondedor de ciberincidentes

Informe de ciberincidente

Informe que proporciona detalles sobre uno o más ciberincidentes.

Responsable de Ciberseguridad, Política y Cumplimiento Normativo

Manual de cumplimiento

Un manual que proporciona un conocimiento exhaustivo de las obligaciones de cumplimiento normativo de una organización. Puede incluir políticas o procedimientos internos para garantizar el cumplimiento de las leyes, reglamentos y/o normas.

Responsable de Ciberseguridad, Política y Cumplimiento

Informe de cumplimiento

Informe que presenta el estado actual de la postura de cumplimiento de una organización.

Especialista en inteligencia sobre ciberamenazas

Manual (o manual) de inteligencia sobre ciberamenazas

Manual que presenta herramientas y/o metodologías para recopilar y/o compartir inteligencia sobre ciberamenazas.

Especialista en Inteligencia sobre Ciberamenazas

Informe sobre ciberamenazas

Informe en el que se identifican las principales amenazas, las principales tendencias observadas con respecto a las amenazas, los actores de las amenazas y/o las técnicas de ataque. El informe también puede incluir las medidas de mitigación pertinentes.

Arquitecto de ciberseguridad

Diagrama de arquitectura de ciberseguridad

Representación visual de la arquitectura de sistemas de ciberseguridad de una organización utilizada para proteger los activos frente a ciberataques.

Arquitecto de ciberseguridad

Informe de requisitos de ciberseguridad

Informe que enumera un conjunto de requisitos necesarios para garantizar la ciberseguridad de un sistema.

Auditor de ciberseguridad

Plan de auditoría de ciberseguridad

Un plan que presenta la estrategia general y los procedimientos que seguirá un auditor para llevar a cabo una auditoría de ciberseguridad.

Auditor de ciberseguridad

Informe de auditoría de ciberseguridad

Informe que proporciona un conocimiento exhaustivo del nivel de seguridad de un sistema, evaluando sus puntos fuertes y débiles en materia de ciberseguridad. También puede proporcionar medidas correctoras para mejorar la ciberseguridad general del sistema.

Educador en ciberseguridad

Programa de concienciación sobre ciberseguridad

Programa de actividades de concienciación sobre temas relacionados con la ciberseguridad (por ejemplo, conferencias sobre ataques y amenazas) que ayuda a las organizaciones a prevenir y mitigar los riesgos relacionados con la ciberseguridad.

Educador en ciberseguridad

Material de formación sobre ciberseguridad

Material que explica conceptos, metodologías y herramientas relacionados con la ciberseguridad para la formación o el perfeccionamiento de las personas. Puede incluir manuales para profesores, conjuntos de herramientas para estudiantes y/o imágenes virtuales para apoyar las sesiones de formación práctica.

Implementador de ciberseguridad

Soluciones de ciberseguridad

Las soluciones de ciberseguridad pueden incluir herramientas y servicios destinados a proteger a las organizaciones contra los ciberataques.

Investigador en ciberseguridad

Publicación en ciberseguridad

Publicación académica que da a conocer los hallazgos y resultados de la investigación en el contexto de la ciberseguridad. El objetivo de la publicación puede ser el avance de la tecnología y/o el desarrollo de nuevas soluciones innovadoras.

Gestor de riesgos de ciberseguridad

Informe de evaluación de riesgos de ciberseguridad

Informe que enumera los resultados de la identificación, el análisis y la evaluación de los riesgos de ciberseguridad de un sistema. También puede incluir controles para mitigar o reducir los riesgos identificados a un nivel aceptable.

Gestor de riesgos de ciberseguridad

Plan de Acción de Remediación de Riesgos de Ciberseguridad

Un plan de acción que enumera las actividades relacionadas con la aplicación de medidas de mitigación destinadas a reducir los riesgos de ciberseguridad.

Investigador forense digital

Resultados del análisis forense digital

Resultados del análisis de datos digitales que descubren pruebas potenciales de incidentes maliciosos e identifican posibles actores de amenazas.

Investigador forense digital

Pruebas electrónicas

Pruebas potenciales derivadas de datos contenidos o producidos por cualquier dispositivo cuyo funcionamiento dependa de un programa informático o de datos almacenados en un sistema o red informáticos o transmitidos a través de ellos. (por ejemplo, recopilación precisa de registros)

Probador de penetración

Informe de resultados de la evaluación de vulnerabilidades

Informe que enumera y evalúa la importancia de las vulnerabilidades descubiertas en un sistema durante una exploración de vulnerabilidades (normalmente automática). El informe también puede sugerir acciones básicas de corrección.

Examen de Penetración

Informe de prueba de penetración

Informe que proporciona un análisis detallado y exhaustivo de las vulnerabilidades de un sistema identificadas durante una prueba de seguridad. El informe también puede incluir sugerencias de medidas correctivas.