DOCUMENTOS SiC
Nº 23
JUNIO 2017

FUJITSU

Servicios integrados de ciberseguridad global

María Gutiérrez
Directora de Ciberseguridad de Fujitsu España

SERVICIOS Y SOLUCIONES

- **Prevención inteligente de amenazas**
- **Privacidad de datos**
- **Gestión de Identidades SaaS**
- **Ciberseguridad OT**

PRONÓSTICO

- **Informe de predicciones de amenazas 2017**

Fujitsu apuesta por la prestación de servicios integrados de ciberseguridad para entornos IT y OT

Acorde con su visión 'Una sociedad inteligente centrada en el ser humano', la ciberseguridad se ha convertido en una prioridad para Fujitsu, que ha elevado a una magnitud de primer orden su compromiso con la protección de la información y la privacidad de los datos personales. Para ello, la multinacional ha desarrollado una amplia oferta de servicios gestionados y profesionales con el objetivo de aumentar la ciberseguridad de los procesos de negocio dependientes de las TIC.

Ante el escenario actual que está conformando la era digital, la preparación contra el creciente número de ciberataques transfronterizos y la protección de la información privada y confidencial son requisitos a los que las organizaciones deben responder con urgencia. Por este motivo, Fujitsu ha decidido situar la ciberseguridad en un primer plano empresarial. Históricamente, la multinacional nipona viene prestando gran relevancia a la protección de las infraestructuras y de los datos propios y de sus clientes en su Código de Conducta y de Responsabilidad Social Corporativa. Pero la realidad actual ha provocado que eleve dicho compromiso a una magnitud de orden superior.

Guiada por su visión 'Una sociedad inteligente centrada en el ser humano', donde cualquiera puede utilizar las TIC para sacar su máximo potencial en una sociedad más segura, abundante y sostenible, el propio Presidente de Fujitsu, Tatsuya Tanaka, ha manifestado su férreo compromiso con la ciberseguridad a través de una carta donde explica que, además de las mencionadas normas internas, el Grupo ha establecido una 'Política de Seguridad de la Información', que se aplica tanto en Japón como en el ámbito internacional. Tal como manifiesta Tanaka, *"Creemos que es nuestra responsabilidad social como empresa tecnológica global utilizar el poder de las TIC para contribuir a la realización de una tierra sostenible y mantener y reforzar una sociedad digital segura".* Sin duda, un paso significativo que la compañía ha plasmado en su 'Informe de Seguridad de la Información 2016', en el cual, se presentan sus actividades relacionadas con esta materia.

UNA UNIDAD DE NEGOCIO DESTACADA

En España, desde el pasado mes de abril, la ciberseguridad también se ha situado en el primer plano empresarial en forma de Unidad de Negocio destacada.

En línea con este movimiento estratégico global, Fujitsu se posiciona en el mercado español con una amplia oferta de ciberseguridad, vertebrando su propuesta en servicios de consultoría, integración y gestionados de protección TI y privacidad de los datos personales, prevención inteligente de ciberamenzas, gestión de identidades y accesos (incluida la modalidad SaaS), gestión del riesgo y cumplimiento normativo, ciberseguridad industrial (OT) y seguridad física biométrica. Todas ellas, áreas que se articulan sobre un conjunto de capacidades tecnológicas, experiencia y capital humano altamente especializado y cualificado.

En este sentido, Fujitsu cuenta con una red global de centros especializados (SOCs) desde los que monitoriza y entrega sus servicios avanzados de ciberseguridad. En España, la compañía cuenta con un SOC en Sevilla, y dos Centros Especializados –uno ubicado en Madrid y otro en Barcelona–, conformados por un equipo de 40 profesionales altamente cualificados. Desde dichos centros se realizan análisis con base al procesado inteligente

Vista del SOC ubicado en Madrid.

Fujitsu se posiciona en el mercado español con una amplia oferta de ciberseguridad, vertebrando su propuesta en servicios avanzados de protección IT y privacidad de los datos, prevención inteligente de ciberamenzas, gestión de identidades, gestión del riesgo y cumplimiento normativo, ciberseguridad industrial (OT) y seguridad física biométrica.

de información disponible en todas las fuentes accesibles de información sobre amenazas y vulnerabilidades, nuevos tipos de ataques... Además, es posible incluir información sobre el contexto de la organización que ayude a dotar de relevancia detalles como el estado o las características de cada cliente. El objetivo es ofrecer un servicio siempre actualizado y preparado para cualquier eventualidad, incluida la asistencia en la gestión de crisis.

Vista del SOC ubicado en Reino Unido.

CATÁLOGO DE SERVICIOS

Fujitsu complementa sus capacidades fundamentales de detección, protección y respuesta a incidentes de seguridad con una oferta de servicios avanzados, entre los que destacan (ver **Figura 1**):

Cyber Threat Intelligence (CTI)

Se trata de un novedoso servicio de protección centrado en responder a amenazas y *malware* que ya han atravesado los cortafuegos de una compañía. El CTI aumenta las defensas mediante monitorización continua y una respuesta proactiva –evitando que se cause mayor daño en la red– encaminada a proteger la infraestructura y los servicios de los clientes. El servicio de inteligencia de amenazas de Fujitsu ha permitido a Scottish Water, por ejemplo, fortalecer su ciberseguridad aumentado su nivel de detección y prevención a través de análisis con base en IA. En dicho proceso, se correlacionan datos con varios productos de socios estratégicos para proporcionar a la empresa la información que necesita para comprender la amenaza.

Gestión de Identidades como Servicio

Dentro de la oferta de Fujitsu en España, la firma nipona también ha desarrollado una oferta enfocada en la gestión de identidades, atendiendo a este reto a través de una propuesta *end-to-end*, que permite al cliente administrar, crear, ajustar y eliminar permisos, la autenticación mediante múltiples métodos, integración en los diferentes sistemas de la organización –en nube, entornos dedicados o bajo gestión de terceros– y una escalabilidad adecuada a sus necesidades. En este sentido, destaca el desarrollo de dos sistemas: Vetuma –servicio online de autenticación y pago de ciudadanos– y Virtu –servicio de inicio de sesión único para funcionarios– para el gobierno finlandés, los cuales, procesan millones de *logs* cada mes.

Ciberseguridad industrial

Otra de las apuestas de Fujitsu consiste en los servicios de ciberseguridad OT. Dentro de esta oferta, la compañía dispone de todo un catálogo de soluciones enfocadas a la protección de los entornos de producción, entre las que se incluyen: la protección de protocolos industriales, la inteligencia de ciberamenazas, el acceso remoto y la monitorización OT. La compañía aprovecha así su origen industrial y su experiencia como proveedor de servicios para ofrecer un valor diferencial, tanto en enfoque y estrategia, como en tecnologías, conocimiento y prácticas.

Privacidad de datos y cumplimiento normativo

Fujitsu cuenta, además, con un conjunto de servicios de consultoría relacionados con el Reglamento General de Protección de Datos de la UE (RGPD), que permite a las empresas cambiar su perspectiva sobre la protección de datos personales e ir más allá del mero cumplimiento. A través de una evaluación inicial, el cliente podrá adquirir un conocimiento general de su estado de preparación, con un enfoque práctico que permite evaluar el estado del arte de las soluciones y procesos de ciberseguridad ya implantados, valorando cuáles de estos elementos pueden servir como palanca para un óptimo cumplimiento.

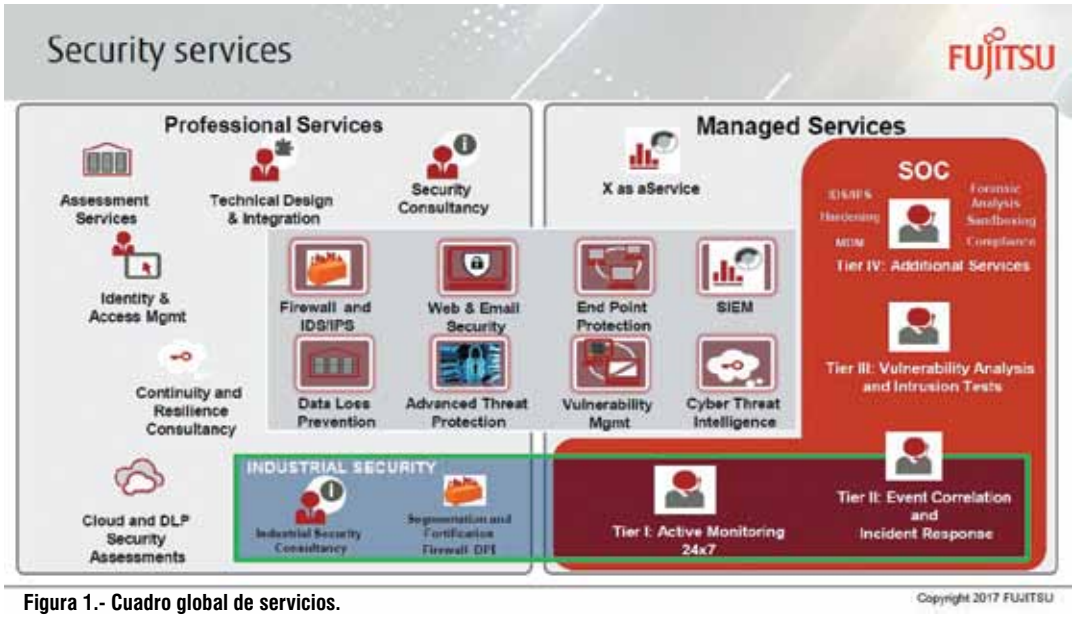


Figura 1.- Cuadro global de servicios.

María Gutiérrez

Directora de Ciberseguridad de Fujitsu España

Fujitsu ha situado la ciberseguridad como una de las piezas claves de su oferta de productos y servicios. En España, este hecho se ha traducido en la creación de una Unidad de Negocio específica, dirigida por una especialista con gran experiencia en la materia, María Gutiérrez, quien detalla en esta entrevista cómo se estructura dicha Unidad y la estrategia de la compañía en este segmento de mercado.

"Nuestra oferta de servicios de ciberseguridad IT y OT nos permite ser el referente en un mercado donde no existen muchos prestadores de servicios integrados"

– ¿Cómo se estructura el Departamento de Ciberseguridad de Fujitsu en España?

– La organización del Departamento consiste en un Equipo de Operación, un Equipo de Venta y un Equipo de Preventa. En total, La Unidad de Ciberseguridad está formada por 40 profesionales y, viendo las expectativas y tendencias que hay en el mercado, vamos a crecer. Asimismo, y como la seguridad es un área horizontal a todos los servicios que presta la compañía, la Dirección del Departamento posee un Comité Asesor formado por especialistas de todas las áreas con los que colaboramos, especialmente las que van a ser prioritarias en los próximos años, como son las de soluciones en la nube, *analytics* e IoT. Todas ellas tienen un componente de ciberseguridad que tenemos en cuenta.

– ¿Cuál es la oferta de valor en ciberseguridad que Fujitsu ofrece desde España?

– Contamos con servicios avanzados que se prestan de forma global o específica en sus distintas capas: monitorización, administración, correlación, prevención inteligente de amenazas, identidad digital como servicio, *pentesting*, forensía y vigilancia digital, entre otras. Los servicios se ofrecen, en su mayoría, desde el SOC de Sevilla, que a día de hoy está muy centrado en el segmento de protección de infraestructuras críticas y servicios industriales. No obstante, contamos también

"La Unidad de Ciberseguridad de Fujitsu en España está formada por 40 profesionales y, viendo las expectativas que hay en el mercado, nuestro objetivo es seguir creciendo"

con dos centros especializados, uno en Madrid y otro en Barcelona. Todos ellos pertenecen a una federación de Centros de Operaciones que la compañía posee a nivel mundial y, aunque todos compartimos la práctica general de un SOC, la idea de la organización es estar fuertemente verticalizado, en nuestro caso, en el entorno industrial con el Centro de Sevilla.

– ¿Cuáles son las necesidades del sector industrial en materia de ciberseguridad?

– Muchos análisis de mercado nos indicaban que faltaba una oferta especializada en este sector. La propuesta de valor de Fujitsu es, en sí, diferencial en un mercado donde no existen muchos prestadores de servicios de ciberseguridad especializados. Desde sus orígenes, nuestra empresa ha estado muy vinculada al mundo de la automatización industrial y, por tanto, posee capacidades que le permiten entender los protocolos de comunicación, el funcionamiento de los sistemas industriales, sus debilidades y la mejor forma de gestionar el riesgo.

– Fujitsu España también cuenta con un laboratorio. ¿Qué líneas de investigación tienen abiertas?

– Desde hace un año y medio, Madrid, es el único lugar de Europa continental que posee una sede de los laboratorios de Fujitsu, en nuestro caso, especializado en *analytics*, ya que los laboratorios que investigan específicamente en ciberseguridad están en Japón. No obstante, en nuestro laboratorio aterrizan tecnologías, especialmente, para el entorno industrial, que están aprendiendo a interpretar protocolos para detectar si un comportamiento es normal o se trata de un ataque. Nos basamos en ODMA, nuestra sistema de inteligencia, que es capaz de entender, conectar e interpretar más de 200 protocolos, entre ellos los SCADA. Otra de las tecnologías que nos hemos traído de Japón es un sistema de autenticación biométrica basado en el reconocimiento de patrones de venas. Poseemos el *copyright* del algoritmo en el que se basa esta técnica. Todo ello, hace que estemos armados para dar soporte a todo el ciclo de vida de una solución de ciberseguridad en IT y OT, porque tenemos las piezas necesarias: método, tecnologías, expertos y servicios.

– Fujitsu dispone de un servicio de prevención inteligente de amenazas con gran renombre en el mercado profesional. ¿Qué elementos diferenciales incorpora?

– La solución está diseñada para ir mostrando a los clientes una película de todo lo que está pasando en su organización en materia de ciberseguridad y qué exposición tiene al riesgo y a las ciberamenazas, tanto interna como externamente. Fujitsu posee una gran base de datos sobre ataques, comportamientos, etc., alimentadas por acuerdos con socios estratégicos y terceros a escala global y multisectorial. Aunque bien merece resaltar que el valor diferencial lo dan nuestros expertos y herramientas especializadas con las que contamos gracias a acuerdos con proveedores de información de calidad y en tiempo real.

"La mayoría de los servicios se prestan desde el SOC de Sevilla. No obstante, contamos también con dos centros especializados, uno en Madrid y otro en Barcelona"

– ¿Con qué otros servicios se posiciona Fujitsu?

– En España también contamos con servicios profesionales orientados a la adecuación y el cumplimiento del RGPD. Ofrecemos al cliente una visión de su estado de adaptación a la normativa para, posteriormente, definir recomendaciones, desarrollos y tecnologías que ayudan a planificar y llevar a cabo los siguientes pasos para el cumplimiento. En nuestro portafolio destaca, asimismo, la solución *Identity as a Service*, que permite la gestión de identidades desde una perspectiva global *end-to-end.* Por otra parte, conviene resaltar el desarrollo de una plataforma de *cybertraining*, en un principio dirigida a Cuerpos Y Fuerzas de Seguridad del Estado, pero que hemos adecuado para realizar programas de concienciación en ciberseguridad a la medida de cualquier grupo de usuarios del cliente. ●

La ciberprotección OT, un valor diferencial

Una de las líneas estratégicas más destacadas dentro de la apuesta de Fujitsu por la ciberseguridad reside en su oferta de servicios profesionales y gestionados específicos para el sector industrial y entornos de producción.

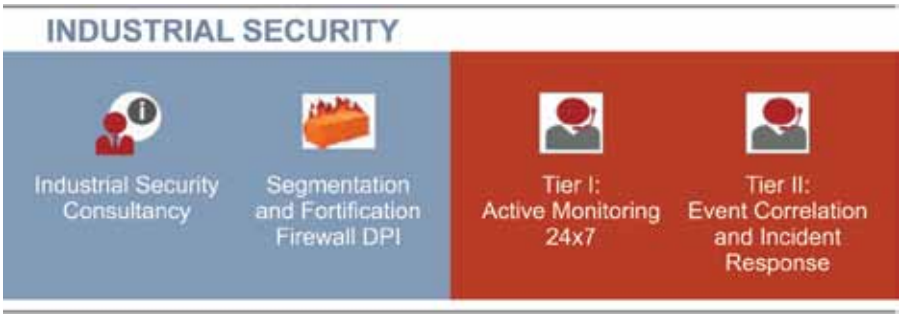
Fujitsu tiene su origen en el sector industrial, y por ello tiene una larga trayectoria y capacidades que la permiten contar con soluciones orientadas a este ámbito, algunos de ellos con una destacada presencia en el mercado español. Esta característica particular, junto con su profunda experiencia como proveedor de servicios e integrador, hacen que su aproximación a la ciberseguridad y la protección de los entornos industriales tenga un valor diferencial.

En la actualidad, la multinacional nipona dispone de un robusto catálogo de servicios en toda la cadena de valor, y que le permiten analizar el caso específico de cada cliente y proporciona una respuesta personalizada basada en las necesidades percibidas, multiplicando la ciberseguridad y potenciando la protección de sus redes e infraestructuras industriales a través de capacidades de inteligencia de ciberamenazas, protección de protocolos de comunicación, acceso remoto OT seguro y monitorización continua.

Fujitsu articula su propuesta de servicios y soluciones en las siguientes cuatro áreas:

• **Consultoría de seguridad industrial.** Fujitsu dispone de un servicio que permite revisar las políticas y procedimientos de ciberseguridad que afecten a los procesos productivos y realizar un análisis y verificación de arquitectura de red, así como de las configuraciones existentes por defecto, usuarios, servicios y aplicaciones innecesarias, a través de herramientas de gestión de eventos y *logs*. Todo ello, bajo una monitorización y captura continua del tráfico en tiempo real. El objetivo final de este servicio es realizar un análisis multidimensional y una auditoría de ciberseguridad de las redes industriales, permitiendo a las organizaciones obtener una visión global y certera de su estado y poder, en base a los resultados, elaborar un plan pormenorizado de mejora.

• **Fortificación y segmentación de redes OT.** La finalidad de este servicio es incrementar el nivel de ciberseguridad de la red de producción, reduciendo su grado de exposición y minimizando el impacto de posibles amenazas en la misma. Para ello, Fujitsu realiza labores de segmentación de red en base a ISA 95 e IEC 62443; análisis de protocolos y comunicaciones con el fin de determinar qué activos y en qué medida impactan en el negocio; inspección y decodificación nativa de protocolos industriales e implantación de cortafuegos DPI para fortificar la red OT; implantación de IDS para la detección de anomalías en base a líneas umbral de comportamiento y patrones, etc.; implantación de tecnologías anti*malware offline*; e, implantación de accesos remotos seguros vía VPN o SSL para asegurar la confidencialidad e integridad de la comunicación.



• **Monitorización Activa 24x7**. A través de este servicio se efectúa la detección no invasiva de amenazas y la activación de los protocolos necesarios ante posibles ciberataques dentro del entorno OT. Los elementos que componen este servicio se singularizan en una monitorización remota en tiempo real de *logs* y alertas, recepción de incidencias de seguridad de clientes a través de distintos canales –teléfono, correo-e, portal web, etc.–, aplicación de procedimientos remotos de comprobación básicos de la monitorización activa, y la elaboración de informes de las diferentes métricas registradas.

• **Gestión de eventos y respuesta ante incidentes.** Fujitsu también responde a las necesidades particulares de las empresas que operan en el sector industrial en lo referente a la gestión de eventos y la respuesta ante incidentes en aras de detectar y dar remedio a las posibles brechas de ciberseguridad que pudieran encontrarse, además de realizar un análisis e implementación de las contramedidas necesarias. Para ello, realiza un estudio y optimización de las distintas alertas y datos procesados por los SIEM para la rápida detección y escalado de las incidencias de ciberseguridad. Asimismo, diseña e implementa respuestas de contención o remedio adecuadas a las amenazas recibidas en los dispositivos gestionados. Y, finalmente, crea una evolución de las políticas aplicadas en función de las amenazas recibidas por el SOC y las alternativas de respuesta disponibles y adecuadas a cada caso.

Fujitsu dispone de un catálogo de servicios para analizar el caso específico de cada organización en función de las necesidades percibidas, multiplicando la protección de sus redes e infraestructuras industriales.

Informe anual de predicciones de ciberamenazas 2017

La IA cambiará el modo de análisis de eventos en los SOC y se usará por la delincuencia organizada para burlar los sistemas de ciberseguridad

Hacer pronósticos siempre es tan arriesgado como necesario. Fujitsu publica desde hace años un informe anual de predicción de ciberamenazas en base al análisis de la información continua de la que dispone por la actividad de su red mundial de SOCs de servicios IT y OT.

La multinacional nipona ha realizado diez predicciones para este año en curso 2017, que en líneas generales están marcando y marcaran la realidad global del comportamiento de la prevención, la defensa y la reacción en la gestión de riesgos de seguridad de la información y la continuidad de negocio.

1. **Muchas empresas seguirán teniendo un punto ciego**. O lo que es lo mismo: los ataques seguirán teniendo éxito, no tanto por la aparición de nuevas amenazas, como por la falta de diligencia de las organizaciones en paliar los puntos ciegos que existen asociados a los ataques a través de canales cifrados no atendidos debido a la falta de capacidad de inspección de tráfico SSL.

2. **La IA cambiará el análisis en los centros de operaciones de ciberseguridad (SOC)**. El uso de técnicas de inteligencia artificial, entre las que se encuentran las de aprendizaje automático va a comportar un cambio sustancial en la forma de clasificar y analizar los eventos, y de lo que deba entenderse por un comportamiento normal o anómalo. Y si fuera esto último, si hay que identificarlos como un intento de ataque. La delincuencia organizada también utilizará capacidades IA para burlar los sistemas de ciberseguridad.

3. **Los delincuentes seguirán atacando las aplicaciones de "core" bancario**. No se espera un freno en los ataques de los delincuentes mediante los caballos de Troya bancarios dirigidos contra las aplicaciones de administración para explotar las vulnerabilidades en las tecnologías heredadas. El caballo de Troya Odinaff, que tenía como objetivo SWIFT a finales de 2016, registrará nuevas variantes y métodos de ataque.

4. **Los atacantes aumentarán el foco contra el mercado móvil**. El uso personal y empresarial masivo de los dispositivos móviles inteligentes y algunas carencias en la seguridad de las plataformas móviles harán que la delincuencia se centre de modo creciente en su ataque con diversos fines, económicos y no económicos.

5. **Los atacantes tendrán como objetivo las ciudades inteligentes**. Éste es un terreno abonado para la delincuencia, que encontrará distintas formas de realizar ataques a los dispositivos inteligentes, a las plataformas de gestión, a las infraestructuras y a los muy diversos procesos de gestión y servicios de las ciudades inteligentes.

6. **La resistencia y la recuperación serán diferenciadores comerciales**. Los agentes del mercado valorarán positivamente la buena gestión de la ciberseguridad de las organizaciones (protección, detección y respuesta), incluida la gestión de la crisis y la recuperación.

7. **La custodia de datos se convertirá en un punto clave para todas las organizaciones**. Los inversores, los accionistas, los clientes, los reguladores y otros interesados demandarán de modo creciente garantías del correcto tratamiento de datos (personales y no) en las organizaciones.

8. **Los clientes globales exigirán inspeccionar sus cadenas de suministro de seguridad de datos**. Por razones de responsabilidad corporativa y buen gobierno, y por razones de corte legal, las organizaciones verificarán el correcto tratamiento de los datos personales que traten y de sus datos corporativos a sus proveedores.

9. **Las juntas directivas tratarán la seguridad IT de forma rutinaria**. Este hecho, que en 2016 empezó a manifestarse, se generalizará durante 2017, y no solo en el sector financiero.

10. **Las malas prácticas de IT rutinarias seguirán causando la mayor parte del daño evitable**. Un sorprendente número de empresas no lleva a cabo las tareas de gestión y organización que reducen los riesgos (parcheado, gestión de identidades, autenticación, revisión de privilegios…). Esto seguirá ocurriendo este año y siendo fuente de problemas de ciberseguridad.

General Data Protection Regulation (GDPR)

Metodología Fujitsu para facilitar la adaptación

¿Cumple su organización con la nueva regulación europea de protección de datos?

Fujitsu dispone de las herramientas y el conocimiento para ayudarle a abordar con garantías el proceso de adecuación al nuevo Reglamento.

Infórmese en: **www.fujitsu.com/es/ciberseguridad**
info.spain@ts.fujitsu.com

shaping tomorrow with you