Taxonomía de soluciones de ciberseguridad

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

2006-2016

TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

1 Prólogo

El continuo avance de las tecnologías ha propiciado que los agentes responsables de las amenazas hayan incrementado la sofisticación de sus ataques y sus herramientas, dando lugar a un ciberespacio cada vez más hostil, que obliga a las organizaciones a disponer de los medios técnicos más novedosos para poder hacer frente a los ataques y a sus posibles impactos, así como adoptar políticas de seguridad proactiva para mitigarlos.

En la actualidad este enfoque está evolucionando hacia la gestión de los riesgos del ciberespacio (*Information Assurance*, IA), donde la ciberseguridad consiste en un proceso continuo de análisis y gestión de los riesgos asociados al ciberespacio.

Las amenazas más importantes relacionadas con el ciberespacio se pueden clasificar en dos grupos: amenazas contra la información, y amenazas contra la infraestructura. Las amenazas contra la información son aquellas que provocan una pérdida o un uso indebido de la información, el espionaje, el fraude, el robo de identidad, entre otras muchas. Por otro lado, las amenazas contra la infraestructura son aquellas que pueden provocar la interrupción parcial o total de los sistemas, como la infección de *malware*, ataques contra redes, sistemas, etc.

La ciberseguridad no es algo meramente técnico sino que requiere involucrar a las organizaciones y definir nuevas actividades y responsabilidades, con el fin de salvaguardar la información y las infraestructuras. Será necesario identificar un escenario que contemple la seguridad de los sistemas de información y las comunicaciones, así como los sistemas de control de procesos, incluyendo los diferentes actores de la cadena, personal, organización y la infraestructura.

Otros factores de cambio son las tecnologías móviles y la computación en la nube (*cloud computing*) que están generando cambios muy importantes en la seguridad de las organizaciones, alterando la demanda de soluciones o propiciando en muchos casos la innovación de dichas soluciones.

Todos los cambios que se han producido en estos últimos años, han puesto a prueba la taxonomía y han hecho necesaria su revisión, de forma que esta asimile la evolución que se está produciendo en las soluciones de seguridad y pueda hacer frente con garantías al futuro inmediato de un mercado en constante cambio.

Las amenazas más importantes relacionadas con el ciberespacio se pueden clasificar en dos grupos: amenazas contra la información, y amenazas contra la infraestructura.

2 Presentación

El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

El CERT de Seguridad e Industria (CERTSI), centro de respuesta a incidentes de ciberseguridad operado por INCIBE, trabaja para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información. Aumentar la ciberresiliencia de las organizaciones y el diseño de medidas preventivas para atender a las necesidades de la sociedad en general y, en virtud del Convenio de Colaboración suscrito entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, a las necesidades de seguridad de las infraestructuras críticas, de apoyo en la investigación y lucha frente a ciberdelitos y ciberterrorismo.

La misión de INCIBE es por tanto reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general.

La misión de INCIBE es reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la Sociedad de la Información.

3 La taxonomía de soluciones de ciberseguridad

Las tecnologías móviles, junto con el enorme crecimiento de las redes sociales y de otros servicios, como la mensajería instantánea y la computación en la nube han provocado una socialización y masificación de las tecnologías de la información y la seguridad sin precedentes, tanto en el ámbito del consumo, como en el profesional.

Todos los cambios que se han producido en estos últimos años, han puesto a prueba la taxonomía y han hecho necesaria su revisión, de forma que esta asimile la evolución que se está produciendo en las soluciones de seguridad y pueda hacer frente con garantías al futuro inmediato de un mercado en constante cambio.

3.1 Metodología

La taxonomía de soluciones de ciberseguridad va dirigida hacia una nueva etapa de amenazas y vulnerabilidades en el ciberespacio, es por ello, que conlleva una actualización de la clasificación de las categorías y subcategorías actuales.

Para la realización de estas mejoras se ha tenido en cuenta una herramienta fundamental y que ha sido de base para las anteriores ediciones de la taxonomía, el Catálogo de Empresas y Soluciones de Ciberseguridad de INCIBE, el cual ha aportado las claves necesarias para adaptar la taxonomía al mercado actual de la ciberseguridad.

Se ha tenido en cuenta a los diferentes actores del mercado de la ciberseguridad, como son los proveedores de soluciones de seguridad, así como a los diferentes organismos nacionales e internacionales que marcan la tendencia actual.

Todo esto ha permitido establecer una metodología de trabajo muy completa que, como veremos más adelante, se materializará en una taxonomía más depurada, con mayor sencillez y lo que se pretendía, ajustada al a evolución del mercado de la ciberseguridad.

3.2 Alcance de productos y servicios

El alcance permite establecer dónde o en qué área de cualquier organización actúan cada una de las categorías de productos y servicios. El alcance está predefinido para cada categoría y aporta información adicional sobre la misma.

Para los productos se determinan cinco alcances diferentes:

- gestión de acceso e identidad;
- protección en el puesto de trabajo;
- seguridad en aplicaciones y datos;
- seguridad en los sistemas;
- seguridad en las redes.

3 La taxonomía de soluciones de ciberseguridad

Estos alcances están ordenados en base a cualquier proceso de implantación de soluciones de seguridad en una organización, comenzando con la "gestión de acceso e identidad" y finalizando con la "seguridad en las redes".

En los servicios, se establecen alcances de aplicación más heterogéneos, debido a que los propios servicios son soluciones más genéricas, y pueden ser aplicados no solo a infraestructuras y sistemas, sino a personas o a la propia organización.

Para los servicios se establecen los siguientes alcances:

- personas;
- información;
- infraestructura;
- negocio.

Los alcances posibilitan la realización de una búsqueda más sencilla de soluciones de seguridad, puesto que no solo utilizamos las categorías sino que también podemos filtrar por qué queremos proteger, dónde se van a utilizar estas soluciones, o en qué área de nuestra organización necesitamos integrar una solución de seguridad.

3.2.1 Descripción de los alcances de productos

Para los productos se han identificado los siguientes alcances:

GESTIÓN DE ACCESO E IDENTIDAD

En cualquier entidad, el primer elemento de seguridad que es necesario proteger es el acceso a los sistemas y las aplicaciones.
Estos mecanismos son los responsables de establecer los permisos y vigilar los accesos a los sistemas y aplicaciones locales o remotas, de asignar, mantener y controlar los perfiles de los usuarios.
La movilidad y el *cloud computing* plantean nuevos retos para el acceso en remoto a los sistemas y la identificación de los usuarios. Por todo ello cobran especial importancia los mecanismos de control de acceso e identidad, así como los elementos de autenticación.

PROTECCIÓN EN EL PUESTO DE TRABAJO

Después de tener protegido el acceso, se ha de tener la garantía de seguridad de los sistemas de los dispositivos que forman el puesto de trabajo. En este alcance se tiene en cuenta la seguridad aplicable a los sistemas operativos de los dispositivos que están ante el usuario.
Los productos de seguridad de este alcance se encargan de proteger al usuario y su

3 La taxonomía de soluciones de ciberseguridad

equipo contra posibles incidentes de seguridad. Son los productos que aportan seguridad en el entorno local, en el *hardware* y *software* del usuario. Suelen incluir funciones que vigilan la actualización del *software* instalado en nuestros sistemas, advirtiendo de posibles amenazas.

SEGURIDAD EN APLICACIONES Y DATOS

Partimos de que nuestros recursos básicos están a salvo, de que solo puede acceder quién está autorizado para ello y de que trabajamos en un entorno seguro. El usuario necesita aplicar las tecnologías de seguridad a los datos y a las aplicaciones con los que trabaja.
Este nivel es el encargado de dotar de seguridad a las aplicaciones y datos, desde los sistemas de almacenamiento local hasta los remotos. Productos que cifran la información, así como los que establecen políticas de respaldo de la información, copias de seguridad, etc.
Particular interés tienen en este alcance la protección de datos personales y la autenticación (comercio electrónico, banca online...) que en la actualidad está siendo objeto de un incremento de ataques.

SEGURIDAD EN LOS SISTEMAS

Este alcance va dirigido a los usuarios técnicos y administradores de sistemas. En este nivel, el usuario necesita aplicar medidas técnicas y organizativas que protejan los sistemas informáticos de la empresa de forma centralizada ante incidentes de seguridad, tanto de forma preventiva como reactiva.
Las soluciones que aplican sirven con frecuencia para aplicar métodos de supervisión y mecanismos de auditoría. Se incluyen herramientas para servidores corporativos, herramientas de restauración en caso de incidentes de seguridad para sistemas de almacenamiento, así como herramientas de auditorías técnicas de sistemas y gestión de eventos de seguridad.

SEGURIDAD EN LA RED

El último nivel es de la seguridad en la red, que engloba los elementos directamente aplicables a las redes. Estos productos van a garantizar al usuario poder confiar el transporte de la información a través de los diferentes mecanismos transmisores.
En este alcance se incluyen principalmente los cortafuegos, las redes privadas virtuales, sistemas de prevención y detección de intrusiones, herramientas para la protección de redes inalámbricas y dispositivos móviles, así como herramientas para el control de tráfico de red y comunicaciones.
Aquí se garantiza la seguridad en los accesos remotos de equipos entre redes, y la trasferencia de información, permitiendo solo a usuarios autorizados, la supervisión, análisis y control de los tráficos entrantes y salientes y garantizando la continuidad de conectividad de los quipos transmisores.

3 La taxonomía de soluciones de ciberseguridad

3.2.2 Descripción de los alcances de servicios

Los alcances identificados para los servicios son los siguientes:

PERSONAS

El primer nivel se refiere a los servicios de seguridad relacionados con el sistema organizativo de la empresa, funciones, responsabilidades, procedimientos que realizan las personas.
Los servicios bajo este alcance están relacionados con la concienciación y la formación sobre medidas de seguridad. Los servicios de aplicación de medidas de seguridad organizativas; permisos y obligaciones, la identificación y prevención ante ataques de ingeniería social, cumplimiento con la legislación. También están los servicios de mantenimiento de la actividad en caso de ataque, restauración de la actividad y búsqueda de los motivos del fallo de seguridad.

INFORMACIÓN

En el alcance relativo a la información se agrupan los servicios de seguridad que permiten directamente la protección y recuperación de datos e información de la empresa.
La información representa uno de los activos más importantes de las empresas, siendo el objetivo de la seguridad de la información es garantizar la confidencialidad, la integridad y la disponibilidad de esta.
Los servicios bajo este ámbito van a permitir el intercambio de información confidencial, también los servicios orientados a la protección frente a pérdidas de información, copias de seguridad y su posterior recuperación, los que evitan la difusión no permitida de la información y los que aplican medidas de protección.

INFRAESTRUCTURA

La infraestructura agrupa los servicios de seguridad que aplican al equipamiento de la entidad y la protección de los sistemas de control industrial.
Bajo este alcance se encuentran los servicios dirigidos a la selección, implementación y operación de las soluciones de seguridad. Se encuentran los servicios que detectan los posibles fallos de seguridad de la infraestructura, y los que proporcionan los recursos necesarios de seguridad y la gestión de los incidentes de seguridad.

NEGOCIO

El ámbito de negocio está referido a los servicios de seguridad relativos al negocio en todas sus expresiones.
Bajo este alcance están los servicios que facilitan los cambios organizativos necesarios para la adecuación de los planes y políticas de seguridad dentro de las organizaciones, las normativas y los requisitos legales aplicables.
También está la implantación de buenas prácticas en materia de seguridad de la información, que afecta de forma positiva en la mejora de los procesos productivos, dotándolos de fiabilidad y seguridad, y permitiendo ahorro de costes y tiempos de indisponibilidad de sus propios servicios, son servicios bajo este alcance.

3.3 Uso o ámbito de aplicación

La taxonomía incluye un concepto que permite establecer a quién va dirigida la solución y de qué modo puede afectar a su infraestructura. Este concepto posibilita la realización de una búsqueda más sencilla de soluciones de seguridad, puesto que no solo utilizamos las categorías y el dónde se utilizan, sino que además podemos utilizar a quién y a qué tipo de cliente podemos proteger.

Los ámbitos de aplicación para las soluciones de ciberseguridad de la taxonomía van dirigidos según el tipo de cliente y son los siguientes:

- microempresa / autónomos;
- pymes (pequeña/mediana empresa);
- gran empresa;
- infraestructuras críticas.

En la descripción de los ámbitos se tiene en cuenta las empresas y organizaciones según el tamaño y su repercusión ante cualquier incidente de seguridad, así como su infraestructura.

MICROEMPRESA / AUTÓNOMOS

En este ámbito se encuentran las empresas que tienen menos de 10 trabajadores y que en muchos de los casos son autónomos, así como un volumen de negocio pequeño. No tienen personal cualificado para la seguridad de sus infraestructuras.
Las soluciones de seguridad enfocadas a este ámbito van dirigidas al cumplimiento normativo y legislativo, a la implantación de soluciones que mitiguen cualquier incidente de seguridad, herramientas de protección y recuperación. Son soluciones que aportan seguridad al entorno local, en el *hardware* y *software* de los usuarios.

3 La taxonomía de soluciones de ciberseguridad

PYMES (pequeña/mediana empresa)

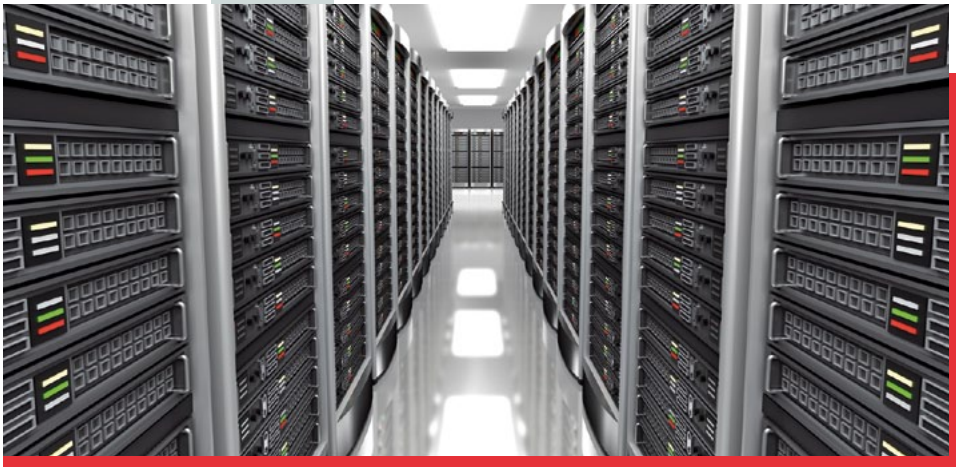
En este ámbito se encuentran las empresas que tienen entre 10 y 250 empleados y un volumen de negocio medio. Tienen su propio equipo técnico y un responsable de seguridad, siendo además los encargados de implantar las soluciones de protección que necesitan en cada momento.
Bajo este ámbito se encuentran las soluciones de seguridad dirigidas a la selección, implementación y operación de las soluciones de seguridad. Se encuentran los servicios que detectan los posibles fallos de seguridad de la infraestructura, y los que proporcionan los recursos necesarios de seguridad y la gestión de los incidentes de seguridad.

GRAN EMPRESA

Las grandes empresas son aquellas cuya estructura organizativa tiene más de 250 empleados, tienen instalaciones propias y su volumen de negocio es muy elevado. Tienen departamentos especializados de seguridad.
Las soluciones de seguridad para este ámbito de aplicación van desde la auditoría, protección, detección y reacción ante incidentes de seguridad. Soluciones de aplicación de medidas de seguridad organizativas, cumplimiento normativo con la legislación, así como la adecuación e implantación de políticas de seguridad corporativas.

INFRAESTRUCTURAS CRÍTICAS

Dentro de este ámbito se encuentran las infraestructuras críticas que son los activos esenciales para el funcionamiento de la sociedad y la economía. Centrales y redes de energía, servicios de transporte, servicios financieros, etc. Estas empresas tienen áreas específicas de ciberseguridad y están protegidas por los organismos públicos.



Dentro de este ámbito se encuentran las infraestructuras críticas que son los activos esenciales para el funcionamiento de la sociedad y la economía.

3 La taxonomía de soluciones de ciberseguridad

3.3.1 Dependencias tecnológicas

Otro factor a tener en cuenta es la dependencia tecnológica de las pymes, se definen tres niveles de dependencia o grados en los que el negocio de una empresa depende de la ciberseguridad. Estos niveles son indicativos de la infraestructura utilizada y de su aplicación en el negocio.

DEPENDENCIA BAJA

En este nivel de dependencia el uso de soluciones de ciberseguridad cumple las siguientes premisas:

- se utilizan ordenadores para realizar trabajos administrativos;
- se utilizan aplicaciones en local para mantenimientos de bases de datos y hojas de cálculo;
- se usa internet para consultas y búsqueda de información;
- es posible que se utilice correo electrónico como medio de comunicación con empresas proveedoras y con clientes, pero no es común que se disponga de servidor de correo;
- puede disponer de una página web informativa (descarga de documentación, información de contacto, etc.) que generalmente se aloja externamente;
- se utiliza la red de área local o wifi para compartir recursos (impresoras, discos, acceso a internet…), pudiendo disponer de un servidor de ficheros.

DEPENDENCIA MEDIA

En este nivel de dependencia el uso de soluciones de ciberseguridad además de las premisas indicadas en nivel anterior también:

- se utilizan herramientas colaborativas en red para gestión del negocio (procesos, rrhh, gestión de clientes, etc.);
- se utiliza internet para potenciar el negocio (*mailings*, publicidad, etc.) y para el cumplimiento de las obligaciones con la administración;
- se dispone de servidores de correo electrónico que se administran localmente o se subcontrata el servicio;
- se usan copias en remoto para salvaguarda de información;
- se utiliza la red de área local para compartir recursos (aplicaciones, ficheros, etc.) con servidores propios;
- su página web cambia con frecuencia de contenidos (noticias, boletines rss, catálogo de productos, etc.) y puede contener servicios interactivos (formularios, etc.);
- es posible que se utilicen dispositivos portátiles para acceso remoto a su red corporativa.

3 La taxonomía de soluciones de ciberseguridad

DEPENDENCIA ALTA

En este nivel de dependencia además de las indicadas en los niveles de dependencia anteriores también:

- se utiliza internet u otras redes para el desarrollo del negocio;
- es posible que disponga de servicios/productos que se distribuyen y/o venden en línea;
- se utiliza el intercambio electrónico para el desarrollo del negocio (contratación, facturación, etc.);
- dispone de una intranet (formación, aplicativos internos, etc.);
- forma redes particulares con sus proveedores y sus clientes (extranet);
- utiliza herramientas colaborativas en su página web;
- tienen en su estructura perfiles técnicos capaces de resolver cualquier incidente;
- en función del tamaño de la empresa y de su dependencia tecnológica podemos seleccionar la mejor herramienta según cada necesidad.

3.4 Taxonomía de soluciones de ciberseguridad

La taxonomía de soluciones de ciberseguridad establece varios niveles, por un lado se clasifican las soluciones en productos y por otro lado en servicios.

Se establece como segundo nivel de clasificación las categorías de las soluciones, tanto de productos como de servicios, adecuadas según el mercado actual de ciberseguridad. Dentro de las categorías, se definen las subcategorías, las cuales están pensadas para que puedan cambiar y adaptarse a los diferentes cambios que se vayan produciendo en el mercado de la seguridad.

En la taxonomía se marca los alcances de las soluciones, permitiendo establecer el área de aplicación para cada categoría de producto o servicio, así como los ámbitos de aplicación, que permiten establecer a quién van dirigidas las soluciones de seguridad, teniendo en cuenta el tamaño y la estructura organizativa.

3.4.1 Taxonomía

Todos los elementos que hemos descrito en los apartados anteriores dan como resultado de su combinación el cuadro final que presentamos a continuación, y que contiene el modelo final de la taxonomía de soluciones de ciberseguridad.

3 La taxonomía de soluciones de ciberseguridad

CATEGORÍA DE PRODUCTO	ÁMBITO DE APLICACIÓN				
	Gestión de acceso e identidad	Seguridad en el puesto de trabajo	Seguridad en aplicaciones y datos	Seguridad en los sistemas	Seguridad en la red
Anti-fraude Anti-*phising*, Anti-spam, Herramientas de filtrado de navegación, UTM, *Appliance*		✓	✓	✓	✓
Anti-malware Anti-virus, Anti-*Adware*, Anti-*spyware*, UTM, *Appliance*		✓	✓	✓	✓
Auditoría técnica Análisis de logs y puertos, vulnerabilidades, Auditoría de contraseñas, Auditoría de sistemas y ficheros	✓		✓		✓
Certificación normativa SGSI, Análisis de riesgos, Planes y políticas de seguridad, Normativas de seguridad		✓	✓	✓	✓
Contingencia y continuidad H. de gestión de planes de contingencia y continuidad, Copias de seguridad, Infraestructura de respaldo, Virtualización, *Cloud*		✓	✓	✓	✓
Control de acceso y autenticación Control de acceso a red, NAC, Gestión de identidad y autenticación, *Single Sign-On,* Certificados digitales, Firma electrónica	✓				
Cumplimiento legal Herramientas de cumplimiento legal (LOPD, LSSI,...), Borrado seguro, Destrucción documental	✓	✓	✓		
Inteligencia de seguridad Gestión de eventos de seguridad, SIM/SIEM, *Big Data,* Herramientas de monitorización y *reporting*			✓	✓	✓
Prevención de fuga de información Control de contenidos confidenciales, Gestión del ciclo de vida de la información, Herramientas de cifrado		✓	✓		✓
Protección de las comunicaciones Cortafuegos *(firewall)*, VPN, IDS, IPS, UTM, *Appliance,* Filtro de contenidos, P2P, Gestión y control de ancho de banda		✓	✓	✓	✓
Seguridad en dispositivos móviles Seguridad para dispositivos móviles, Seguridad para redes inalámbricas, BYOD		✓			✓

3 La taxonomía de soluciones de ciberseguridad

CATEGORÍA DE SERVICIO	ÁMBITO DE APLICACIÓN: Personas	Información	Infraestructuras	Negocio
Auditoría técnica test de intrusión, *hacking* ético, análisis de vulnerabilidades, ingeniería de seguridad, auditorías de código, auditoría forense		✓	✓	
Certificación de normativa SGSI, certificación y acreditación, planes y políticas de seguridad, análisis de riesgos	✓	✓	✓	✓
Contingencia y continuidad copias de seguridad remotas (backup), planes de contingencia, centros de respaldo				✓
Cumplimiento legal consultoría legal, auditoría de legislación, borrado seguro, destrucción documental	✓	✓	✓	
Formación y concienciación formación en materia de ciberseguridad, certificación profesional, sensibilización y concienciación	✓			
Gestión de incidentes prevención, detección, respuesta a incidentes de seguridad	✓	✓	✓	
Implantación de soluciones soluciones de ciberseguridad, ciber-resilencia, ciberseguridad industrial			✓	
Seguridad en la nube *software* como servicio (SaaS), plataforma como servicio (PaaS), infraestructura como servicio (IaaS)		✓	✓	✓
Soporte y mantenimiento seguridad gestionada, *outsourcing* de personal, externalización de servicios		✓	✓	

4 Fichas de productos de ciberseguridad

A continuación, se describen las fichas de las categorías de productos consideradas:

4.1 Anti-fraude

DESCRIPCIÓN - ¿Qué es?

Las soluciones Anti-Fraude están destinadas a proteger a los usuarios de todo tipo de ingeniería social. Uno de los objetivos de la ingeniería social es realizar actividades fraudulentas en internet, como el robo de información personal o datos bancarios, suplantación de identidad y otras. Todas ellas llevadas a cabo mediante técnicas como el *phishing,* el correo electrónico no deseado (*spam*) o el *malware* diseñado al efecto.

El fraude *on-line* es una amenaza de amplio espectro, puesto que hace uso de múltiples técnicas, vías de entrada, servicios en internet o *malware,* pero sobre todo se basa en explotar la confianza de los usuarios, en base a la dificultad que tienen estos en diferenciar aquello que es legítimo de lo que no lo es.

SUBCATEGORÍAS - ¿Tipos?

Podemos encontrar las siguientes subcategorías dentro de los productos anti-fraude:

- **Anti-*phishing***
  Protegen del fraude iniciado a través del correo electrónico. Son comunicaciones destinadas a engañar a un usuario para conectar a un servicio fraudulento con el fin de obtener información de pago o credenciales de acceso al servicio legítimo.
- **Anti-spam**
  Son herramientas destinadas a filtrar el correo electrónico no deseado, también llamado correo basura.
- **Herramientas de filtrado de navegación**
  Son herramientas destinadas a proteger al usuario durante la navegación en internet, controlando los sitios a los que se accede mediante listas, reputación u otras.
- **UTM, *Appliance* (*Unified Threat Management*)**
  Gestión Unificada de Amenazas, son dispositivos de seguridad en forma de Appliance que proporcionan varias funciones de seguridad en un único dispositivo. Suelen incluir funciones de anti-virus, anti-spam, *firewall* de red, detección y prevención de intrusiones, filtrado de contenidos y prevención de fuga de información.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones anti-fraude:

- usar los certificados digitales que nuestra página web o tienda online utilice en el protocolo https con un certificado emitido por una entidad de confianza;
- implementar medios de pago que nos protejan en la medida de lo posible contra el fraude;
- realizar comprobaciones sobre los pedidos, de modo que podamos mitigar en la medida de lo posible la gestión y envío de un pedido fraudulento;
- concienciar a nuestros empleados para que hagan un correcto uso de los sistemas corporativos: que no instalen *software* sin autorización, ni naveguen por páginas web de contenido dudoso y, en general, que se cumpla todo lo establecido en la política de seguridad de la empresa;
- detectar posibles copias o usos no autorizados de las marcas o distintivos comerciales;
- proteger las cuentas con contraseñas complejas. cambiar las claves de manera periódica.

USO - Escenario de aplicación

Son productos destinados a la protección general contra el fraude *on-line,* mejorando enormemente la seguridad en todo tipo de transacciones electrónicas, pero también en el uso diario de Internet, con servicios habituales como el correo electrónico, los portales web, o la mensajería instantánea.
Son herramientas con un ámbito de utilización muy amplio, desde la protección de un puesto de trabajo, hasta la seguridad de aplicaciones, sistemas y redes.
Se recomienda su uso en aquellos escenarios en los que se realizan transacciones electrónicas en Internet, en particular banca electrónica o comercio electrónico, ya sea entre empresas o particulares.

El fraude on-line es una amenaza de amplio espectro, puestos que hace uso de múltiples técnicas.

4.2 Anti-malware

DESCRIPCIÓN - ¿Qué es?

Son herramientas destinadas a la protección de sistemas informáticos: servidores, ordenadores de sobremesa, portátiles, dispositivos móviles, etc., frente a todo tipo de *software* malicioso que pueda afectarles (virus, troyanos, gusanos, spyware, etc.). Detectan y eliminan todo tipo de malware.
El software malicioso o *malware* es una amenaza que tiene como objetivo dañar el dispositivo para obtener un beneficio. El *malware* es una amenaza de amplio espectro, puesto que hace uso de amplias técnicas y vías de entrada, como páginas web, correos electrónicos, dispositivos de almacenamiento, etc. siendo elementos utilizados para infectar y propagar el código malicioso.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos anti-*malware*:

- **Anti-virus**
  Son herramientas cuyo objetivo es detectar y eliminar virus. Con la aparición de Internet, ha hecho que los anti-virus hayan evolucionado hasta programas más avanzados, que no solo buscan detectar y eliminar los virus, sino bloquearlos, desinfectar archivos y prevenir una infección de los mismos.
- **Anti-*adware***
  Son herramientas anti-*malware* destinadas a detectar anuncios publicitarios no deseados, que pueden llegar a cambiar la configuración del navegador para dirigirnos a sitios web que no hemos solicitado. Este *malware* ralentiza internet y el sistema.
- **Anti-*spyware***
  Son herramientas anti-*malware* centradas en la lucha contra los programas creados con fines de marketing o publicitarios que suelen terminar en los ordenadores de los usuarios por el simple hecho de navegar o usar el correo electrónico.
- **UTM, *Appliance* (*Unified Threat Management*)**
  Gestión Unificada de Amenazas, son dispositivos de seguridad en forma de Appliance que proporcionan varias funciones de seguridad en un único dispositivo. Suelen incluir funciones de anti-virus, anti-spam, *firewall* de red, detección y prevención de intrusiones, filtrado de contenidos y prevención de fuga de información.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones anti-*malware:*

- mantener los sistemas actualizados y libres de virus y vulnerabilidades. de este modo estaremos protegidos frente ataques, *malware,* etc;
- concienciar a nuestros empleados para que hagan un correcto uso de los sistemas corporativos: que no instalen *software* sin autorización, ni naveguen por páginas web de contenido dudoso y, en general, que se cumpla todo lo establecido en la política de seguridad de la empresa;
- mantener actualizado los sistemas operativos y aplicaciones;
- evitar la descarga e instalación de programas desde sitios web que no ofrezcan garantías;
- utilizar redes seguras para todas las comunicaciones con nuestros clientes. y emplear cifrado cuando la información intercambiada sea especialmente sensible;
- realizar copias periódicas de seguridad que incluyan los datos del cliente que debamos proteger. también debemos tener procedimientos de restauración de dichas copias.

USO - Escenario de aplicación

Son herramientas con un ámbito de utilización muy amplio, desde protección de un puesto de trabajo o un único usuario, hasta la protección de una organización completa.
Se recomienda su uso en todo tipo de sistemas informáticos, ya sean servidores, dispositivos de sobremesa o portátiles, incluyendo PDAs y *Smartphones*. Se recomienda también su uso en aquellos escenarios en los que se realiza un uso intensivo de Internet y del correo electrónico, y el intercambio frecuente ficheros o de memorias USB (*pendrives*).

El software malicioso o malware es una amenaza que tiene como objetivo dañar el dispositivo para obtener un beneficio.

4.3 Auditoría técnica

DESCRIPCIÓN - ¿Qué es?

Son herramientas que abarcan desde la revisión hasta la evaluación de la seguridad desde todos los ámbitos técnicos, tecnológicos y organizativos de la seguridad. La constante evolución de las metodologías y técnicas de auditoría, permiten a estas herramientas la revisión de cualquier tecnología existente en el mercado, de cualquier infraestructura sensible de sufrir deficiencias de seguridad y de ser vulnerable.

Están destinadas a la realización de auditorías de sistemas, aplicaciones y datos, siendo herramientas de prevención, determinando posibles fallos de seguridad. Se incluyen las herramientas de auditoría forense, que determinan qué ocurrió ante un caso de incidente de seguridad.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos de auditoría técnica:

- **Análisis de *logs* y puertos**
  Son herramientas destinadas a analizar los registros de actividad que se almacenan, con el fin de determinar la causa de un incidente de seguridad.
- **Análisis de vulnerabilidades**
  Son herramientas de auditoría que permiten identificar las vulnerabilidades de sistemas y aplicaciones, así como otros agujeros de seguridad.
- **Auditoría de contraseñas**
  Son aplicaciones diseñadas para realizar análisis de contraseñas, estableciendo el cumplimiento de políticas de seguridad de cualquier organización, detectando contraseñas débiles o que no cumplen dicha política.
- **Auditoría de sistemas y ficheros**
  Son herramientas destinadas a registrar y analizar la actividad sobre ficheros y datos de los sistemas.
- **Auditoría de red**
  Son herramientas que permiten detectar, evaluar y remediar cualquier vulnerabilidad de seguridad en la red. Realizan auditorías completas de las infraestructuras de comunicaciones.
- **Herramientas de recuperación de datos**
  Son herramientas que recuperan rastros de un incidente que hayan podido ser eliminados de forma intencionada o accidental.
- **Herramientas de testeo de *software*/aplicaciones web**
  Son herramientas que permiten obtener un mejor rendimiento de las aplicaciones y optimizan la calidad final.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones anti-*malware*:

- mantener estas herramientas actualizadas;
- mantener los sistemas actualizados y libres de virus y vulnerabilidades. de este modo estaremos protegidos frente ataques, *malware*, etc;
- tener empresas y profesionales especializados, a la hora de obtener información fidedigna y contrastada sobre la situación de la seguridad en su organización, o sobre un incidente de seguridad;
- concienciar a nuestros empleados para que hagan un correcto uso de los sistemas corporativos: que no instalen *software* sin autorización, ni naveguen por páginas web de contenido dudoso y, en general, que se cumpla todo lo establecido en la política de seguridad de la empresa.

USO - Escenario de aplicación

Son herramientas utilizadas en todo tipo de organizaciones con infraestructuras, donde deban llevarse a cabo auditorías internas de seguridad, permitiendo realizar una valoración del estado de la seguridad y también puedan analizar incidentes de seguridad, con el objetivo de conocer la causa.
En aquellas organizaciones donde se haya implantado un SGSI o se haya realizado una adecuación a algún tipo de normativa o legislación, es muy importante contar con mecanismos de registro de la actividad, no solo en los sistemas, sino también de los procesos y actividades.

Herramientas destinadas a la realización de auditorías de sistemas, aplicaciones y datos, siendo herramientas de prevención.

4.4 Certificación normativa

DESCRIPCIÓN - ¿Qué es?

Son herramientas destinadas a facilitar el cumplimiento normativo aplicable en materia de seguridad y la obtención de certificados en esas normativas.
Posibilitan la implementación de políticas de seguridad, la realización de análisis de riesgos, la valoración de activos, la implantación de medidas de seguridad, la verificación y el cumplimiento de las políticas y medidas establecidas.
En este grupo se incluyen las herramientas de Gestión de Riesgos, así como los Sistemas de Gestión de Seguridad de la Información (SGSI), los planes y las políticas de seguridad.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos cumplimiento legal:

- **Sistemas de Gestión de la Seguridad de la Información (SGSI)**
  Es el conjunto de procesos para la gestión de la accesibilidad de la información. Estas herramientas buscan minimizar los riesgos de seguridad de la información. El estándar utilizado es la norma ISO/IEC 27001.
- **Análisis de riesgos**
  Son herramientas destinadas a facilitar el cumplimiento e implantación de la normativa en materia de seguridad. Tiene la finalidad de detectar los activos y procesos críticos y conocer sus vulnerabilidades y amenazas.
- **Planes y políticas de seguridad**
  Son herramientas que consisten en la definición y priorización de un conjunto de proyectos en materia de seguridad dirigido a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.
- **Normativas de seguridad**
  Son herramientas destinadas a facilitar el cumplimiento normativo aplicable en materia de seguridad y la obtención de certificados en esas normativas.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de certificación normativa:

- desarrollar políticas de seguridad en las que se valoren los riesgos a los que están expuestos los sistemas de información;
- contar con servicios de consultoría previos a la implantación de cualquier herramienta asociada a esta categoría, debido a la complejidad a la hora de abordar cualquier proceso de adecuación y cumplimiento de normativa;
- establecer rutinas de gestión de la seguridad y verificar su cumplimento para minimizar riesgos de seguridad.

USO - Escenario de aplicación

Para cualquier proceso de adecuación y cumplimiento normativo es necesario contar con servicios de consultoría previos a la implantación de cualquier herramienta de esta categoría.
Estas herramientas establecen rutinas de gestión de la seguridad y verifican su cumplimiento para minimizar riesgos y amenazas de seguridad.

Herramientas de Gestión de Riesgos, así como de Sistemas de Gestión de Seguridad de la Información.

4.5 Contingencia y continuidad

DESCRIPCIÓN - ¿Qué es?

Son herramientas cuyo objetivo es planificar planes de actuación y contingencia destinados a mitigar el impacto provocado por cualquier incidente de seguridad, constituidos por un conjunto de recursos de respaldo y procedimientos de actuación, encaminados a conseguir una restauración ordenada y progresiva de los sistemas y los procesos de negocio considerados críticos en cualquier organización.

Están muy enfocadas a la recuperación ante desastres e incidentes de seguridad, la externalización se ha convertido en un elemento fundamental de este tipo de herramientas, como las soluciones de copia de seguridad remota, la virtualización, así como la seguridad en la nube *(cloud computing)*. Estas herramientas llevan a cabo una reducción de tiempos de despliegue y puesta en marcha de infraestructuras de respaldo.

Es necesario proteger los principales procesos de negocio a través de un conjunto de tareas que permita a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. De esta forma se garantiza puede dar una respuesta planificada ante cualquier fallo de seguridad. Esto repercutirá positivamente en el cuidado de nuestra imagen y reputación como empresa, además de mitigar el impacto financiero y de pérdida de información crítica ante estos incidentes

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos de contingencia y continuidad:

- gestión de planes de contingencia y continuidad. Tienen como objetivo gestionar de la manera óptima en tiempo y forma una situación de crisis no prevista, reduciendo así los tiempos de recuperación y vuelta a la normalidad;
- herramientas de recuperación de sistemas. Son herramientas destinadas a posibilitar una rápida recuperación de los sistemas y las aplicaciones ante un posible incidente de seguridad;
- copias de seguridad. Son herramientas destinadas al almacenamiento de datos o información con el fin de disponer de un medio para poder recuperarlos en caso de pérdida accidental o intencionada;
- infraestructura de respaldo. Son herramientas destinadas a posibilitar el despliegue rápido de infraestructura de respaldo en caso de pérdida, con el objetivo de reducir al mínimo los tiempos de interrupción de la actividad;
- seguridad en Virtualización. Dentro de estas herramientas se engloban los mecanismos y tecnologías que aportan seguridad a los sistemas virtualizados.

- Herramientas en la nube. Son las plataformas tecnológicas que permiten configurar y utilizar recursos tanto *hardware, software* y comunicaciones en un tiempo mínimo para la recuperación en caso de incidente de seguridad. Se caracterizan por la transparencia para el usuario y el acceso remoto desde cualquier lugar y dispositivo.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de contingencia y continuidad:

- realizar copias periódicas de seguridad. También debemos tener procedimientos de restauración de dichas copias;
- identificar los servicios y procesos críticos junto con los activos tecnológicos que los sustentan y sus dependencias;
- elaborar el plan de crisis para identificar las primeras acciones a realizar cuando ocurre un incidente;
- concienciar a nuestros empleados para que hagan un correcto uso de los sistemas corporativos: que no instalen *software* sin autorización, ni naveguen por páginas web de contenido dudoso y, en general, que se cumpla todo lo establecido en la política de seguridad de la empresa.

USO Escenario de aplicación

Estas herramientas son de uso generalizado y recomendado en cualquier organización que utilice o cuyos procesos de negocio dependan del uso de sistemas de información. Organizaciones y empresas de cualquier tamaño.
Son recomienda utilizar productos y herramientas de copias de seguridad como medida básica y fundamental en seguridad.

Herramientas muy enfocadas a la recuperación ante desastres e incidentes de seguridad.

4.6 Control de acceso y autenticación

DESCRIPCIÓN - ¿Qué es?

Son productos destinados a dotar a las empresas y organizaciones de mecanismos que permitan gestionar usuarios y sus datos de identificación; asociar roles, perfiles y políticas de seguridad; y controlar el acceso a los recursos. Suelen estar integrados con mecanismos de autenticación que posibilitan el control del acceso lógico de los usuarios en los sistemas informáticos.
Herramientas destinadas al uso y utilización de certificados digitales que aportan mayor seguridad a procesos, aplicaciones y sistemas. Los certificados digitales se usan con las tarjetas inteligentes *"Smart card"* en la cuales se pueden almacenar certificados digitales. El DNIe es un ejemplo de tarjeta inteligente que incluye certificados digitales para autenticación y firma.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos acceso e identidad:

- **Control de acceso a red (*Network Access Control, NAC*)**
  Son herramientas destinadas a proporcionar mecanismos para administrar y controlar el acceso de usuarios a una red. Aplican configuraciones y soluciones de seguridad para aumentar la disponibilidad de red y el cumplimiento normativo.
- **Gestión de identidad y autenticación**
  Son herramientas destinadas a verificar la identidad de un usuario, permiten realizar la autenticación y autorización a los sistemas y recursos de una organización.
- **Herramientas *Single Sign-On***
  Son herramientas de autenticación que habilitan el acceso a varios sistemas con una sola instancia de identificación.
- **Certificados digitales**
  Son herramientas que permiten autentificar y garantizar la confidencialidad de las comunicaciones a través de redes, asociando unos datos de identidad a una persona física, organismo o empresa confirmando su identidad digital en internet, evitando suplantaciones.
- **Firma electrónica**
  Son herramientas que permiten firmar todo tipo de documentos electrónicos, identificando al firmante de manera inequívoca y asegurando la integridad de los documentos firmados.
- **Tarjetas inteligentes y dispositivos biométricos**
  Son herramientas que permiten la autenticación e identificación de usuarios mediante el uso de lectores de tarjetas o lectores de huella digital.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de control de acceso y autenticación:

- actualizar frecuente del producto;
- utilizar redes seguras para todas las comunicaciones con nuestros clientes. Y emplear cifrado cuando la información intercambiada sea especialmente sensible;
- mantener nuestros sistemas actualizados y libres de virus y vulnerabilidades. De este modo estaremos protegidos frente a ataques, *malware,* etc;
- proteger las cuentas con contraseñas complejas. Cambiar las claves de manera periódica;
- mantener réplicas de los repositorios de identidad y que tengan una alta disponibilidad;
- incluir una adecuada política de seguridad para la gestión de los certificados digitales, así como para la gestión de las claves y contraseñas asociadas a estos.

USO - Escenario de aplicación

Es recomendable para todo tipo de empresas, son herramientas dirigidas a la gestión de los accesos e identidades para su seguridad. Donde exista una necesidad de identificar personas u organizaciones de forma segura en un entorno digital.
Donde sea necesario implementar tramitación electrónica que incluya capacidades de firma, envío de documentación. Se utilizan para mejorar el cumplimiento de la normativa y la legislación.
Para la firma de documentos digitales, correos electrónicos u otro tipo de contenidos.
Mantenimiento de la integridad y confidencialidad de archivos y documentos.

Productos que dotan a las empresas y organizaciones de mecanismos que permitan gestionar, entre otras cosas, usuarios y sus datos de indentificación.

4.7 Cumplimiento legal

DESCRIPCIÓN - ¿Qué es?

Son herramientas destinadas a facilitar el cumplimiento legal, aplicable en materia de seguridad de la información, como es el caso de la Ley Orgánica de Protección de Datos (LOPD) en organizaciones y empresas.

Estas normas se desarrollan con el objetivo de proteger el interés general mostrando las buenas prácticas para garantizar y proteger los derechos fundamentales de los ciudadanos. Proporcionan guías o instrucciones en forma de procesos estándares desde el punto de vista de la implementación de medidas destinadas al cumplimiento legal.

En este grupo se incluyen las herramientas que facilitan el cumplimiento con la legislación en materia de protección de datos de carácter personal (LOPD), comercio electrónico (LSSI), el borrado y la destrucción de información de forma segura y cumpliendo con la normativa vigente.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos cumplimiento legal:

- **Herramientas de Cumplimiento legal (LOPD, LSSI, etc.)**
  Estas herramientas permiten el cumplimiento con la legislación en materia de seguridad de la información.
  Se encuentra la LOPD (Ley Orgánica de Protección de Datos), LSSI (Ley de Servicios de la Sociedad de la información), LPI (Ley de Propiedad Intelectual), etc.
- **Borrado seguro**
  Son herramientas que permiten realizar la eliminación de archivos, carpetas o unidades lógicas de forma segura.
- **Destrucción documental**
  Son herramientas destinadas a la destrucción de datos confidenciales y documentos.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de cumplimiento legal:

- contar con servicios de consultoría previos a la implantación de cualquier herramienta asociada a esta categoría, debido a la complejidad a la hora de abordar cualquier proceso de adecuación y cumplimiento de normativa y de legislación;
- desarrollar políticas de seguridad en las que se valoren los riesgos a los que están expuestos los sistemas de información que sustentan su negocio;
- establecer rutinas de gestión de la seguridad y verifique su cumplimento para minimizar riesgos de seguridad.

USO - Escenario de aplicación

Para cualquier proceso de adecuación y cumplimiento legal es necesario contar con servicios de consultoría previos a la implantación de cualquier herramienta de esta categoría.
Estas herramientas establecen rutinas de gestión de la seguridad y verifican su cumplimiento para minimizar riesgos y amenazas de seguridad.

Herramientas que facilitan el cumplimiento legal, aplicable en materia de seguridad de la información, como es el caso de la Ley Orgánica de Protección de Datos (LOPD) en organización y empresas.

4.8 Inteligencia de seguridad

DESCRIPCIÓN - ¿Qué es?

Son herramientas que permiten llevar a cabo la gestión de eventos o incidentes de ciberseguridad en cualquiera de sus fases, ya sea antes, durante o después de que se produzca el incidente. El objetivo es obtener información y ayudar a detectar las amenazas de forma rápida, identificar vulnerabilidades, priorizar riesgos y automatizar actividades de cumplimiento normativo.

Permiten establecer un flujo para la gestión de eventos de seguridad de forma que sea posible tratar los incidentes de forma organizada y siguiendo procedimientos cuyo objetivo sea la resolución en el menor tiempo posible y con las menores consecuencias.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos gestión de eventos:

- **Gestión de eventos de seguridad, SEM *(Security Event Management)***
  Son herramientas destinadas a dar respuesta a incidentes de seguridad, apoyando a las organizaciones en cualquiera de las fases de un evento Están enfocados en la recopilación, análisis en tiempo real, correlación y detección de anomalías de eventos, permitiendo realizar una trazabilidad completa de la actividad de forma sencilla.
- **SIM / SIEM**
  Son herramientas de gestión y análisis de logs, para la protección de activos e información frente a amenazas. Reúnen datos de los eventos, de las amenazas y de los riesgos para proporcionar la mayor información de la seguridad, para poder lograr respuestas rápidas a los incidentes, gestionar los registros de forma sencilla y generar informes de cumplimiento.
- ***Big Data***
  Son herramientas de tratamiento de grandes volúmenes de datos para sacar información concreta y útil en función de unas reglas definidas.
- **Herramientas de monitorización y *reporting***
  Son herramientas de vigilancia que permiten identificar y resolver problemas de infraestructura antes de que afecten a procesos críticos, controlando la seguridad de red. Pueden generar informes y reportes que aportan información muy precisa del estado actual, para actuar en caso de un posible incidente de seguridad.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de inteligencia de seguridad:

- actualizar frecuente el producto.
- mantenimiento continuo debido a que interactúan con distintos tipos de infraestructuras es fundamental que estas herramientas sean revisadas y se mantengan actualizadas constantemente.

USO - Escenario de aplicación

Es recomendable en organizaciones y empresas de gran tamaño, allí donde existan procesos y actividades críticas e importantes para el buen funcionamiento.
Son fundamentales en organizaciones que cuenten con infraestructuras tecnológicas importantes, puesto que ayudan a la gestión de todos los aspectos relativos a la seguridad, minimizando cualquier incidente.

Las herramientas de monitorización y reporting permiten identificar y resolver problemas de infraestructura antes de que afecten a procesos críticos.

4.9 Prevención de fuga de información

DESCRIPCIÓN - ¿Qué es?

Son herramientas que garantizan la confidencialidad, la disponibilidad y la integridad de la información. Evitan la pérdida de la información a través de diferentes medios como el correo electrónico, transferencias de ficheros, dispositivos externos de almacenamiento (memorias USB), etc.
Tienen la función de identificar, monitorizar, detectar y prevenir fugas de información desde y hacia el exterior de la organización, implementando políticas de uso de la información, de los dispositivos y periféricos.
Se incluyen en estas herramientas aquellos sistemas que gestionan el ciclo de vida de la información, controlando el uso autorizado de documentos electrónicos, así como herramientas de cifrado de la información, que impiden el uso indebido por accesos no autorizados y permiten el intercambio de información de forma segura, protegiendo la integridad de la información.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos de control de contenidos confidenciales:

- **Control de contenidos confidenciales**
  Son herramientas que impiden y evitan la transferencia de datos no autorizados y la fuga de información confidencial.
- **Gestión del ciclo de vida de la información (*ILM: Information Life Cicle*)**
  Son herramientas que permiten gestionar el ciclo completo de vida de la información, implementando políticas y mecanismos para garantizar el nivel de confidencialidad de la información.
- **Control de dispositivos externos de almacenamiento**
  Son herramientas destinadas a controlar el acceso físico de puertos y otros dispositivos extraíbles (memorias USB), para evitar el robo de información.
- **Herramientas de encriptación**
  El cifrado consiste en ofuscar la información mediante técnicas de codificación, evitando que los datos sean accesibles por cualquier persona que desconozca la clave de decodificación.
- **Cifrado de discos duros y soportes de almacenamiento**
  Son herramientas destinadas a la encriptación de todo tipo de soportes de almacenamiento, discos duros y memorias USB.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de prevención de fugas de información:

- identificar los datos de carácter personal y los documentos confidenciales que desea proteger;
- concienciar a nuestros empleados para que hagan un correcto uso de los sistemas corporativos: que no instalen *software* sin autorización, ni naveguen por páginas web de contenido dudoso y, en general, que se cumpla todo lo establecido en la política de seguridad de la empresa;
- realizar copias periódicas de seguridad. También debemos tener procedimientos de restauración de dichas copias;
- proteger las cuentas con contraseñas complejas. Cambiar las claves de manera periódica;
- identificar los usuarios autorizados y definir los privilegios para el uso de datos y documentos confidenciales.

USO - Escenario de aplicación

Son herramientas indicadas para cualquier organización, en especial aquellas que tratan información de carácter personal, la cual está sometida a una regulación específica y de cumplimiento normativo.
También son muy recomendables en aquellas empresas que dispongan de equipos y personal externos que trabajan con datos confidenciales.
Se recomienda el uso de sistemas y herramientas criptográficas para cualquier tipo de empresa, para la protección de la información y de las comunicaciones, cuando se lleven transacciones electrónicas o intervenga cambio de información, así como cuando se trasmita la información a través de correo electrónico.
Su uso es fundamental para el cifrado de información confidencial almacenada en soportes o dispositivos de almacenamiento tanto fijos como extraíbles.

4.10 Protección de las comunicaciones

DESCRIPCIÓN - ¿Qué es?

Son productos destinados a proteger los sistemas y dispositivos conectados a una red. Herramientas que permiten establecer un perímetro de seguridad y garantizan las comunicaciones seguras para evitar accesos no autorizados y ataques provenientes de redes externas y de internet.

Son herramientas destinadas al control de la actividad de las infraestructuras de comunicaciones de una organización con distintos objetivos: cumplimiento de políticas de seguridad de la organización, seguridad perimetral y disponibilidad y uso adecuado de los recursos.

Permiten controlar el tráfico generado y recibido, realizando un control sobre el uso de ancho de banda, el tráfico y el rendimiento. Esta categoría agrupa a productos que aseguran las comunicaciones hacia y desde la red, cumplen las políticas de seguridad establecidas. Para ello rastrean y controlan las comunicaciones, bloqueando el tráfico, detectando comportamientos anómalos y ataques y evitando intrusiones no autorizadas.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos cortafuegos:

- **Cortafuegos (*firewall*)**
  Son herramientas que bloquean el acceso no autorizado a una red. También impiden que los equipos envíen *software* malintencionado a otros equipos.
- **Redes privadas virtuales o VPN (*Virtual Private Network*)**
  Son herramientas que permiten crear una conexión segura con otra red a través de internet mediante la creación de túneles cifrados, ofreciendo acceso inalámbrico seguro a los recursos de la red corporativa.
- **UTM, Appliance (*Unified Threat Management*), Gestión Unificada de Amenazas**
  Son dispositivos de seguridad en forma de Appliance que proporcionan varias funciones de seguridad en un único dispositivo. Suelen incluir funciones de antivirus, anti-spam, *firewall* de red, detección y prevención de intrusiones, filtrado de contenidos y prevención de fuga de información.
- **Prevención y detección de intrusiones IPS / IDS (*Intrusion Prevention System / Intrusion Detection System*)**
  Son herramientas para detectar y prevenir accesos no autorizados a un equipo o a una red. Monitorizan el tráfico para determinar y prevenir comportamientos sospechosos. Se integran con frecuencia con cortafuegos para proteger la red y los accesos no autorizados.

- **Cifrado de las comunicaciones**
  Son herramientas destinadas al cifrado de la información en tránsito en aplicaciones de mensajería instantánea, correo electrónico, navegación web, etc. Permiten ocultar la información en mensajes y ficheros adjuntos para que se puedan enviar de forma segura.
- **Filtro de contenidos**
  Son herramientas para controlar, restringir y limitar el acceso a contenidos web, evitando el acceso a sitios peligrosos o de dudosa credibilidad. Configuran condiciones de acceso a internet a través de navegadores.
- **Herramientas de control P2P (*peer-to-peer*)**
  Son herramientas que bloquean y controlan el tráfico a través de redes P2P. Impiden y restringen el acceso por parte de los usuarios, controlando el tipo de información transmitida.
- **Gestión y control de ancho de banda**
  Son herramientas destinadas a uso eficiente y adecuado del ancho de banda disponible, facilitando una mejor fluidez de los datos y un mejor aprovechamiento de los recursos de la red.
- **Herramientas de monitorización y *reporting***
  Son herramientas de vigilancia que permiten identificar y resolver problemas de infraestructura antes de que afecten a procesos críticos, controlando la seguridad de red. Pueden generar informes y reportes que aportan información muy precisa del estado actual, para actuar en caso de un posible incidente de seguridad.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de protección de las comunicaciones:

- Mantener nuestros sistemas actualizados y libres de virus y vulnerabilidades. De este modo estaremos protegidos frente a ataques, *malware,* etc.
- Utilizar redes seguras para todas las comunicaciones con nuestros clientes. Y emplear cifrado cuando la información intercambiada sea especialmente sensible.
- Monitorizar la red y su ancho de banda para detectar el uso de programas de compartición de ficheros no autorizados.
- Implantar políticas de seguridad, diseñadas y adaptadas para su organización.

USO - Escenario de aplicación

Es recomendable para todo tipo de empresas que dispongan de infraestructuras de comunicaciones, como una red corporativa o una intranet.
Son herramientas que podemos encontrar en cualquier dispositivo con capacidad de conectarse a redes. Para infraestructuras que sean necesarias realizar la monitorización de equipos y sistemas de comunicaciones.

4.11 Seguridad en dispositivos móviles

DESCRIPCIÓN - ¿Qué es?

Son herramientas destinadas a la protección de redes inalámbricas y dispositivos móviles o de dispositivos en movilidad, de forma que se minimicen o reduzcan los incidentes de seguridad.
Así mismo, protegen no solo a dispositivos en movilidad, sino que proporcionan protección y seguridad a aquellos dispositivos e infraestructuras a las cuales se conectan dichos dispositivos, proporcionando mecanismos de acceso y autenticación que posibilitan el uso de redes de comunicaciones desde cualquier localización o situación de forma segura.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los productos de seguridad en dispositivos móviles:

- **Seguridad para dispositivos móviles**
  Son herramientas destinadas a proteger la información, como las aplicaciones y sistemas de estos dispositivos. Incorporar mecanismos de protección contra *malware,* copias de seguridad, protección de las comunicaciones, cifrado de los datos almacenados en el dispositivo para salvaguardar la información.
- **Seguridad para redes inalámbricas**
  Son herramientas destinadas a proteger el acceso y la conexión a redes inalámbricas, incorporando mecanismos de control de acceso, encriptación y otros.
- **BYOD**
  Son herramientas basadas en tecnologías de gestión de movilidad que permiten la protección de estos dispositivos. Incorporan mecanismos de autenticación accediendo a las aplicaciones y datos en cualquier dispositivo.

RECOMENDACIONES

Recomendaciones a tener en cuenta en relación a las soluciones de seguridad en dispositivos móviles:

- adoptar medidas de seguridad que garanticen la autenticación de usuario, la integridad de los datos y la confidencialidad de las comunicaciones.
- desarrollar una política de seguridad para la movilidad en toda la empresa y concienciar a los empleados para que cumplan las directivas de seguridad.
- proteger las redes inalámbricas de la organización.
- establecer una política de uso del byod corporativa en la que se establezcan los usos permitidos y las restricciones con respecto al uso de los dispositivos personales.
- utilizar redes seguras para todas las comunicaciones con nuestros clientes. y emplear cifrado cuando la información intercambiada sea especialmente sensible.

USO - Escenario de aplicación

Son recomendables estas herramientas para cualquier tipo de empresa, que dispongan de dispositivos de movilidad o inalámbricos y que necesiten conectarse a la red corporativa.
Se usan estas herramientas para la protección de la información de los dispositivos móviles ante el riesgo de robo o de perdida, cuando esta información sea sensible o de importancia para la organización, no solo desde el punto de vista de que esta se pueda perder, sino también teniendo en cuenta que esta puede terminar en manos de terceros.

Protegen tanto a los dispositivos móviles como a aquellos dispositivos e infraestructuras a las cuales se conectan.

5 Fichas de servicios de ciberseguridad

A continuación se describen las fichas de las categorías de servicios consideradas:

5.1 Auditoría técnica

DESCRIPCIÓN - ¿Qué es?

Son servicios destinados a la realización de auditorías de seguridad de carácter técnico que permiten analizar y establecer el nivel real de seguridad. La información obtenida de estas auditorías es muy valiosa, permite detectar vulnerabilidades y posibles amenazas de seguridad, estableciendo planes destinados a mejorar su nivel de seguridad.

También se incluyen en esta categoría los servicios destinados a la realización de auditorías posteriores a un evento o incidente de seguridad, para establecer las causas y las consecuencias reales del mismo.

Además están los servicios cuyo objetivo es la actualización sistemática y automatizada de sistemas y aplicaciones, dirigida a la aplicación de parches y medidas para eliminar vulnerabilidades y fallos de seguridad.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de auditoría técnica:

- **Test de intrusión**
  Son servicios de evaluación de la seguridad de los sistemas de protección perimetral así como los sistemas que están accesibles desde internet.
- ***Hacking* ético**
  Son servicios de auditoría para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y tomar medidas correctoras.
- **Análisis de vulnerabilidades**
  Son servicios de auditoría que permiten conocer las vulnerabilidades de sistemas y aplicaciones, así como contraseñas débiles u otros agujeros de seguridad.
- **Ingeniería de seguridad**
  Son servicios de estudio previo de la seguridad, donde se analizará el estado actual y se obtendrá la información necesaria para diseñar una solución a medida.
- **Auditorías de código**
  Son servicios destinados a identificar las posibles vulnerabilidades de un programa, servicio o aplicación. Permiten conocer el nivel de seguridad de las aplicaciones utilizadas en sus sistemas de información.
- **Auditoría de seguridad web**
  Son servicios destinados a dar a conocer el estado en el que se encuentra la aplicación web, descubre cualquier tipo de fallo en la implementación de la aplicación o servicio web.

- **Auditoría forense**
  Son servicios posteriores a un evento o incidente de seguridad, y están orientados a identificar las causas que lo produjeron.
- **Gestión de parches y vulnerabilidades**
  Son servicios destinados a la automatización de la actualización necesaria de los sistemas que evite la explotación de vulnerabilidades detectadas en otros sistemas.

USO - Escenario de aplicación

Escenarios de uso contemplados para los servicios de auditoría técnica:

- **Diseño del plan de auditoría**
  Durante esta fase se determinan los objetivos, el alcance de la auditoria, los recursos, plazos, etc.
- **Realización de auditoría**
  Etapa durante la cual se realiza el conjunto de análisis técnicos, ya sean preventivos o posteriores a un evento o incidente de seguridad.
- **Análisis y elaboración de informe**
  Una vez recogida la información ésta es revisada y analizada y se procede a la elaboración de un informe de resultados, en el cual se indicarán un conjunto de recomendaciones y medidas para mejorar la seguridad o las deficiencias detectadas.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de auditoría técnica:

- permiten conocer, identificar y analizar los riesgos y vulnerabilidades, pudiendo reducir así sus impactos;
- son un paso fundamental antes de implementar medidas de seguridad;
- permiten mejorar los procesos de negocio desde el punto de vista de la seguridad y la gestión;
- permiten mejorar la imagen externa de la organización, ofreciendo mayores garantías y niveles de seguridad.

5.2 Certificación de normativa

DESCRIPCIÓN - ¿Qué es?

Son servicios orientados a facilitar a las empresas y organizaciones la adecuación de cumplimiento normativo en materia de seguridad y obtención de certificados en estas normativas.
Se incluyen los servicios de orientados a la implantación de normativas de seguridad en las organizaciones; sistemas de gestión de seguridad de la información (SGSI), políticas de seguridad, análisis de riesgos, etc. También se incluyen los servicios de certificación, que tiene como objetivo acreditar y certificar las implantaciones de normativa realizadas, verificando y controlando si estas cumplen con los requisitos que indica cada norma.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de certificación normativa:

- **Sistemas de Gestión de la Seguridad de la Información (SGSI)**
  Los servicios SGSI son un conjunto de políticas de administración de la información según la normativa vigente. Contribuyen a asegurar los activos información de que disponen las organizaciones, validando su confidencialidad, integridad y disponibilidad. Los SGSI se gestionan con el marco normativo UNE ISO/IEC 27001.
- **Análisis de riesgos**
  Son servicios que tienen como finalidad detectar los activos y procesos críticos y conocer sus vulnerabilidades, para implementar medidas de detección, protección y recuperación de forma eficaz y efectiva.
- **Planes y políticas de seguridad**
  Son servicios que tienen la finalidad de analizar los riesgos a los que se enfrenta una organización y tomar medidas necesaria para reducir el nivel de riesgo, reflejando una serie de normas y reglamentos donde se definan las medidas seguridad.
- **Auditorías de seguridad y cumplimiento**
  Son servicios ofrecen la revisión y verificación de los niveles de seguridad y del cumplimiento de políticas y normativas.
- **Certificación y acreditación**
  Son servicios para la obtención de los certificados asociados a la implantación de determinada normativa.

5 Fichas de servicios de ciberseguridad

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de certificación normativa:

- **Plan de implantación**
  Se corresponde con la selección del tipo de normativa a implantar y el establecimiento de los objetivos, recursos, plazos, coste, etc.
- **Auditoria y análisis de la situación**
  En este paso se estudia la situación de la organización respecto de la normativa que se trata de implantar para obtener un imagen lo más completa y detallada posible de la situación.
- **Implantación de la normativa**
  Se corresponde con los trabajos específicos de implantación, elaboración de documentación, formación a los trabajadores, elaboración de políticas, etc.
- **Revisión y auditoría interna**
  Es el proceso de revisión interno de la implantación realizada. Se trata de verificar los trabajos realizados, identificar deficiencias y realizar las mejoras necesarias.
- **Auditoría externa y certificación**
  La auditoría externa es el proceso de revisión realizado por entidades externas a la organización, necesario para la obtención de un certificado que acredita la validez conforme a la normativa de la implantación realizada.
- **Mantenimiento y mejora continua**
  Proceso de revisión cíclico y continuo de la normativa implantada y proceso de mejora continua.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de certificación de normativa:

- permiten mejorar los procesos de negocio desde el punto de vista de la seguridad;
- permiten mejorar la imagen externa de la organización mediante las acreditaciones y certificaciones;
- permiten que las organizaciones puedan diferenciarse y destacar por su gestión de la seguridad;
- son también un mecanismo en manos de las organizaciones para promover la concienciación y formación en seguridad, las buenas prácticas y la aplicación de políticas de seguridad;
- permiten conocer, identificar y analizar los riesgos y vulnerabilidades existentes, pudiendo reducir así sus impactos.

5.3 Contingencia y continuidad

DESCRIPCIÓN - ¿Qué es?

Son servicios cuyo objetivo es realizar acciones encaminadas a contrarrestar y evitar interrupciones de las actividades del negocio y proteger sus procesos críticos ante incidentes y desastres de seguridad, garantizando la continuidad de los procesos de negocio.

Estos servicios facilitan la elaboración y aplicación de Planes de Contingencia y Continuidad que permiten definir e implantar un marco tecnológico, funcional y operativo que garantice la continuidad de las funciones críticas del negocio en caso de contingencia, mejorando la disponibilidad y confidencialidad del tratamiento de la información.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de contingencia y continuidad:

- **Planes de contingencia y continuidad de negocio**
  Son servicios para el diseño e implantación de medidas y planes relacionados con la respuesta ante incidentes y desastres que afecten a la información, permitiendo restablecer la continuidad del negocio.
- **Copias de seguridad remotas *(backup)***
  Son servicios de almacenamiento de datos fuera de la organización, permitiendo la restauración de la información de forma inmediata en caso de robos o pérdida de datos.
- **Custodia y archivo seguro**
  Son servicios de almacenamiento con fuertes medidas de seguridad y en un emplazamiento distante de la organización.
- **Centros de respaldo**
  Son servicios diseñados de réplica y almacenamiento que permiten a las organizaciones disponer de infraestructuras secundarias ante incidentes de seguridad.
- **Análisis de impacto en el negocio (*Business Impact Analysis, BIA*)**
  Servicio destinado a la identificación de los procesos o actividades de cada una de las áreas del negocio, cuantificando el impacto ante incidentes de seguridad que puedan afectar al negocio. Define el plan de recuperación ante desastres.
- **Gestión del ciclo de vida de la información**
  Son soluciones que permiten gestionar el ciclo completo de vida de la información, implementando políticas y mecanismos para garantizar el nivel de confidencialidad de la información.

5 Fichas de servicios de ciberseguridad

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de contingencia y continuidad:

- **Diseño general del plan**
  Servicios orientados a la definición del plan de contingencia, de su alcance, objetivos y métricas.
- **Auditoria y análisis de la situación**
  Estos servicios van orientados a determinar la situación actual del negocio y la organización en cuanto a los riesgos de contingencia y continuidad de negocio.
- **Proyecto de implantación**
  Elaboración del proyecto de implantación, fases, recursos, coste, etc. del plan de contingencia y continuidad de negocio.
- **Implantación**
  Implantación de planes, medidas, sistemas, políticas, etc. relativas a contingencia y continuidad de negocio.
- **Revisión y prueba**
  Servicios de evaluación de la implantación realizada, pruebas del sistema de gestión, copias de seguridad, sistemas de respaldo, etc.
- **Mantenimiento y mejora continua**
  Servicios orientados a la revisión y mejora continua de los planes sistemas políticas.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de contingencia y continuidad:

- mejora la preparación ante desastres de seguridad que puedan afectar a la actividad y negocio de las organizaciones;
- permiten que las empresas se puedan recuperar con rapidez y eficacia ante interrupciones de su actividad, pérdida de recursos, etc;
- permiten garantizar la continuidad de los procesos de negocio ante incidentes y desastres de seguridad;
- son un mecanismo para la concienciación, implementación de buenas prácticas y aplicación de políticas de seguridad relativas a las situaciones de contingencia;
- permiten ofrecer mejores garantías de seguridad y niveles de servicio a nuestros clientes, partners y socios;
- permiten conocer, identificar y analizar los riesgos y vulnerabilidades, con un enfoque de continuidad de negocio, pudiendo reducir así sus impactos.

5.4 Cumplimiento legal

DESCRIPCIÓN - ¿Qué es?

Son servicios que ayudan a las empresas a cumplir con la legislación vigente en materia de seguridad tecnológica o de seguridad de la información, como son la Ley Orgánica de Protección de Datos (LOPD), la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSICE), la Ley de Propiedad Intelectual (LPI) y otras.

Mediante estos servicios se ofrece apoyo y guía a las organizaciones desde el diseño a la auditoria, pasando por la implantación de las medidas de tipo jurídico, técnico y organizativo que garantizan el cumplimiento de la legislación.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de cumplimiento con la legislación:

- **Consultoría legal**
  Son servicios de consultoría que permiten saber el estado actual de las empresas en materia de legislación, proporcionado servicios de formación e información necesaria sobre la normativa, funciones y obligaciones que se han de seguir.
- **Adaptación a la legislación (implantación)**
  Son servicios destinados a llevar a cabo la adecuación de las empresas y organizaciones a la legislación aplicable, llevando a cabo la implantación de las medidas de tipo jurídico, técnico y organizativo.
- **Auditoría de legislación**
  Son servicios destinados a la realización de auditorías de nivel de cumplimiento de la legislación aplicable a una empresa u organización, con el fin de determinar y analizar si la empresa ha adoptado los cambios según la legislación.
- **Asesoramiento legal**
  Son servicios de revisión del grado de cumplimiento en materia relacionada con la legislación aplicable relativa a la seguridad. También se incluyen los servicios de asesoramiento en procesos sancionadores.
- **Borrado seguro**
  Son servicios que permiten realizar la eliminación de archivos, carpetas o unidades lógicas de forma segura según la normativa vigente.
- **Destrucción documental**
  Son servicios destinados a la destrucción de datos confidenciales y documentos, con el fin de evitar sanciones administrativas por incumplimiento con la legislación.

5 Fichas de servicios de ciberseguridad

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de cumplimiento legal:

- **Diseño del plan de adecuación a la legislación**
  Determinación de la legislación a cumplir, plazos, objetivos, fases.
- **Auditoria y análisis de la situación**
  Determinación de la situación actual del negocio y la organización respecto de la legislación a cumplir.
- **Proyecto de implantación**
  Elaboración del proyecto de adecuación, fases, recursos, coste, soluciones, etc.
- **Implantación**
  Proceso de adecuación, que incluye la implantación de las medidas de tipo jurídico, técnico y organizativo.
- **Auditoría interna**
  Evaluación interna, por personal de la propia organización, de la implantación realizada, pruebas sobre las medidas implantadas, revisión de la documentación asociada, etc.
- **Auditoría externa**
  En caso de que así lo requiera la legislación y muy recomendable tener un análisis externo de la situación real de la organización respecto del cumplimiento de la legislación aplicable.
- **Mantenimiento y mejora continua**
  Revisión y mejora continua de la implantación y adecuación realizada, para el mantenimiento de la adecuación y el cumplimiento legislativo.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de cumplimiento legal:

- permiten a las empresas y organizaciones cumplir con la legislación aplicable y estar preparados ante posibles denuncias o incidentes de seguridad relativos al cumplimiento de la legislación;
- permiten mejorar los procesos de negocio desde el punto de vista de la seguridad y la gestión;
- permiten mejorar la imagen externa de la organización, ofreciendo mayores garantías y niveles de seguridad;
- permiten que las organizaciones puedan diferenciarse y destacar sobre otras.
- ofrecen mecanismos para la concienciación y formación en seguridad, las buenas prácticas y la aplicación de legislación de seguridad;
- permiten ofrecer mejores garantías de seguridad y niveles de servicio a nuestros clientes, partners y socios;
- permiten conocer, identificar y analizar los riesgos y vulnerabilidades que afectan a la legislación, pudiendo reducir así sus impactos.

5.5 Formación y concienciación

DESCRIPCIÓN - ¿Qué es?

Son servicios destinados a ofrecer formación relativa a la seguridad de la información. El objetivo es conocer los retos a los que se enfrenta la seguridad y cómo afrontar los desafíos que se presentan, tanto desde el punto de vista técnico como jurídico.
Los servicios de formación y concienciación de la seguridad pueden ser presenciales o a través de *eLearning* o formación *on-line* a través de internet que permitan llevar a cabo una formación a distancia.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de formación:

- **Formación en materia de ciberseguridad (máster, postgrados, especialidades)**
  Son servicios de formación impartidos por centros autorizados que posibilitan la obtención de títulos académicos en materia de ciberseguridad.
- **Certificación profesional**
  Servicios de formación impartidos por organismos acreditados y certificados, que posibilitan la obtención de títulos específicos (CISA, CISM, CISSP,…) y muy demandados en el ámbito profesional.
- **Sensibilización y concienciación**
  Servicios orientados a la sensibilización de los usuarios, creando una conciencia de buenas prácticas y usos de las infraestructuras y los recursos de las organizaciones y las empresas.
- **Formación técnica en soluciones específicas de ciberseguridad**
  Son los servicios de formación muy especializada destinados a forman a personal en herramientas y soluciones de seguridad específicas.

5 Fichas de servicios de ciberseguridad

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de formación y concienciación:

- **Diseño del plan de formación**
  Durante esta fase se determinan los objetivos, el alcance de la formación, los recursos, plazos y evolución de dicho plan.
- **Formación**
  Fase durante la cual se lleva a cabo la formación y del seguimiento y medida del progreso de la actividad formativa.
- **Examen y valoración de los conocimientos adquirido**
  Se evalúa, si procede, el nivel de aprendizaje y los conocimientos que han asimilado los participantes en la formación. En esta fase se obtiene la acreditación en caso de enseñanza reglada o formación para certificación de profesionales.
- **Análisis y elaboración de informe**
  Si procede, sobre todo de cara a formación para empresa, es fundamental realizar un informe de resultados, evaluando la aceptación de la formación por parte de los participantes, de forma que permita una mejora continua de la formación.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de formación y concienciación:

- entender y utilizar de manera eficiente todos los recursos que posee la empresa para proteger sus sistemas y cumplir con la legalidad en materia de seguridad;
- optimizar el manejo y funcionamiento de los sistemas de seguridad implantados;
- garantizar el cumplimiento de la legislación y de las políticas de seguridad.

Los servicios de formación y concienciación pueden ser presenciales o a través de eLearnig o formación on-line.

5.6 Gestión de incidentes

DESCRIPCIÓN - ¿Qué es?

Los servicios de gestión de incidentes de seguridad de la información, están destinados a prevenir, detectar y solucionar incidentes de seguridad de la información. Tienen el objetivo de obtener información y ayudar y detectar las amenazas de forma rápida, identificar vulnerabilidades y priorizar riesgos. Permiten llevar la gestión antes, durante y después de cualquier incidente de seguridad.

Los servicios preventivos son la concienciación, la definición de buenas prácticas y políticas, definición de planes de contingencia y continuidad. Los servicios de detección de incidentes consisten en la instalación de programas anti-*malware,* IDS, eventos de seguridad y monitorización de red. Los servicios correctivos son los procedimientos de restauración de *backups* y auditoría forense.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de gestión de incidentes:

- **Prevención de incidentes de seguridad**
  Son servicios destinados a prevenir incidentes de seguridad, para ello se llevan cabo servicios de concienciación, definición de buenas prácticas y políticas de seguridad, definición de planes de contingencia.
- **Detección de incidentes de seguridad**
  Son los servicios destinados a la detección de incidentes de seguridad, consisten en la instalación de herramientas de seguridad, anti-*malware*, IDS, gestión de *logs* y eventos de seguridad.
- **Respuesta de incidentes de seguridad**
  Son servicios destinados a resolver incidentes de seguridad que hayan ocurrido, consisten en procedimientos de restauración de *backups*, eliminación de *malware* y auditoría forense.

5 Fichas de servicios de ciberseguridad

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de gestión de incidentes:

- identificación y valoración de incidentes;
- coordinación con fuentes externas;
- investigación forense;
- definición y ejecución de programas y procedimientos de gestión de incidentes;
- desarrollo y mantenimiento de perfiles de configuración de sistemas;
- aislamiento de sistemas y plataformas afectadas;
- asistencia técnica para análisis de eventos;
- elimina las causas de los incidentes y los efectos;
- acciones correctoras;
- recuperación y vuelta al funcionamiento normal;
- soporte preventivo y soporte postincidentes.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de gestión de incidentes:

- estar preparado ante incidentes y eventos de seguridad que afecten al negocio.
- rapidez de actuación en caso de incidentes;
- análisis de la causa de incidentes que permite tomar medidas para impedir su repetición;
- garantizar el cumplimiento de la legislación y de las políticas de seguridad.

Los servicios de detección de incidentes consisten en la instalación de programas antimalware, IDS, eventos de seguridad y monitorización de red.

5.7 Implantación de soluciones

DESCRIPCIÓN - ¿Qué es?

Son servicios destinados a la planificación, diseño e implantación de infraestructuras y soluciones de ciberseguridad, centrándose en la integración y puesta en marcha de estas infraestructuras y soluciones tecnológicas.
La infraestructura es la base donde descansan todas las herramientas y soluciones que las organizaciones utilizan para desarrollar su actividad. Un buen diseño de la infraestructura permitirá disponer de sistemas de la información seguros, aumentando la productividad y la reducción de costes de cualquier empresa u organización.
Se integran en esta categoría todos aquellos servicios destinados a gestionar infraestructuras y soluciones de ciberseguridad.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de implantación de infraestructuras:

- **Diseño de soluciones de ciberseguridad**
  Son servicios destinados para desarrollar soluciones necesarias para tener un nivel de seguridad adecuado.
- **Implantación de soluciones de ciberseguridad**
  Servicios para realizar la implantación de soluciones e infraestructuras de seguridad en las organizaciones.
- **Diseño, implantación y operación de Soluciones de Ciberresiliencia**
  Son aquellos servicios que tienen la finalidad de proteger y defender el uso del ciberespacio de los atacantes.
- **Diseño, implantación y operación de soluciones de ciberseguridad industrial**
  Son aquellos servicios destinados a incorporar procesos con el fin de garantizar la seguridad en entornos industriales, van desde las auditorías (SCADA) a la implantación de planes de ciberseguridad.

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de implantación de soluciones:

- **Consultoría y análisis previo**
  En esta fase se realiza un análisis del nivel de seguridad de la organización, que puede ser en profundidad o afectar solamente a una parte de la organización.
- **Selección de soluciones de seguridad e infraestructuras necesarias**
  A continuación, a partir de las necesidades detectadas se seleccionan las mejores soluciones de seguridad e infraestructuras.
- **Planificación de la implantación tecnológica**
  Se realiza una planificación de la implantación que se va a realizar, tiempos, costes y otras cuestiones relativas a cómo puede afectar la implantación a los distintos procesos de negocio y a la actividad de la organización.
- **Implantación de la infraestructura**
  Fase en la cual se lleva a cabo la instalación, parametrización y puesta en marcha de las soluciones e infraestructuras de seguridad en la organización.
- **Elaboración de documentación y formación**
  Una vez finalizado la fase de implantación, y en ocasiones paralela a esta, se lleva a cabo la elaboración de la documentación y la formación al personal de la organización.
- **Gestión y mantenimiento**
  La gestión y el mantenimiento puede ser un proceso que se realice tanto por personal de la propia organización, como una empresa externa o una combinación de ambos.
- **Revisión de la implantación**
  Finalmente es posible realizar una revisión periódica encaminada a mantener los niveles de seguridad alcanzados y adaptarse a los posibles cambios de la organización con el tiempo.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de implantación de soluciones:

- garantía de que la instalación y configuración de las herramientas de seguridad informática es realizada por profesionales;
- garantía de la selección de las herramientas adecuadas para su negocio;
- la empresa se beneficia del conocimiento y experiencia aportada por la consultora;
- se reduce el riesgo asociado a la inversión en tecnología de seguridad al contar con una metodología o con el consejo profesional para su selección.

5.8 Seguridad en la nube

DESCRIPCIÓN - ¿Qué es?

Son servicios destinados a la protección de las infraestructuras alojados en la nube "*cloud computing*", permiten el uso de recursos de *hardware, software,* almacenamiento y comunicaciones proporcionado a las empresas un servicio adicional de seguridad.
Estos servicios persiguen reducir las consecuencias de un incidente de seguridad, incluso aquellos que ocasionen la interrupción de la actividad de la empresa, permiten diseñar y activar alternativas en caso de incidentes a través de estrategias de recuperación y políticas de respaldo.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de integración *cloud*:

- **Software como servicio (*Software as a Service, SaaS*)**
  Son servicios de despliegue de *software* en que las aplicaciones y los recursos se han diseñado para ser ofrecidos como servicios bajo demanda, con estructura de servicios llave en mano. Las consideraciones de seguridad son controladas por el proveedor del servicio. El suscriptor del servicio únicamente tiene acceso a la edición de las preferencias y a unos privilegios administrativos limitados.
- **Plataforma como servicio (*Platform as a Service, PaaS*)**
  Son servicios de entrega bajo demanda, desplegándose el entorno (*hardware* y *software*) necesario para ello. El suscriptor del servicio tiene control parcial sobre las aplicaciones y la configuración del entorno ya que la instalación de los entornos dependerá de la infraestructura que el proveedor del servicio haya desplegado. La seguridad se comparte entre el proveedor del servicio y el suscriptor.
- **Infraestructura como servicio (*Infrastructure as a Service, IaaS*)**
  Son servicios en el cual la infraestructura básica de cómputo (servidores, *software* y equipamiento de red) es gestionada por el proveedor como un servicio bajo demanda, en el cual se pueden crear entornos para desarrollar ejecutar o probar aplicaciones. El suscriptor mantiene generalmente la capacidad de decisión del sistema operativo y del entorno que instala. Por lo tanto, la gestión de la seguridad corre principalmente a cargo del suscriptor.

5 Fichas de servicios de ciberseguridad

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de seguridad en la nube:

- **Planificación de la implantación tecnológica**
  Se realiza una planificación de la implantación que se va a realizar, tiempos, costes y otras cuestiones relativas a cómo puede afectar la implantación a los distintos procesos.
- **Gestión y mantenimiento**
  La gestión y el mantenimiento puede ser un proceso que se realice tanto por personal de la propia organización, como una empresa externa o una combinación de ambos.
- Servicios de evaluación de la implantación realizada, pruebas del sistema de gestión, copias de seguridad, sistemas de respaldo, anti-virus, etc.

BENEFICIO - ¿Qué ofrece el negocio?

Beneficios ofrecidos al negocio por los servicios de formación y concienciación:

- estar preparado ante incidentes y eventos de seguridad que afecten a la empresa;
- rapidez de actuación en caso de incidentes;
- permiten conocer, identificar y analizar los riesgos y vulnerabilidades, pudiendo reducir así sus impactos;
- permiten mejorar los procesos de negocio desde el punto de vista de la seguridad y la gestión.

Servicios destinados a la protección de las infraestructuras alojados en la nube "cloud computing".

5.9 Soporte y mantenimiento

DESCRIPCIÓN - ¿Qué es?

Son servicios que permiten a las empresas externalizar procesos, infraestructuras y personal de seguridad, de forma que sea una empresa especializada en materia de seguridad la que se encargue de dicha actividad de forma local o en remoto.
La externalización de servicios de seguridad consiste en la subcontratación de actividades propias de seguridad o actividades que garantizan la seguridad de la información en las empresas. Normalmente la empresa descarga la responsabilidad de los servicios de seguridad a una empresa especializada la cual se encarga de garantizar la seguridad mediante contrato, y reportando a través de informes, logs (registros de actividad de los equipos) o paneles de monitorización y seguimiento.

SUBCATEGORÍAS - Tipos

Podemos encontrar las siguientes subcategorías dentro de los servicios de seguridad gestionada:

- **Seguridad Gestionada**
  Son servicios de externalización total o parcial de la infraestructura de seguridad, llevando a cabo la gestión, supervisión y administración. Puede realizarse *in situ* o de forma remota.
- **Outsourcing de personal**
  Son servicios de externalización de personal de seguridad, puede realizarse in situ o de forma remota.
- **Externalización de servicios**
  Son aquellos servicios que se contratan a terceros para la realización de actividades relacionadas con el mantenimiento de los sistemas y procesos de cualquier entidad.

USO - Escenario de uso

Escenarios de uso contemplados para los servicios de soporte y mantenimiento:

- **Definir los servicios de seguridad a externalizar**
  La organización o empresa que desea externalizar alguna de sus actividades de seguridad, evalúa que procesos, infraestructuras y personal que puede externalizar, desde múltiples puntos de vista, como pueden ser costes, complejidad en la administración y gestión, personal necesario, etc.
- **Proyecto de externalización**
  Se trata de evaluar el proyecto, los participantes y los detalles de la prestación de servicios, los niveles de servicios necesarios, etc.
- **Prestador de servicios**
  En esta fase se trata de establecer y seleccionar el prestador de servicios, o el tipo de prestador de servicios necesario para cubrir las necesidades identificadas y los niveles de servicio deseados.
- **Revisión y nivel de servicio**
  A lo largo del mantenimiento del contrato con el prestador de servicios, se realiza una revisión y un análisis del nivel de servicio ofrecido y alcanzado, para detectar deficiencias o posibles mejoras, tanto en los servicios como en el nivel de servicio ofrecido.

USO - Escenario de uso

Beneficios ofrecidos al negocio por los servicios de soporte y mantenimiento:

- la empresa se beneficia del conocimiento y experiencia aportada por la empresa externa que le proporcionará eficiencia y rendimiento de los sistemas de seguridad subcontratados;
- se reduce el riesgo asociado a la inversión en tecnología de seguridad;
- permite a la empresa enfocarse en la gestión de las actividades fundamentales del negocio;
- aumento de la disponibilidad de los sistemas y de su fiabilidad. Horario 24x7;
- utilización de las últimas tecnologías de seguridad aplicables a las necesidades particulares de cada organización.

6 Recomendaciones y buenas prácticas

Recomendaciones y buenas prácticas para el uso de la taxonomía y el catálogo de empresas y soluciones de ciberseguridad:

- utilizar los términos de alcance y ámbito de aplicación para saber dónde y a quién van dirigidas cada una de la soluciones de seguridad;
- revisar las subcategorías de cada categoría para identificar las soluciones que mejor se adapten a cada necesidad;
- seguir las recomendaciones de cada solución y los beneficios que aportan;
- todas soluciones registradas en el catálogo van dirigidas según el tamaño de la empresa;
- buscar las empresas y las soluciones en el catálogo aprovechando los diferentes filtros que contiene;
- identificar el problema nos ayudará a la búsqueda de soluciones y a los proveedores de dichas soluciones.

Identificar el problema nos ayudará a la búsqueda de soluciones y a los proveedores de dichas soluciones.

7 Referencias

Hay que destacar que para la realización de este documento de la taxonomía, se ha tenido en cuenta la propia evolución del mercado, así como las diferentes clasificaciones de los productos y servicios de los principales de proveedores de soluciones de seguridad y de las instituciones, los organismos nacionales e internacionales que desarrollan informes y estudios detallados de las soluciones actuales de ciberseguridad.

Destacar la relevancia de empresas y entidades del sector de la ciberseguridad para los cuales se han realizado un mapeo de las categorías tanto de productos como de servicios, entre ellos destacar las clasificaciones de Gartner, IDC, entre otras.

	TAXONOMÍAS DE REFERENCIA	
CATEGORÍA DE PRODUCTO	GARTNER	IDC
Anti-fraude Anti-*phising*, Anti-spam, Herramientas de filtrado de navegación, UTM, Appliance	*E-Mail Security Software, Content Monitoring and Filtering, Internet Security Software*	*Anti-spam, Social Networking Security, Messaging Security*
Anti-*malware* Anti-virus, Anti-*Adware*, Anti-*spyware*, UTM, Appliance	*Anti-virus Software*	*Anti-malware, UTM*
Auditoría técnica Análisis de *logs* y puertos, vulnerabilidades, Auditoría de contraseñas, Auditoría de sistemas y ficheros	*Vulnerability Management*	*Security and Vulnerability Management, Forensics and incident Investigation, Specialized Threat Analysis and Protection*
Certificación normativa SGSI, Análisis de riesgos, Planes y políticas de seguridad, Normativas de seguridad	*Security Management, Performance Metrics, Policies*	*Risk Management, Regulatory Compilance*
Contingencia y continuidad H. de gestión de planes de contingencia y continuidad, Copias de seguridad, Infraestructura de respaldo, Virtualización, *Cloud*	*Storage and servers, Cloud/ Client Computing*	*Storage Software, Networking Virtualization, Cloud Security Gateways*
Control de acceso y autenticación Control de acceso a red, NAC, Gestión de identidad y autenticación, Single Sign-On, Certificados digitales, Firma electrónica	*NAC, Identity & Access Management, Single Sign-On, Authentication*	*Identity and Access Management, User Provisioning*
Cumplimiento legal Herramientas de cumplimiento legal (LOPD, LSSI,...), Borrado seguro, Destrucción documental	*Legal Compilance*	*Regulatory Compilance*
Inteligencia de seguridad Gestión de eventos de seguridad, SIM/SIEM, *Big Data*, Herramientas de monitorización y *reporting*	*Big Data*	*SIEM, Threat intelligence, Security and Vulnerability Management*
Prevención de fuga de información Control de contenidos confidenciales, Gestión del ciclo de vida de la información, Herramientas de cifrado	*Information Protection, Encryption software*	*Application Life-Cycle Management, Encryption Toolkits, Advanced Authentication*
Protección de las comunicaciones Cortafuegos (firewall), VPN, IDS, IPS, UTM, *Appliance*, Filtro de contenidos, P2P, Gestión y control de ancho de banda	*Network Security Software, Firewall Software, VPN Software, Intrusion Detection Software*	*Network Security/Firewall, Ethernet Swithc/ UTM, IDP, Endpoint Security*
Seguridad en dispositivos móviles Seguridad para dispositivos móviles, Seguridad para redes inalámbricas, BYOD	*Mobile and wireless, Wireless Security Softare, BYOD*	*Mobile Security*

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10 incibe_
2005-2015
TRABAJANDO POR LA CONFIANZA DIGITAL