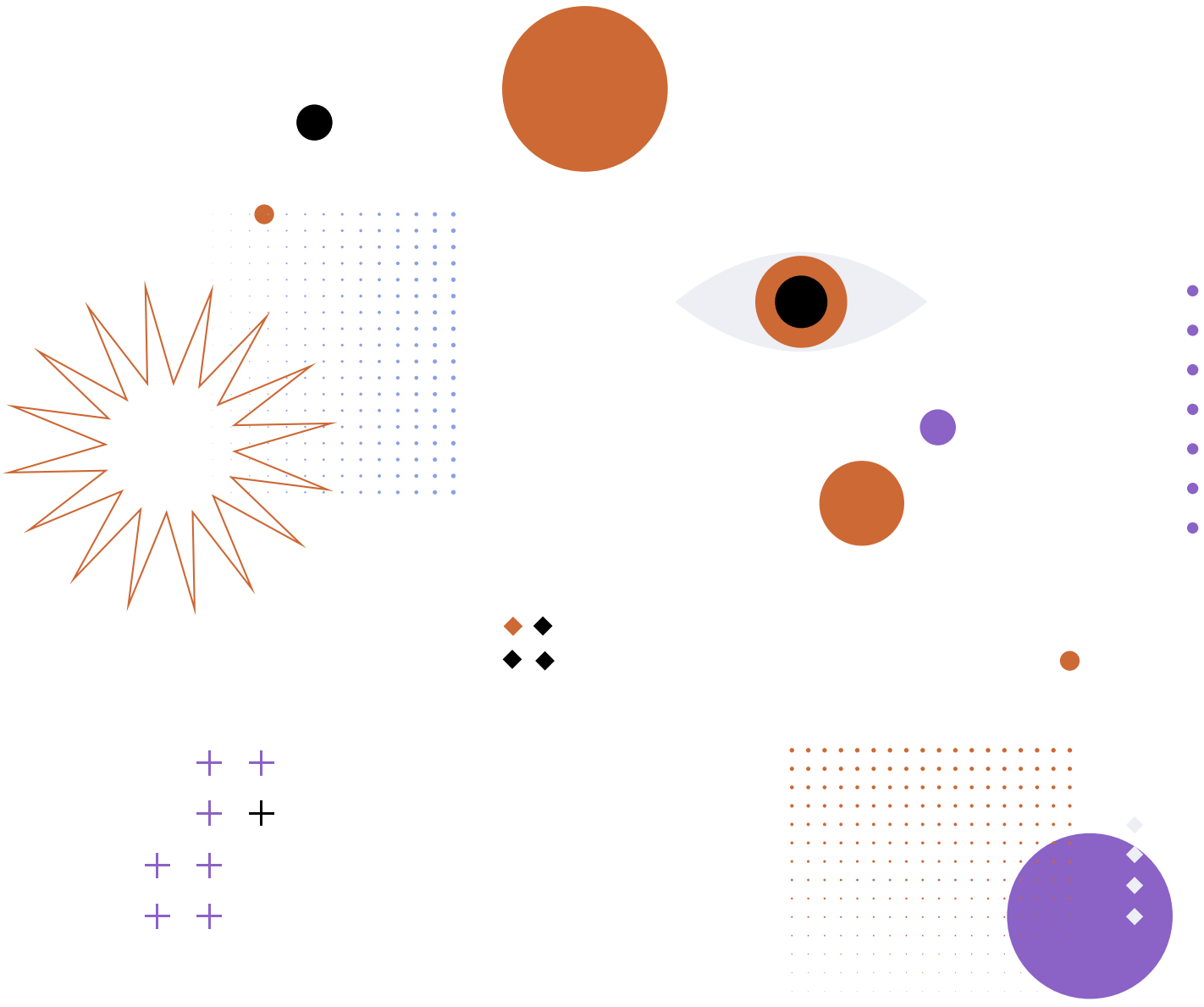
FUNDACIONSADOSKY.ORG.AR

Perfiles en ciberseguridad

Conocimientos y habilidades necesarias para los desafíos actuales.



Fundación SADOSKY

Ministerio de Ciencia, Tecnología e Innovación Argentina

Perfiles en ciberseguridad

Conocimientos y habilidades necesarias para los desafíos actuales.

Autoría

Marcela Pallero
Directora del área de Seguridad TIC de la Fundación Sadosky

Juan Martín Heguiabehere
Seguridad TIC, Fundación Sadosky

Diseño Gráfico

Jaqueline Schaab
Fundación Sadosky

Autoridades de la Fundación Dr. Manuel Sadosky

Daniel Filmus
Presidente

Fernando Schapachnik
Director Ejecutivo

Índice

Introducción

El objetivo del presente trabajo es brindar una orientación a las organizaciones sobre diferentes áreas de aplicación de la ciberseguridad y al mismo tiempo ámbitos de trabajo.

Fortalecer la ciberseguridad en las organizaciones resulta hoy una necesidad imperiosa como resultado del crecimiento de la incorporación de las tecnologías de la información y las comunicaciones en casi todos los servicios modernos, que adquieren un rol cada vez más central en nuestras sociedades.

Los servicios digitales de distintos ámbitos como las finanzas, la enseñanza, las relaciones sociales, tienen un lugar cada vez más grande del conjunto total de servicios y productos que utilizamos.

Para hacer efectiva la implementación de medidas de seguridad, un requisito es contar con personas formadas en los distintos dominios de esta disciplina así como crear planes de formación y educación de acuerdo con las necesidades concretas detectadas.

Las actividades contempladas en los marcos de buenas prácticas o estándares internacionales más conocidos y utilizados en seguridad de la información y ciberseguridad prevén tareas que pertenecen a distintas áreas de conocimiento o especialidades. En este sentido, y con el surgimiento, el despliegue e interconexión de múltiples tecnologías en los últimos años, los marcos de referencia se han concentrado en actualizar sus contenidos y adaptarse a los cambios tecnológicos y de paradigmas y contemplar las medidas necesarias para hacer frente a los riesgos actuales.

A fin de incorporar personal en las organizaciones para realizar las principales actividades, es necesario identificar los perfiles, las actividades y las áreas de conocimiento que incorporen tales buenas prácticas. Con ese objetivo se puede formar o capacitar al personal de la propia organización o contratar actividades como servicio, en caso de ser necesario.

Los roles planteados en este documento tienen la finalidad de orientar a quienes tienen la responsabilidad de incorporar a la ciberseguridad y seguridad de la información a una organización pública o privada en función de los estándares internacionales en la materia se ha tomado como base el marco de referencia de la ENISA, la Agencia Europea para la Ciberseguridad.

Consideraciones sobre el tamaño y complejidad de las organizaciones

En función de transitar un camino de mejora en la gestión de la ciberseguridad de las organizaciones más pequeñas o con menor complejidad tecnológica y también menores presupuestos, es necesario mencionar que hay actividades, que no son permanentes o, que si bien lo son, podrían delegarse en un tercero a contratar como servicio, ya sea a un o una profesional o empresa, recordando que se pueden delegar las actividades, pero nunca la responsabilidad. En estos agrupamientos de actividades, se ha agregado la mención, en el listado que sigue, como “factible de tercerizar”, a modo de orientación, mas allá que la decisión de tercerizar las actividades la toman las autoridades de cada organización. En particular, son ejemplos de actividades que pueden ser contratadas las que se refieren a

pruebas de intrusión, de forensia informática, auditorías específicas y las de capacitación. Por otro lado, es relevante mencionar que si bien hay actividades que pueden ser realizadas por roles no especializados, cómo podrían ser la gestión de vulnerabilidades, o la seguridad de la red, la función de responsable de "seguridad de la información o ciberseguridad", es decir, un rol con la responsabilidad de velar por la efectivo cumplimiento de las tareas de ciberseguridad y realizar un seguimiento aparece como obligatorio, a la luz de la relevancia y necesidad. Adicionalmente se debe mencionar como buena práctica y en la medida de las posibilidades, que el rol de responsable de ciberseguridad o de seguridad de la información debería ser independiente del área de Sistemas o Tecnologías de la Información.

Esta obligatoriedad tiene sustento en la medida que pueden existir intereses opuestos entre las necesidades funcionales o de negocio de los sistemas o productos y las de seguridad de la información, por ejemplo cuando existe una fecha de puesta en producción y las pruebas de seguridad no cumplen los mínimos necesarios. El rol es también necesario para llevar adelante planes, adecuaciones y mejoras.

En esta línea cabe mencionar que la función de gobierno o gobernanza de la ciberseguridad debería consolidarse mediante la capacitación de una autoridad de la organización, ya que las decisiones estratégicas corresponden a quienes velan por los objetivos centrales de cada entidad.

Cabe mencionar que no se incluyen en estas descripciones perfiles que deberían considerarse al tratarse la ciberseguridad a nivel Estado, en el que deberían considerar aspectos como planes de educación y formación como carreras profesionales, Investigación, Innovación y Desarrollo, o ciberdiplomacia, entre otros temas. Así como tampoco se encuentran incluidos perfiles en rubros específicos como podrían ser fraudes para el caso de empresas relacionadas con servicios digitales financieros.

Esta publicación es una propuesta que se encuentra abierta a comentarios. Quedan invitados a enviarlos a stic@fundacionsadosky.org.ar.

Perfiles, entregables, áreas de conocimiento y actividades

Perfil	Gobierno de ciberseguridad
Entregables	• Estrategia de ciberseguridad • Política de ciberseguridad • Presupuesto de ciberseguridad
Áreas de conocimiento	• Estrategia de ciberseguridad • Políticas de ciberseguridad. • Visión corporativa o de gobierno. • Riesgos organizacionales • Programas de ciberseguridad. • Planificación financiera. • Conciencia de las amenazas (situational awareness) • Cumplimiento
Actividades	• Definir la estrategia y las políticas de ciberseguridad de la organización y asegurar su ejecución. • Asegurar que la estrategia de ciberseguridad se encuentre alineada con los objetivos de negocio. • Asegurar el presupuesto de ciberseguridad. • Asegurar los recursos para implementar la estrategia de ciberseguridad. • Evaluar y aceptar los niveles de apetito y tolerancia del riesgo de ciberseguridad. • Promover la cultura de ciberseguridad. Impulsar las iniciativas que involucren cualquier aspecto de ciberseguridad.

Perfil	Gestión de Riesgos y Seguridad de la Información
Entregables	• Planes de mitigación de riesgos • Programa de seguridad de la información • Diseño del marco organizativo. • Informes de gestión (incidentes y controles) • Plan de Respuesta ante incidentes de seguridad de la información • Plan de Continuidad del Negocio (aspectos de TI) • Programas de concientización • Programa de educación • Material para capacitación y entrenamiento
Áreas de conocimiento	• Gestión del riesgo de seguridad de la información • Gestión de la seguridad de información • Plan de continuidad del Negocio • Capacitación, concientización y comunicación

Actividades	<u>De gestión de seguridad de la información</u> • Diseñar y supervisar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). • Concientizar y capacitar al nivel gerencial sobre los riesgos y amenazas de ciberseguridad y su impacto en la organización. • Asesorar y asistir a la Dirección en los procesos de identificación y análisis de riesgos de ciberseguridad de la organización. • Desarrollar planes de ciberseguridad. • Mantener informada a la Dirección sobre la ocurrencia de incidentes, los procesos de gestión de riesgos y los hallazgos en materia de ciberseguridad • Asegurar la resiliencia de la organización ante ciberincidentes. • Asegurar el control de accesos a la información y los servicios. • Evaluar la selección e implementación de certificaciones en ciberseguridad (para desarrollo, centro de datos, organizacionales, etc.) • Gestionar la capacitación continua dentro de la organización. • Implementar buenas prácticas en materia de seguridad de la información. <u>De gestión de riesgos de ciberseguridad</u> • Desarrollar la estrategia de gestión de riesgos de ciberseguridad de una organización. • Gestionar el inventario de activos de información de la organización. • Identificar y evaluar amenazas y vulnerabilidades relacionadas con la ciberseguridad de los sistemas de TIC. • Identificar escenarios de amenazas, incluyendo perfiles de atacantes y estimación del potencial de ataques. • Evaluar los riesgos de ciberseguridad e implementar mecanismos de tratamiento de riesgos en línea con los objetivos estratégicos del negocio y el apetito de riesgo determinado por las autoridades, incluyendo controles de seguridad, mitigación y medidas para evitar riesgos. • Monitorear la efectividad de los controles de ciberseguridad y los niveles de riesgo. • Asegurar que todos los riesgos de ciberseguridad permanezcan en un nivel aceptable para los activos de la organización. • Desarrollar, mantener, reportar y comunicar el ciclo completo de gestión de riesgos.

Actividades	<u>De gestión de accesos e identidades</u> • Establecer y mantener un inventario de cuentas de personas usuarias y servicios. • Establecer una política de contraseñas y métodos de autenticación en general y establecer medidas para monitorear su cumplimiento. • Elaborar e implementar política de inhabilitación de cuentas sin actividad. • Elaborar e implementar una política de cuentas con privilegios administrativos y establecer medidas para monitorear su cumplimiento. • Establecer un proceso de otorgamiento y revocación de accesos. • Establecer y mantener mecanismos de control de accesos y establecer medidas para monitorear su cumplimiento. <u>Capacitador en ciberseguridad</u> → **Área de trabajo: Factible de tercerizar** • Desarrollar, actualizar, brindar y monitorear programas de formación y material educativo sobre ciberseguridad y protección de datos para la formación y la concientización en función del contenido, método, herramientas y necesidades de los y las estudiantes. • Organizar, diseñar, brindar y monitorear actividades de concientización sobre ciberseguridad y protección de datos, seminarios, cursos y formación práctica, medir y evaluar efectividad. • Mantener y mejorar continuamente la experiencia y conocimientos del personal; fomentar y potenciar la mejora continua de las capacidades y habilidades de ciberseguridad.

Perfil	**Asesoría legal y cumplimiento**
Entregables	• Manual de cumplimiento • Reportes de cumplimiento • Cláusulas de confidencialidad • Evaluación de impacto en Protección de datos
Áreas de conocimiento	• Políticas, normas y procedimientos de seguridad de la información • Aspectos legales generales • Protección de datos y privacidad • Propiedad intelectual • Defensa de consumidores
Actividades	• Realizar acciones que impulsen el cumplimiento del marco normativo externo aplicable y del marco interno. • Proporcionar asesoramiento y guía legal sobre estándares, leyes y regulaciones de privacidad de datos y protección de datos. • Identificar y documentar brechas de cumplimiento. • Realizar evaluaciones de impacto en la privacidad y desarrollar, mantener, comunicar y entrenar en las políticas y procedimientos de privacidad.

Actividades	• Asegurar que las personas propietarias, titulares, controladores, entidades de procesamiento de datos, sujetos, socios internos o externos y entidades estén informados sobre sus derechos, obligaciones y responsabilidades en materia de protección de datos. • Asistir en el diseño, implementación, auditorías y pruebas de cumplimiento para garantizar el cumplimiento de las medidas y requerimientos vinculados a la ciberseguridad y la privacidad. • Contribuir al desarrollo de la estrategia, política y procedimientos de ciberseguridad de la organización. • Gestionar aspectos legales de las responsabilidades de seguridad de la información y las relaciones con terceros. • Monitorear las actividades de entrenamiento relacionadas con la protección de datos. • Identificar aquellos incidentes que puedan considerarse delitos para prever acciones necesarias. • Identificar riesgos legales derivados del uso de tecnologías emergentes.

Perfil	**Seguridad informática**
Entregables	• Manual de inteligencia en amenazas • Reportes de inteligencia en amenazas • Diagrama de arquitectura de ciberseguridad • Informe de requerimientos en ciberseguridad • Diagnóstico de vulnerabilidades técnicas y planes de remediación
Áreas de conocimiento	• Arquitectura de ciberseguridad • Respuesta ante incidentes • Inteligencia en Amenazas • Forensia digital • Pruebas de intrusión • Gestión de vulnerabilidades técnicas
Actividades	De arquitectura en ciberseguridad • Diseñar, gestionar y documentar una arquitectura segura para implementar la estrategia de la organización. • Establecer un entorno seguro durante el ciclo de vida de desarrollo de sistemas, servicios y productos. • Coordinar el desarrollo, integración y mantenimiento de componentes de ciberseguridad asegurando las especificaciones de ciberseguridad. • Adoptar las medidas de seguridad en el intercambio de información en los servicios con terceras partes con las que se interconecta. • Adaptar la arquitectura de la organización a amenazas emergentes, teniendo en cuenta las capacidades de procesamiento y almacenamiento requeridas. Respaldos, copias de seguridad y backup.

Actividades	De seguridad de la red • Establecer y mantener un proceso de configuración segura para dispositivos de red. • Establecer procedimientos y responsabilidades para la gestión de equipos y dispositivos de red. • Mantener documentación actualizada incluyendo diagramas de red y configuración de dispositivos. • Separar la red de datos de la red de servicio, si fuera necesario. • Establecer y mantener una política de acceso externo a la red acorde con los requerimientos de seguridad de la entidad. • Implementar formas de autenticación y cifrado para el acceso externo (por ejemplo VPNs). • Monitorear y registrar información relevante a la seguridad de la red. • Inhabilitar protocolos de red vulnerables. De implementación de ciberseguridad • Desarrollar, implementar, mantener, mejorar y probar productos de ciberseguridad. • Proporcionar soporte relacionado con la ciberseguridad a las personas usuarias y clientela. • Integrar soluciones de ciberseguridad y asegurar su buen funcionamiento. • Supervisar el uso de funciones y sistemas de criptografía. • Configurar de manera segura sistemas, servicios y productos. • Mantener y mejorar la seguridad de sistemas, servicios y productos. • Implementar y monitorear procedimientos y controles de ciberseguridad. • Trabajar coordinadamente con el personal de TI (tecnologías de la información) /OT (tecnología de operaciones, o tecnologías de gestión de procesos de producción) en acciones relacionadas con la ciberseguridad. • Promover y controlar la adopción de prácticas de desarrollo seguro. • Implementar, aplicar y administrar actualizaciones/parches de seguridad en productos para abordar y minimizar cualquier vulnerabilidad. Del ambiente físico y ambiental asociado a los intercambios y procesamiento de información • Definir perímetros físicos de seguridad y protegerlos. • Proteger apropiadamente las áreas seguras con controles de acceso en los puntos de entrada física. • Aplicar una política de escritorios limpios y pantallas limpias. • Asegurar físicamente oficinas, habitaciones y dependencias.

Actividades	• Implementar vigilancia física (cámaras, guardias, detectores varios). • Adoptar medidas de protección contra amenazas físicas y ambientales que atenten con los dispositivos o el procesamiento (AA, otros) • Asegurar la provisión de los servicios básicos en las instalaciones de procesamiento de información. • Proteger el cableado en las instalaciones. • Dotar de medidas de protección de los activos de información que salen del perímetro de seguridad. • Adoptar las medidas de seguridad en el ciclo de vida de los medios de almacenamiento. • Reutilizar o descartar equipos en forma segura. De forensia digital → Área de trabajo: Factible de tercerizar. • Desarrollar políticas, planes y procedimientos de investigación forense digital. • Colaborar en el plan de respuesta ante incidentes. • Identificar, recuperar, extraer, documentar y analizar pruebas digitales. • Preservar y proteger pruebas digitales y hacerlas disponibles para las personas interesadas autorizadas. • Revisar entornos en busca de evidencia de acciones no autorizadas e ilegales. • Documentar, reportar y presentar de manera sistemática y determinística los hallazgos y resultados del análisis forense digital. • Seleccionar y personalizar técnicas de pruebas, análisis y reporte forenses. De inteligencia en amenazas → Área de trabajo: Factible de tercerizar. • Desarrollar planes y procedimientos para gestionar los procesos de inteligencia de amenazas. • Traducir los requisitos del negocio en requisitos de Inteligencia. • Identificar, monitorear y evaluar las Tácticas, Técnicas y Procedimientos (TTP) utilizados por los actores de amenazas cibernéticas al analizar datos, información e inteligencia de fuentes abiertas y propietarias. • Producir informes basados en datos de inteligencia de amenazas. • Aprovechar los datos de análisis de amenazas para apoyar y ayudar en el modelado de amenazas, las recomendaciones de mitigación de riesgos y la búsqueda de amenazas cibernéticas.

Actividades	• Comunicar a las personas interesadas no técnicas la gravedad de las implicancias en términos de protección de los activos de información al explicar la exposición al riesgo y sus consecuencias. De pruebas de intrusión → **Área de trabajo: Factible de tercerizar.** • Identificar, analizar y evaluar vulnerabilidades técnicas y organizativas de ciberseguridad. • Identificar vectores de ataque, descubrir y demostrar la explotación de vulnerabilidades técnicas de ciberseguridad. • Seleccionar y desarrollar técnicas de pruebas de penetración adecuadas e implementarlas periódicamente. • Organizar planes y procedimientos de pruebas de penetración. • Establecer procedimientos para el análisis y reporte de resultados de pruebas de penetración. • Documentar y reportar resultados de pruebas de penetración a los interesados. • Desplegar herramientas de pruebas de penetración y programas de prueba y adoptar las medidas necesarias para mitigar los riesgos identificados.

Perfil	**Auditoría de ciberseguridad** → Área de trabajo: Factible de tercerizar.
Entregables	• Plan de auditoría. • Programa de auditoría. • Informes de auditoría.
Áreas de conocimiento	• Auditoría de ciberseguridad. • Riesgos de seguridad de la información. • Controles internos.
Actividades	• Auditar la conformidad con los estándares aplicables relacionados con la ciberseguridad, la legislación y regulaciones. • Ejecutar el plan de auditoría y recopilar evidencia y mediciones. • Asegurar la integridad de los registros de auditoría. • Desarrollar y comunicar informes de evaluación de conformidad, aseguramiento, auditoría, certificación y mantenimiento de las certificaciones. • Monitorear el proceso de gestión de riesgos de seguridad de la información, particularmente las actividades de mitigación.

Áreas de conocimientos para la ciberseguridad

En un ámbito organizacional, sea público o privado.

A continuación se mencionan los temas y subtemas en materia de ciberseguridad, así como campos donde la ciberseguridad contribuye. Entre estos se encuentran por ejemplo, la continuidad y la resiliencia.

Las responsabilidades, funciones y actividades relacionadas con la continuidad y la resiliencia corresponden al ámbito de los riesgos organizacionales, que están directamente relacionados con la misión y función de la organización.

Gobierno de la ciberseguridad

- Estrategia de ciberseguridad.
- Políticas de ciberseguridad.
- Visión corporativa o de gobierno.
- Riesgos organizacionales (ERM).
- Programas de ciberseguridad.
- Planificación financiera.

Gestión de la seguridad de información

- Planificación de la seguridad, en función de los objetivos, de los riesgos y los recursos disponibles.
- Políticas, normas y procedimientos.
- Marco de control (métricas incluidas).
- Coordinación con el resto de la organización los aspectos de seguridad.
- Supervisión del cumplimiento de métricas.
- Estándares y buenas prácticas en las distintas áreas en ciberseguridad.
- Gestión de vulnerabilidades.

Gestión del riesgo de seguridad de la información

- Metodologías de gestión de riesgo.
- Evaluación de amenazas.
- Supervisión de lo planificado, corrección de objetivos.
- Evaluación de niveles de riesgo en función de los objetivos de la organización.
- Plan de mitigación de riesgos
- Comunicación de visión, riesgos y necesidades a la alta gerencia.

Gestión de la continuidad de negocio o la gestión

- Análisis de impacto del negocio o servicio (BIA) en los aspectos vinculados a la protección de la información.
- Gestión de los aspectos de seguridad del riesgo de continuidad.
- Planes de Continuidad del Negocio o del servicio, en sus aspectos de ciberseguridad.

Operación de base en seguridad informática

- Arquitectura de la seguridad.
- Implementación de sistemas de seguridad informática.
- Implementación de prácticas de Seguridad en el desarrollo.
- Implementación de prácticas Seguridad en la configuración de redes.
- Implementación de parches y actualizaciones.
- Implementación de seguridad física.

Criptografía

- Algoritmos de hash.
- Algoritmos de cifrado. PFS.
- Sistemas criptográficos y sus implementaciones, como PKI, blockchain, DLT.

Respuesta ante incidentes

- Planes de respuesta ante incidentes.
- Aspectos de forensia digital para la investigación del origen y los responsables.
- (Redes, sistemas, dispositivos móviles, web, bases de datos, etc)

Inteligencia en amenazas

- Inteligencia: Recolección, análisis y producción.
- Utilización de la inteligencia para guiar acciones.
- Intercambio de información de inteligencia con otras partes interesadas.

Pruebas de intrusión

- Pruebas en Aplicaciones web.
- Pruebas y testeos en Redes (internas, wifi, Internet).
- Pruebas técnicas en Sistemas operativos.
- Pruebas técnicas en Aplicaciones móviles.

Aspectos legales

- Asistencia en la elaboración de políticas.
- Asistencia en la elaboración de Plan de respuesta ante incidentes.
- Asistencia en evaluación de riesgos legales.
- Asistencia en contrataciones, cláusulas de seguridad en las cadenas de servicios.
- Asistencia en la redacción de acuerdos de confidencialidad (NDA) y Acuerdos de niveles de servicio.
- Cumplimiento de la regulación general y de la normativa interna.
- Procesos que involucren sanciones por incumplimiento.
- Procesos de gestión de incidentes de seguridad de la información/ciberseguridad
- Cumplimiento en las medidas tendientes a la protección de datos personales y privacidad.

Capacitación y concientización

- Concientización sobre uso responsable de activos de información (amenazas).
- Capacitación sobre el plan de incidentes y los aspectos vinculados a la resiliencia.
- Capacitación en dominios específicos. (Arquitectura, desarrollo seguro, pentester, etc.)

Auditoría (La función de auditoría es básica para los procesos de aseguramiento)

- Auditoría de gestión de riesgo.
- Auditoría de gestión de seguridad de la información.
- Auditoría de software.
- Auditoría sobre procesos específicos.
- Auditorías para las distintas áreas de ciberseguridad.

Niveles de conocimiento

Cada conjunto de actividades agrupadas en estos perfiles, como en todas las áreas de conocimiento tiene niveles de expertise, es decir, que siendo éstos niveles derivados mayoritariamente de la cantidad de prácticas, de investigación y tiempo de estudios.

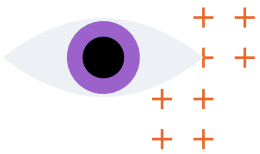
Adicionalmente, cabe mencionar que para un nivel avanzado, la mayoría de las actividades, requiere como prerequisito conocimientos de las tecnologías específicas y ciencias básicas como podría ser el caso de redes, de sistemas de información, programación o criptografía, por citar algunos ejemplos, que corresponden a distintas ingenierías o ciencias básicas como la matemática, en otros casos son temas abordados por las ciencias económicas o de la administración, en menor medida.

- **Nivel básico**: son conocimientos básicos, adquiridos en cursos cortos o autodidactas o por breves experiencias prácticas, sin conocimientos profundos en el tema.

- **Nivel intermedio**: conocimientos generales y breve experiencia en algún tema específico, con alguna certificación pero sin experiencia práctica o con experiencia limitada y sin ninguna capacitación (sea formal o autodidacta).

- **Nivel avanzado**: Profesional especializado con amplia experiencia (podrían ser más de 8 años) y conocimientos en una o varias áreas de la ciberseguridad.

- **Nivel experto**: Este nivel incluye conocimientos, experiencia y habilidades altamente especializados en ciberseguridad y la capacidad de aplicar estos conocimientos a situaciones complejas, nuevas y cambiantes, con conocimientos profundos de las ciencias básicas o aplicadas al área de expertise.



Perfiles en ciberseguridad

FUNDACIONSADOSKY.ORG.AR

Fundación SADOSKY
Ministerio de Ciencia, Tecnología e Innovación Argentina