BASQUE CYBERSECURITY CENTRE

GRUPO spri TALDEA

EUSKO JAURLARITZA
GOBIERNO VASCO
EKONOMIAREN GARAPEN ETA AZPIEGITURA SAILA
DEPARTAMENTO DE DESARROLLO ECONÓMICO E INFRAESTRUCTURAS

TAXONOMÍA DE CIBERSEGURIDAD

TABLA DE CONTENIDO

1. Descripción de la taxonomía 3

1. DESCRIPCIÓN DE LA TAXONOMÍA

La taxonomía de ciberseguridad propuesta establece varios niveles, en los que principalmente podemos diferenciar los correspondientes a productos y servicios.

Esta clasificación permite conocer en detalle los servicios y productos que se encuentran actualmente en el mercado de la ciberseguridad. Así, el alcance de los productos y servicios permite identificar las principales áreas a las que afectan cada uno de ellos.

Por otra parte, la taxonomía también permite establecer a quién van dirigidos las soluciones y productos.

Estos alcances permiten realizar búsquedas y clasificaciones de forma sencilla, dado que además de utilizar categorías, permite buscar en función del área o ámbito en el que se desea aplicar.

Los ámbitos de aplicación para dichas soluciones son los siguientes:

- Startup
  - Son empresas que buscan arrancar, emprender o montar un nuevo negocio, y aluden a ideas de negocios que están empezando, están en construcción o están a punto de producir a escala.
- Microempresa
  - Empresas que cuentan con menos de 10 trabajadores o en muchos casos son autónomos.
- Pyme
  - Empresas que cuentan con 10 y 250 empleados, y tienen un volumen medio de negocio.
- Gran empresa
  - Empresas que cuentan con más de 250 empleados, tienen infraestructuras propias y un volumen de negocio elevado.

Todo lo detallado anteriormente, da como resultado el modelo final de la taxonomía. Por una parte, se muestran los elementos correspondientes a la categoría de productos de ciberseguridad y los ámbitos de aplicación a los que afecta cada uno de ellos:

ÁMBITO DE APLICACIÓN						
CATEGORÍA DE PRODUCTO		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-malware		☑	☑	☑	☑
	Auditoría técnica	☑		☑		☑
	Certificación normativa		☑	☑	☑	☑
	Contingencia y continuidad		☑	☑	☑	☑
	Control de acceso y autenticación	☑				
	Cumplimiento legal	☑	☑	☑		
	Inteligencia de seguridad			☑	☑	☑
	Prevención de fuga de información		☑	☑		☑
	Protección de las comunicaciones		☑	☑	☑	☑
	Seguridad en dispositivos móviles		☑			☑

A continuación, se ofrece una breve descripción correspondiente a cada uno de los elementos anteriormente mostrados:

- **Anti-fraude**: Soluciones destinadas a proteger a los usuarios de ingeniería social para el robo de información o suplantación de identidad con técnicas como el phishing, correo electrónico no deseado o malware diseñado para ello.
- **Anti-malware**: Herramientas destinadas a proteger los sistemas informáticos (servidores, ordenadores, portátiles, dispositivos móviles, etc.) frente a software malicioso como virus, troyanos, spyware, etc. que pueda afectarles.
    - Su función es detectar y eliminar el software malicioso o malware sin que infecte el equipo.
- **Auditoría técnica**: Herramientas para la revisión y evaluación de la seguridad desde todos los ámbitos técnicos, tecnológicos y organizativos, generalmente tomando un estándar como referencia. Tiene como fin realizar auditorías de sistemas, aplicaciones y datos para la detección de posibles vulnerabilidades de seguridad.
- **Certificación normativa**: Herramientas para facilitar el cumplimento normativo correspondiente a la seguridad y la obtención de certificados de dichas normas. Son utilizadas para la implementación de políticas de seguridad, implantación de medidas de seguridad, o la valoración de activos, entre otros.
- **Contingencia y continuidad**: Herramientas con el fin de planificar planes de actuación y contingencia para mitigar los impactos provocados por cualquier incidencia de seguridad. Están destinadas a la recuperación de los sistemas y procesos considerados críticos ante incidentes de seguridad en una organización. Sistemas en la nube, la virtualización o soluciones de backup remoto son algunas de las soluciones.
- **Control de accesos y autenticación**: Productos destinados a implantar en las empresas de mecanismos para gestionar usuarios, sus permisos o controlar su acceso a los recursos. Para ello se utilizan mecanismos de autenticación y herramientas destinadas al uso de certificados digitales.
- **Cumplimiento legal**: Herramientas para facilitar el cumplimiento legal relacionado con aspectos de seguridad de la información, como el caso del RGPD (Reglamento General de Protección de Datos), comercio electrónico, etc.
- **Inteligencia de seguridad**: Herramientas que permiten establecer un flujo para la gestión de eventos o incidentes de ciberseguridad con el fin de mitigarlos en el menor tiempo posible.
- **Prevención de fuga de información**: Herramientas para asegurar la confidencialidad, disponibilidad e integridad de la información. El principal objetivo es evitar la pérdida de información e identificar, monitorizar y detectar las fugas de información.
- **Protección de las comunicaciones**: Productos destinados a garantizar las comunicaciones seguras para evitar accesos no autorizados o ataques

provenientes de otras redes. Permiten controlar el tráfico, analizarlo y realizar un control sobre su uso.

- **Seguridad en dispositivos móviles**: Herramientas destinas a la protección de redes inalámbricas y dispositivos móviles para evitar los incidentes de seguridad.

Por otra parte, se muestran los elementos correspondientes a la categoría de servicios de ciberseguridad para el de control, cumplimento de la legislación vigente, la gestión de la seguridad, continuidad ante incidentes, etc. y los ámbitos de aplicación de cada uno de ellos.

CATEGORÍA DE SERVICIO		Personas	Información	Infraestructura	Negocio
	Auditoría técnica		☑	☑	
	Certificación normativa	☑	☑	☑	☑
	Contingencia y continuidad				☑
	Cumplimiento legal	☑	☑	☑	
	Formación y concienciación	☑			
	Gestión de incidentes	☑	☑	☑	
	Implantación de soluciones			☑	
	Seguridad en la nube		☑	☑	☑
	Soporte y mantenimiento		☑	☑	

Se incluye una breve descripción de cada uno de los servicios mencionados:

- **Auditoría técnica**: Servicios destinados a realizar diagnósticos técnicos de seguridad, generalmente tomando un estándar como referencia, para

analizar el estado de seguridad y detectar posibles vulnerabilidades o amenazas de seguridad. También pueden ser realizadas tras un evento de seguridad para conocer las causas que lo ocasionaron y consecuencias producidas como resultado.

- **Certificación normativa**: Servicios orientados a facilitar la implantación y el cumplimiento normativo en cuanto a seguridad y a obtener certificados correspondientes a las normativas.
- **Contingencia y continuidad**: Servicios con el objetivo de garantizar la continuidad de los servicios y proteger los procesos críticos a través de la elaboración y aplicación de planes de contingencia y continuidad. Facilitan la elaboración de planes de contingencia y continuidad para garantizar la continuidad de las funciones críticas de la organización
- **Cumplimento legal**: Servicios enfocados a orientar y ayudar a las empresas para cumplir con la legislación actual en cuanto a la seguridad tecnológica o de la información se refiere.
- **Formación y concienciación**: Servicios destinados a ofrecer formación relacionada con la seguridad de la información para conocer los aspectos técnicos y jurídicos de la seguridad de la información.
- **Gestión de incidencias**: Servicios para la detección, prevención y solución de incidencias de seguridad de la información. Su objetivo es obtener información para detectar e identificar vulnerabilidades en los sistemas. Permiten gestionar las incidencias de seguridad antes, durante y después de que ocurran.
- **Implantación de soluciones**: Servicios destinados al diseño, integración y puesta en marcha de infraestructuras y soluciones tecnológicas de seguridad en las organizaciones con la finalidad de protegerse.
- **Seguridad en la nube**: Servicios orientados a proteger las infraestructuras alojados en la nube para reducir las consecuencias de un incidente de seguridad a través de sistemas de recuperación o políticas de respaldo.
- **Soporte y mantenimiento**: Permite que una empresa externa especializada en seguridad se encargue de las tareas de mantenimiento, infraestructuras o sistemas de una empresa.

La taxonomía detallada permite identificar la categoría correspondiente al producto o servicio dentro de la ciberseguridad, ayudando a catalogarlo en el área de aplicación correspondiente.