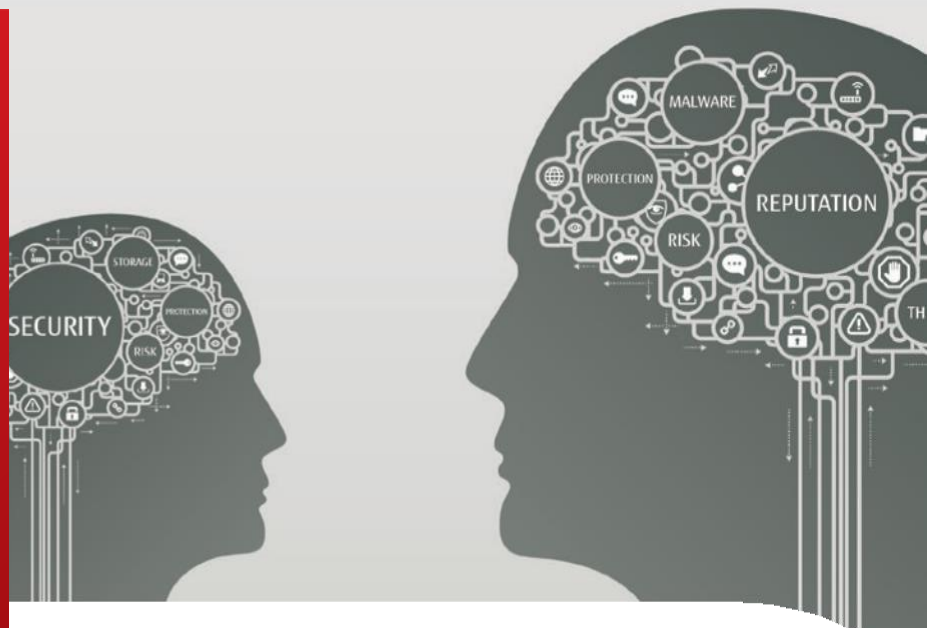


Seguridad de la información

Reducción del riesgo para las organizaciones



Fujitsu ayuda a las organizaciones a gestionar con eficacia los riesgos de continuidad y de seguridad de la información a los que se enfrentan, aportándoles flexibilidad en su forma de trabajar y la capacidad de realizar negocios con seguridad y resiliencia

Al ritmo del cambiante entorno de la seguridad

Actualmente, la capacidad de las empresas para funcionar y crecer se sustenta con su modo de gestionar y utilizar la información. Sin embargo, proteger plenamente estos activos de información y la propiedad intelectual resulta cada vez más desafiante.

Según los analistas de IDC, los ejecutivos sitúan la mejora de la seguridad de TI como la principal prioridad en 2014. Esta clasificación reconoce la progresiva distancia entre las crecientes amenazas de seguridad para las organizaciones y su capacidad para proteger los activos de información corporativos.

Las empresas deben mantenerse al ritmo de un entorno de seguridad que no deja de cambiar, lo que plantea una variedad de exigencias estratégicas y operativas, entre las que se incluyen las siguientes:

- Un número creciente de requisitos normativos y de cumplimiento
- Amenazas internas y externas que no dejan de evolucionar
- El riesgo de filtraciones de datos y la pérdida de propiedad intelectual
- Permitir el uso de dispositivos móviles de trabajo y personales por parte de los empleados
- Aprovechar los servicios en la nube para impulsar la productividad
- Garantizar la continuidad del negocio y del servicio

La gestión y la reducción de estos riesgos resulta cada vez más costosa y compleja para las organizaciones, en un momento en el que los presupuestos de seguridad se someten a un escrutinio más estricto. Además, las empresas se juegan más que nunca, ya que se esfuerzan por hacer algo más que simplemente proteger su información crítica y salvaguardar su reputación y sus ingresos.

En estos tiempos desafiantes, las organizaciones necesitan trabajar con un socio de confianza que pueda aportar una amplia variedad de experiencia y especialización con los que enfrentarse a los retos de seguridad y continuidad. Por este motivo, las organizaciones líderes eligen a Fujitsu.

Gestión del riesgo con Fujitsu

Las capacidades en Seguridad de la información de Fujitsu incluye una variedad de servicios gestionados y servicios expertos profesionales para proteger frente a las amenazas en continuo cambio a las que se enfrentan las organizaciones actualmente

Fujitsu presta una completa gama de servicios de seguridad de la información a clientes de todos los tamaños, tanto en el sector público como en el privado. Aportamos nuestra experiencia forjada tras décadas de prestación de servicios de información segura a una amplia base de clientes, incluidos Administración General del Estado, Comunidades Autónomas, Entidades Financieras e IBEX 35.

Los Servicios de seguridad de la información de Fujitsu ofrecen capacidades de seguridad esenciales a nuestros clientes para sustentar sus acciones de protección de los activos de la información, ante los retos empresariales emergentes estratégicos y operativos. Constituimos un componente crítico para nuestros clientes a la hora de responder a sus exigencias normativas y legales, ayudándoles a gestionar sus riesgos de seguridad de la información con flexibilidad y eficacia.

Ventajas

- **Mejor protección a menor coste:**
Gracias a la fortaleza de las relaciones con nuestros proveedores, la experiencia demostrada y nuestra escala global, podemos optimizar el enfoque de nuestros clientes relativo a la seguridad, generando importantes ahorros de costes.
Ofrecemos a las organizaciones inteligencia real y visibilidad sobre el estado de su entorno, identificando las vulnerabilidades y estableciendo prioridades en la inversión para destinarla allí donde más se necesita.
- **Un servicio flexible y con mayor capacidad de respuesta:**
El objetivo de Fujitsu es hacer que las organizaciones operen del modo más productivo y seguro posible. Puede que implique garantizar un acceso seguro a la información en cualquier momento y lugar; aportar visibilidad rápida y protección frente a nuevas amenazas; o bien permitir un uso controlado de las redes sociales. En todo momento, nos aseguramos de que nuestros clientes disponen de la flexibilidad para responder a los nuevos retos empresariales, al mismo tiempo que se reducen al mínimo los riesgos relativos a su información.
- **Respuesta a las demandas de cumplimiento:**
Todos nuestros clientes tienen que operar en el contexto de un entorno normativo y jurídico en constante cambio. Nos aseguramos de que se aplican los niveles adecuados de protección y de generación de informes para garantizar el cumplimiento normativo. En concreto, contamos con una sólida experiencia en prestar servicios que cumplen las políticas de seguridad en línea con normativas y estándares como PCI DSS, ISO 27001/2, SOX e ISO22301:2012.

Servicios integrales para proteger su empresa

Las capacidades de Fujitsu incluyen una variedad de servicios de seguridad gestionados y servicios profesionales expertos para responder a las rigurosas exigencias de las organizaciones. De este modo, trabajamos de cerca con los clientes para definir, diseñar, prestar y operar servicios integrales y nos encargamos de gestionar su complejidad. Por otro lado, nos aseguramos de que se aplican los controles de seguridad técnicos, físicos, de personal y de procedimientos adecuados. En concreto, nuestros servicios de seguridad gestionada son modulares y se pueden prestar con distintos enfoques, desde las instalaciones de Fujitsu como un servicio probado en la nube, in situ, en las instalaciones del cliente, o con una combinación de ambos.

El Servicio de seguridad de la información de Fujitsu combina una variedad de tecnologías de proveedores y servicios en la nube en un servicio uniforme. De este modo, adaptamos la prestación del servicio de seguridad para responder a los requisitos de cumplimiento y riesgos de cada cliente, al mismo tiempo que se benefician de las economías de escala para reducir al mínimo la necesidad de inversiones.

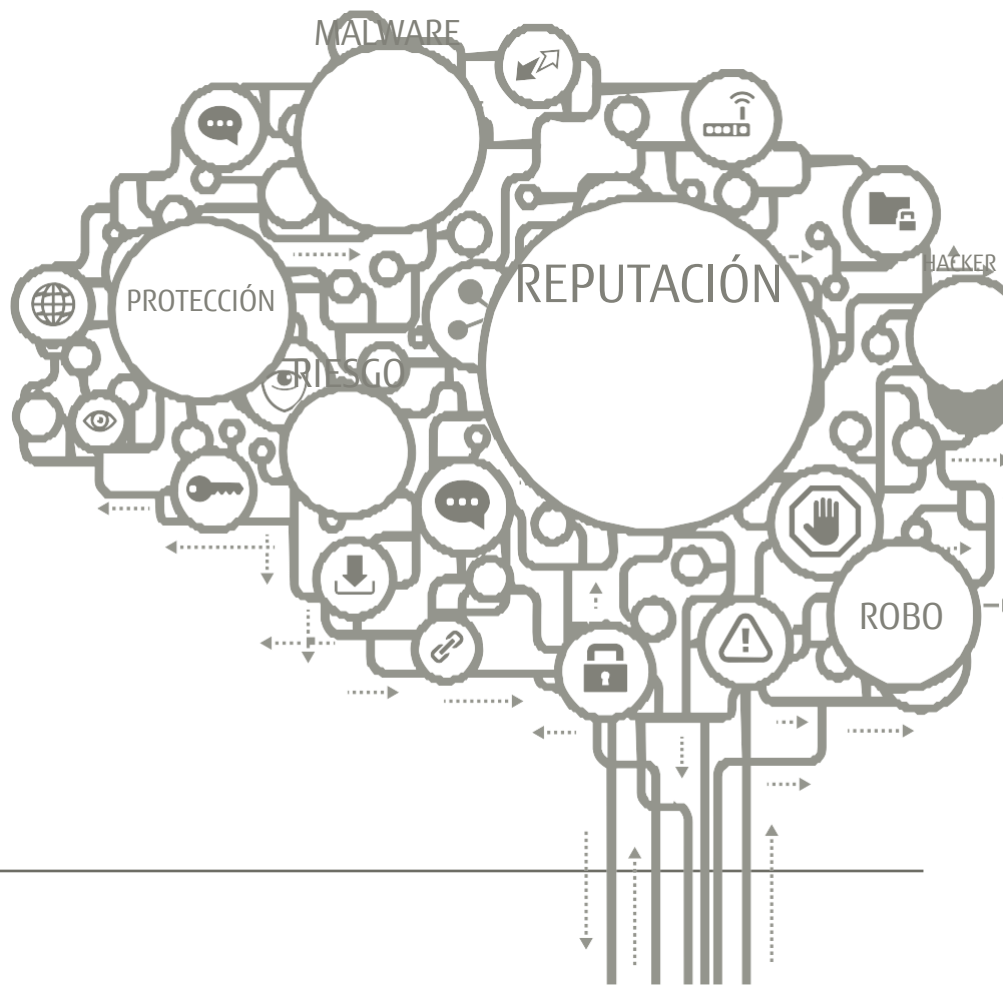
Nuestros servicios de seguridad gestionada son modulares y pueden prestarse como parte de un enfoque combinado: desde las instalaciones de Fujitsu como un servicio probado en la nube, in situ, en las instalaciones del cliente o bien una combinación de ambos.

Servicios de seguridad gestionada de Fujitsu

Fujitsu se responsabiliza de la gestión continua de las funciones de seguridad específicas en nombre de los clientes. Utilizamos productos líderes en el mercado y servicios profesionales expertos para sustentar la evaluación del riesgo, definir los requisitos, ofrecer diseño técnico y de servicio y arquitectura, así como garantizar una implantación efectiva y el funcionamiento del Servicio de seguridad gestionada. Todos nuestros servicios aportan a los clientes la cobertura permanente que necesitan para proteger sus empresas.

Servicios profesionales de seguridad de Fujitsu

Los profesionales de seguridad de Fujitsu actúan como asesores de confianza para los clientes, ofreciéndoles asesoría independiente y consejos para afrontar sus retos. Nuestro equipo está integrado por especialistas en seguridad, expertos en continuidad empresarial y gestión de identidad y acceso y asesoran tanto a clientes del sector público como del privado. Nuestros servicios profesionales se pueden adaptar para responder a requisitos específicos.



Seguridad de la información

Descripción general de los servicios

Servicio gestionado	Función
Firewalls	Aporta protección frente al acceso no autorizado a activos de información críticos.
Detección avanzada de amenazas	Ofrece defensa contra ciberamenazas a lo largo del ciclo de vida de un ataque avanzado
Sistemas de detección de intrusión o IDS (Intrusion Detection Systems) y sistemas de prevención de intrusión o IPS (Intrusion Prevention Systems)	Supervisa el tráfico de las redes para detectar actividades malintencionadas y ofrece alertas de seguridad para realizar análisis y reparaciones.
Gestión de información y eventos de seguridad o SIEM (Security Information and Event Management)	Respalda el cumplimiento de las políticas de seguridad (incluido PCI DSS y CISO Good Practice Guide 13) mediante la recopilación, el almacenamiento, la correlación y el análisis de información de registros de una variedad de dispositivos de seguridad. Esto aporta los componentes fundamentales para la prevención, la detección y la solución de incidentes de seguridad, así como para llevar a cabo análisis retrospectivos con los que sustentar investigaciones de seguridad.
Seguridad Web	Protege contra amenazas basadas en web y código malicioso y además ofrece un filtro del contenido web, en línea con las políticas corporativas y de uso aceptable.
Seguridad de terminales	Garantiza una protección coherente de terminales en toda la empresa, para detectar amenazas de malware. El servicio puede incluir antivirus y antispyware, control de aplicaciones y dispositivos, firewalls de escritorio, prevención de intrusión en host y control de acceso a redes.
Vulnerabilidad	Protege a la empresa de amenazas por correo electrónico entrante o saliente (incluido spam, malware, phishing, etc.) y también puede aplicar las políticas de seguridad (incluidas políticas de filtración de datos y uso aceptable).
Evaluación	Analiza la infraestructura de TI para identificar, establecer prioridades e informar de cualquier vulnerabilidad conocida, que posteriormente puede utilizarse para impulsar la actividad de reparación y mejorar la protección de activos de información críticos.
Prevención de pérdida de datos	Protege la marca y la reputación a través de la aplicación de políticas definidas para mitigar el riesgo de pérdida de datos confidenciales e informar sobre los requisitos de cumplimiento (incluido PCI DSS y DPA).
Cifrado	Aporta protección de la información confidencial estática y en tránsito.
VPN	VPN garantiza el tránsito seguro de la información y permite trabajar con seguridad y flexibilidad de forma remota.

Servicio profesional	Función
Seguridad	Aporta una revisión independiente del estado actual de la seguridad, junto con un plan claramente definido de acción, adaptado al entorno del cliente. Puede identificar el grado de efectividad de los controles de seguridad aplicados para proteger activos fundamentales, almacenes de datos confidenciales e interconexiones empresariales críticas. Las revisiones también pueden incluir auditorías según los requisitos legales (por ejemplo, PCI DSS), normativos (por ejemplo, ISO 27001), mejores prácticas, políticas de seguridad. Por otro lado, la revisión se puede centrar en áreas como la prevención de pérdida de datos o DLP (Data Loss Prevention) y la gestión de riesgos y el cumplimiento o GRC (Governance Risk and Compliance).
Continuidad del negocio y del servicio	Garantiza el desarrollo, la creación, la implantación y la validación de las estrategias de continuidad para responder a los requisitos del cliente. Las pruebas aseguran que el servicio cumple los requisitos acordados de continuidad y que la estrategia está lista para su aplicación. Tras la aplicación, también podemos ofrecer un programa de garantía que incluye auditorías, revisiones y pruebas continuas, para asegurar que se sigue disponiendo de una respuesta efectiva para responder a los requisitos de continuidad. Nuestro enfoque responde a estándares de cumplimiento del sector como ISO22301:2012 y ISO/IEC20000.
Gestión de identidades y acceso	Aplicando nuestra experiencia en gestión del ciclo de vida de la identidad, ayudamos a los clientes a superar sus retos de identidad y acceso y a sustentar sus funciones empresariales, mitigar el riesgo de accesos no autorizados, permitir la movilidad segura y aprovechar las eficiencias empresariales y garantizar el cumplimiento normativo.