

La Seguridad como un todo

La Seguridad de Mapfre se ha planificado con una definición vertical y central, pero se aplica de manera transversal e integral

EN MENOS DE UN AÑO, MAPFRE HA PUESTO EN MARCHA E IMPLANTADO UN CENTRO DE CONTROL GENERAL, DESDE EL QUE GESTIONAR OPERATIVAMENTE SU CONCEPTO Y MODELO DE SEGURIDAD INTEGRAL. UN CAMBIO RADICAL Y POSITIVO, PARA PROTEGER LOS ACTIVOS DEL NEGOCIO, QUE HA IMPLICADO A TODAS LAS ÁREAS DE LA COMPAÑÍA, ASÍ COMO A TODO EL PERSONAL.

Tx: Mercedes Oriol Vico.
Ft: Ana Borredá.

MAPFRE CUENTA con una Subdirección General de Seguridad y Medio Ambiente (DISMA), desde la que se dirigen y gestionan todos los asuntos relacionados con medio ambiente y seguridad, incluyendo las competencias relativas al marco regulatorio (LOPD, etc.), continuidad de negocio y protección contra incendios. Dentro de ella se enmarca la Dirección de Seguridad, liderada por Guillermo Llorente, director de Seguridad de Mapfre, y de la que dependen cinco subdirecciones.

Según Guillermo Llorente, a nivel estratégico, el proceso de conformación de esta estructura de Seguridad en Mapfre ha pasado por fases de defi-



La Central Receptora de Alarmas (CRA), ubicada junto al Centro de Operaciones de Seguridad de la Información (COSI), cuenta con personal de manera permanente, que ofrece soporte a la seguridad de todos los edificios de Mapfre que están conectados a ella.

nición de una Política de Seguridad y de un Plan Director de Seguridad, una progresiva asunción de competencias y funciones y una progresiva adaptación de la estructura de la organización al concepto de funcionamiento definido en el Plan Director y la Política de Seguridad. En este proceso se ha intentado aplicar siempre una visión global: "Desde Seguridad, miramos la organización como un todo, pues ésta afecta a todos los procesos y actividades, a todos los medios e instalaciones y a todo el personal, con una definición vertical y central, pero con una aplicación transversal", explica Llorente. Desde esa visión global, pretenden

dotar a Mapfre de una Seguridad Integral, intentando proteger todos sus activos (personas y patrimonio, información e imagen) frente a todo tipo de amenazas (terrorismo, delincuencia, emergencias, catástrofes, etc.), y conseguir que esa protección sea constante y permanente.

Desde la Subdirección de Seguridad en Aplicaciones, que dirige Jacinto Muñoz, se lleva a cabo la gestión de identidades y criptografía, la seguridad en las aplicaciones a lo largo de todo su ciclo de vida y las revisiones tecnológicas de portales y aplicaciones.

La Subdirección de Infraestructuras Tecnológicas, de la que se encarga

Todo funciona de manera combinada. El SCA y la CRA estarían dentro de la tradicionalmente conocida seguridad física y el COAS y el COSI estarían en lo que se conoce habitualmente como seguridad lógica o informática

Andrés Peral, se centra en la gestión de vulnerabilidades, en los sistemas de información, la contingencia informática y el diseño de arquitectura tecnológica de seguridad (*firewall, antivirus, antispam...*).

Por otra parte, en la Subdirección de Explotación de Tecnologías de Seguridad, que dirige Lionel Güitta, se da servicio al resto de las áreas de seguridad. Estos tecnólogos de seguridad, se encargan del mantenimiento y explotación del laboratorio de investigación, las aplicaciones de seguridad -plataformas antivirus, *antispam...*-, la administración de equipos, etc.

El terreno de las infraestructuras físicas es competencia de la Subdirección de Protección de Instalaciones, con responsabilidad en el diseño e implantación de las medidas de protección pasiva, los Sistemas Electrónicos de Seguridad (SES) y los de Protección Contra Incendios (PCI). Protegen así más de medio centenar de edificios singulares y emblemáticos de Mapfre, unas 3.500 oficinas.

Por último, en la Subdirección de Operaciones, que dirige Joaquín Juárez, se integra el Centro de Control General (CCG), y es donde se diseñan e implantan los Planes de Autoprotección y de Seguridad de las instalaciones y de los eventos, se dirigen investigaciones y se coordina la respuesta a incidentes, además de ocuparse de la seguridad personal de los altos cargos de la compañía.

Centro de Control General (CCG)

El CCG es la piedra angular del sistema implantado, y donde se plasma, de una manera más nítida, el concepto de Seguridad Integral que se aplica en Mapfre. En el CCG existen cuatro órganos clave: El Centro Operativo de

Administración de Usuarios (COAS), para la gestión de accesos a aplicaciones y redes. El Centro Operativo de Seguridad de la Información (COSI), para la vigilancia y monitorización de equipos informáticos y redes. El Sistema de Control de Accesos (SCA), para la gestión de acreditaciones de accesos a edificios y zonas restringidas de los mismos. Y la Central Receptora de Alarmas (CRA), para la vigilancia y monitorización de edificios y oficinas.

Todo funciona de manera combinada, obteniéndose sinergias de la interrelación entre las partes. El SCA y la CRA estarían dentro de la tradicionalmente conocida seguridad física; y el COAS y el COSI estarían en lo que se conoce habitualmente como seguridad lógica o informática. Sin embargo, el CCG juega con otros dos posibles tándem de este completo puzzle: el del COAS y el SCA, que permiten la habilitación para el acceso; y el del COSI y la CRA, que realizan la monitorización. La utilización de tecnología IP en la CRA y el SCA hace posible y facilita esta integración.

Guillermo Llorente argumenta que "la seguridad de un activo debe entenderse como la resultante de las medidas (físicas y lógicas) destinadas a protegerlo; en la que las medidas de seguridad son más eficaces y eficientes cuando se aplican de forma complementaria y en forma escalonada". Para ello, un pilar fundamental es la centralización en el CCG de servicios y actuaciones, ya que, en palabras de este directivo, "redunda en la optimización de procesos, con el consiguiente ahorro de costes y en un aumento del control de las operaciones, dotándonos de una mayor capacidad de respuesta a incidentes".

Daniel Largacha, máximo responsable del CCG y Análisis Forense, es una de las personas clave en el equipo de Guillermo Llorente, y procede de la Dirección General de Tecnología y Procesos (DGTP) de Mapfre -ubicada en Aravaca-, donde realizaba funciones análogas a algunas de las hoy integradas en el área de Seguridad.

Desde su experiencia anterior, Largacha nos señala la evidente y



David Hernán, jefe del Departamento COSI, muestra a RED SEGURIDAD, la consola de gestión de eventos, Security Information Manager (SIM), con la que trabajan.



En la imagen algunos de los directivos y expertos de la Subdirección General de Seguridad y Medio Ambiente de Mapfre, en concreto, pertenecientes a la Dirección de Seguridad, que lidera Guillermo Llorente (primero en la primera fila a la izquierda). Junto a él, en el centro, Joaquín Juárez, subdirector de Operaciones, y Daniel Largacha, responsable del CCG y Análisis Forense. En la línea inferior, de izquierda a derecha: Javier Cepeda, jefe de la CRA; David Hernán, jefe del COSI; y José Manuel Ortiz, jefe del COAS.

significativa diferencia de tamaño entre el área de tecnología (DGTP) y de seguridad, a favor de aquella, así como la necesaria coordinación entre ambos y el establecimiento de una relación "entre iguales".

Uno de los problemas que tradicionalmente se identifican en la ubicación de responsabilidades de seguridad en el área de tecnología, indica Daniel Largacha, es el conflicto de intereses que les surge a los directivos de esta área cuando, en el día a día, tienen que atender, por un lado, a los requerimientos de negocio sobre plazos, etc., y por otro, a la necesidad de implantar criterios de seguridad en los desarrollos y sistemas. Por ello MAPFRE optó por esta segregación de funciones, aunque siempre dentro de una necesaria y cercana colaboración.

Como no podía ser de otra manera, el proyecto de Seguridad Integral que ha realizado Mapfre ha contado con socios de excepción. Uno de los compañeros de trabajo imprescindible ha sido la empresa Sabia, Bioingeniería Aragonesa. Su director general, Gerardo Benavente, asegura que lo que se ha hecho ha sido "integrar la gestión y la seguridad, basado en inteligencia de negocio; *Business Intelligent*, como acelerador del negocio y de la información que se maneja".

De esta forma, se dota a los Centros de Proceso de Datos (CPD) de la compañía del entorno más seguro posible.

El proyecto de Seguridad Integral de Mapfre, plasmado en el CCG, se ha llevado a cabo de forma rápida y eficiente, partiendo de una situación en 2007 que Daniel Largacha describe del siguiente modo: "La CRA estaba en fase avanzada; el COAS y el SCA en desarrollo; y el COSI en definición". Hoy todos ellos están a pleno funcionamiento.

El COAS, un escenario nuevo

El Centro Operativo de Administración de Usuarios (COAS) supone un cambio de paradigma en la gestión de usuarios y autorizaciones en Mapfre. Dicho órgano es concebido, desde su definición por la Comisión Delegada de la multinacional aseguradora, como un elemento común y centralizador, basado en el concepto de ventanilla única para la gestión de usuarios. Desde sus inicios, se ha ido centralizando en el COAS la gestión de usuarios con un enfoque transversal, como servicio global al conjunto de la organización.

La gestión de identidades realizada por el COAS, definida desde la Subdirección de Seguridad en Aplicaciones, se basa en la definición de colectivos, entendidos éstos como conjuntos de usuarios con característi-

cas funcionales similares y que requieren del mismo conjunto de accesos. La relación entre colectivos y autorizaciones se articula a través de una matriz de autorización, definida a partir de los requisitos especificados por las diferentes áreas de negocio.

Este planteamiento tiene como caso de éxito a la estructura de mediadores de la Red Comercial de Mapfre. "Quedan así predefinidos los accesos que un usuario debe tener a los distintos sistemas en función de la actividad laboral que desempeñará para Mapfre. Es un sistema que combina seguridad y operatividad, flexible y sujeto a excepciones", expone Daniel Largacha.

Este enfoque de administración por colectivos, junto con una aproximación basada en la optimización de procesos ha dado muy buenos resultados, según sus responsables, y ha hecho posible reducir el tiempo requerido para dar de alta a un usuario en el conjunto de sistemas de información de Mapfre que necesita para desarrollar su actividad laboral, hasta tan sólo tres horas a día de hoy.

Por otro lado, para la seguridad de una organización, tan importantes son las altas en los sistemas como las bajas. En opinión de Largacha, este es un aspecto que habitualmente "se olvida y no se cuida en algunas organizaciones".



En Mapfre, las operaciones de alta y baja de usuarios están sincronizadas con la herramienta de gestión de Recursos Humanos corporativa. El proceso de alta automatizada lleva asociado la generación del identificador de usuario (Nombre Único de Usuario MAPfre -NUUMA-), junto con los servicios comunes que deben tener todos los trabajadores de Mapfre: acceso a Internet, correo electrónico y Portal Interno.

Daniel Largacha manifiesta el gran cambio que todo esto también ha supuesto para el departamento de Recursos Humanos, al tener que modificar sus procesos internos para alinearlos con el objetivo de agilizar la gestión de usuarios corporativa.

El COSI, un verdadero CERT

El Centro Operativo de Seguridad de la Información (COSI) es el *Computer Emergency Response Team* (CERT) o *Security Operation Center* (SOC) de Mapfre, desde donde se vigila y se analiza la seguridad de las redes y sistemas de información de Mapfre. Asimismo, desde este órgano, se coordina y lleva a cabo la respuesta a incidentes de seguridad acaecidos en los sistemas de información.

Largacha aclara que al igual que en el caso del COAS, son otras Subdirecciones quienes han definido y diseñado los procesos y herramienta soporte asociados a los servicios que se prestan en el CCG. Y es en los órganos de éste, en este caso en el COSI, donde se lleva a cabo la operación, de acuerdo con esas directrices.

El COAS, desde donde se gestionan bajas y altas del personal, cuenta también con personal externo e interno. El responsable del equipo es José Manuel Ortiz, de pie a la derecha.

"En el COSI se controlan, estudian y analizan las redes con, entre otros medios, sistemas de detección de intrusión (*Intrusion Detection System* -IDS-), que son los que 'escuchan' la red y buscan determinados patrones de ataque", añade Largacha. La detección de uno de estos patrones genera eventos que se registran en la consola de gestión centralizada de seguridad.

Y es que, hablando en cifras, cada día se reciben y procesan más de 51 millones de eventos generados en la red y servidores de Mapfre, con un inventario de activos tecnológicos de más de 25.000 equipos.

Respecto al *spam*, según criterios de clasificación establecidos por la consultora Gartner Group, Mapfre se encuentra en la banda alta de las estimaciones mundiales de porcentaje de *spam* recibido con respecto al correo total (entre un 85 y un 95 por ciento). Y es que de los más de cuatro millones de correos electrónicos que llegan diariamente a Mapfre, hay únicamente alrededor de unos 245.000 *e-mails* válidos.

En lo relativo al acceso a Internet, a diciembre de 2008, la multinacional de Seguros tenía más de 120 millones de accesos al mes. Aún así, según el director de Seguridad, Llorente, "sólo el 0,5 por ciento del total de intentos de acceso a Internet por personal propio se bloquean".

A partir de las herramientas disponibles, se ha definido un procedimiento *antiphishing*. El responsable del CCG y Análisis Forense manifiesta, seriamente, que la estrategia para luchar contra el *phishing*, se hace en estrecha colaboración, con todas las partes implicadas, contando con la colaboración de las principales entidades financieras con las que Mapfre se relaciona: "Si se detectan casos, Mapfre, además de ponerse en contacto con la entidad financiera, comunica "personalmente" el intento, o el fraude, a los afectados para que lo comuniquen inmediatamente a su banco".

Como puede deducirse de lo expuesto anteriormente, la relevancia de este centro para Mapfre es muy significativa. Para Llorente "el COSI recaba información de manera centralizada, de la que antes no disponíamos (o nos costaba mucho disponer), lo que representa un salto cualitativo muy importante en la detección y respuesta frente a incidentes de seguridad".

Laboratorio de Investigación de Seguridad

En este laboratorio de Investigación de Seguridad, que gestiona el área de la que se encarga Lionel Güitta, cuentan con 16 puestos de trabajo para la realización de pruebas e investigaciones a disposición de todas las áreas.

El equipo de laboratorio es un rack para herramientas y maquetas de soluciones de seguridad, independiente del resto de la red de Mapfre, con ocho servidores con aumento de la capacidad de proceso y almacenamiento, gracias a 15 o 20 servidores virtuales. Sin embargo, el entorno en el que se trabaja y se hacen las pruebas es lo más parecido a lo que hay en producción. El segundo rack es exclusivo para equipos de producción para la Dirección de Seguridad, con servidores para investigaciones, en los que virtualizan la máquina.

El laboratorio es un área de acceso restringido, controlado desde la Central Receptora de Alarmas, y su configuración permite el trabajo de varios equipos simultáneamente.

Para Mapfre, la seguridad parte de la correcta identificación y valoración de los activos a proteger, siendo necesario entender y mantener las relaciones entre los mismos, independientemente de su naturaleza.

En este sentido, José María García, jefe del Departamento de Gestión de Vulnerabilidades, nos habla del sistema Piscis, desarrollado por los técnicos de la Dirección de Seguridad, que integra, de forma gráfica e intuitiva, sistemas de información, usuarios y ubicación física. Dicho sistema se basa en la herramienta de inventariado de activos tecnológicos y gestión de vulnerabilidades de la compañía. "En el proceso aún nos queda el completar las relaciones entre el inventario de activos de información y el resto de elementos, para saber rápidamente qué impacto potencial puede tener un determinado ataque, y eso es algo en lo que estamos centrando nuestros esfuerzos", dice Llorente.

El SCA, hacia la credencial única

El Sistema de Control de Accesos (SCA) es una herramienta desarrollada plenamente por Sabia, Bioingeniería

Aragonesa. En el SCA se centraliza la gestión de accesos a los edificios y zonas restringidas conectados al sistema con una única tarjeta. Para Daniel Largacha se trata de "un logro de un importante nivel de complejidad y con un muy importante impacto en lo que se refiere a aumento de la seguridad y ahorro de costes, básicamente porque Mapfre posee inmuebles singulares, muchos y muy dispersos; y por la anterior diversidad de tarjetas de identificación y control, incompatibles entre sí, que había en el pasado, con la subsiguiente dificultad en materia de gestión".

Según Gerardo Benavente, "la tarjeta se ha desarrollado en evolución de la tecnología de *Radio Frequency Identification* (RFID) para posibilitar el acceso biométrico". En este sentido, Benavente ahonda: "La creación de SCA es la virtualización de lo físico y lo químico, sobre un sistema de infraestructura IP, concebido en tecnología IP, con un interfaz único, único controlador de usuario, que mejora el control de gestión de acceso". A lo que suma Daniel Largacha: "Todo ello, integra-

do en los sistemas de la compañía, enlazado con el sistema de Recursos Humanos, desde el que al igual que al empleado se le desencadena la generación de los accesos lógicos, también se le emite la tarjeta única de identificación, y ambos elementos se dan de baja cuando esa persona deja de estar "activa" en Mapfre, y eso para nosotros es fundamental".

El SCA es el primer paso hacia un objetivo mucho más ambicioso: conseguir una única credencial para el acceso lógico y físico. "Es un proyecto común a toda la Dirección de Seguridad, cuyos beneficios están claros: autenticación robusta, facilidad para el usuario (un único PIN en la tarjeta), optimización de la gestión (centralizada en el CCG) e integración con sistemas de cifrado de disco (blindaje de puestos)", enumera Guillermo Llorente.

En este sentido, desde la Dirección de Seguridad, de la que es responsable Llorente, han puesto en marcha una nueva PKI corporativa. "Nuestro objetivo es tener una herramienta de gestión del ciclo de vida de los certificados digitales e integrar los mismos en la tarjeta

■ Una base sólida

EL SCA ES UN PRODUCTO que engloba en una única interfaz, un sistema de control de accesos, un sistema completo de seguridad, un sistema de control de presencia, y que permite la gestión de funcionalidades relacionadas con la inmótica. Esto tiene ventajas evidentes en el proceso de implantación, ya que simplifica notablemente el proceso de instalación y de aprendizaje y en el proceso de mantenimiento.

El SCA incorpora un *software* gráfico que permite visualizar mediante un sistema de planos, y en tiempo real, el estado del sistema. Ante una alarma y a la vista del plano se puede valorar la gravedad de la detección de una intrusión por el sistema. Ante una alarma y a la vista de plano, se puede valorar la gravedad de la detección de una intrusión por el sistema. Esto es una ayuda básica para controlar las falsas alarmas.

Dentro del sistema de seguridad, se ha integrado el manejo de grabadores de imágenes. Ante la generación de una alarma se puede mostrar de forma automática la imagen recogida por uno o varias cámaras de la instalación. Como en el apartado anterior, esto permite controlar el número de falsas alarmas.

El hecho de integrar el control de accesos con seguridad permite la generación de alarmas ante intentos de accesos reiterados no permitidos. También ante la apertura de accesos sin intervención del sistema. Estas alarmas serán tratadas de la forma más conveniente por el personal del CRA, aplicando los protocolos adecuados.

Dentro del SCA, destacamos su módulo de visitas. Esta implantado en la Torre Mapfre de Barcelona. En dicha instalación se están gestionando más de 1.000 visitas al día, con tiempos de acreditación inferiores a cinco segundos.

Los diferentes componentes del SCA se comunican mediante protocolo IP nativo. El uso de una conexión IP con las placas que forman el sistema, proporciona un conjunto de ventajas asociadas e innatas a este protocolo:

- La comunicación con el *hardware* esta permanentemente supervisada. Cualquier pérdida de conectividad implica la generación de la correspondiente alarma, activándose los protocolos de actuación adecuados.
- En el caso de disponer de una red informática, no hay un coste adicional para los procesos de comunicación con los elementos instalados.
- La actualización inmediata de la información en cada placa.
- Se dispone de información en el centro de control del estado del sistema en tiempo real.

El SCA trabaja con una única base de datos central. Además de las lógicas ventajas de mantenimiento que esto proporciona, permite la gestión centralizada de permisos. Desde cualquier punto de la red se puede gestionar los permisos de acceso a cualquiera de los edificios conectado al sistema.

A pesar de disponer de un repositorio de datos central, la decisión de la apertura de un acceso, la toma siempre localmente la placa. Esto permite el funcionamiento correcto del sistema ante pérdidas de conectividad entre los elementos.

Gerardo Benavente, director general de Sabia Bioingeniería Aragonesa

de acreditación única, un proyecto que está en marcha".

Pero todo lleva su ritmo. "Este año y el siguiente -relata Guillermo Llorente- la credencial única se va a implantar inicialmente para colectivos muy específicos, en concreto para los usuarios móviles".

Para lograr el objetivo de la credencial única, la coordinación entre el SCA y el COAS es fundamental. "El SCA y el COAS son órganos muy cercanos, pues ambos gestionan "accesos"; y con la CRA y el COSI tendremos que seguir un planteamiento análogo, pues ambos "monitorizan", comenta Largacha.

Una CRA de actividad propia

Mapfre cuenta hoy con una Central Receptora de Alarmas (CRA) de actividad propia, homologada por la Dirección General de la Policía (Ministerio del Interior), es decir, que está destinada a dar servicio exclusivo a las instalaciones de Mapfre, y no a terceros.

En el CCG, tienen tres turnos de personal (mañana, tarde y noche), con sus respectivos responsables. Dentro del recinto (sala blindada) donde se sitúa la CRA, está también el COSI, del que es responsable David Hernán, y el SCA.

Para Javier Cepeda, jefe de la CRA, "la gestión de la CRA de Mapfre es más amplia que una la de una CRA normal, ya que tenemos que garantizar la continuidad del negocio, y si ocurre algo, se tienen que restablecer las oficinas afectadas, con los criterios de seguridad adecuados para desarrollar la actividad, con objeto de poder estar en funcionamiento a la mayor brevedad". Para ello, en la CRA están perfectamente coordinados con otras áreas, y nunca quedan oficinas desconectadas por la noche -algo posible gracias a la tecnología IP-, así como ante cualquier incidente, habitualmente nocturno. La reparación de los daños, impulsada desde la CRA, se realiza durante la misma noche en la que se produce el incidente, permitiendo la continuidad de la actividad normal de la oficina a la mañana siguiente.

"Ha habido veces que el empleado o delegado, no ha sabido del percance hasta que ha notado que su llave habitual no abría la puerta", nos cuenta

Cepeda. "Se le da formación al usuario en detección de falsas alarmas, se estudian y se toman las decisiones, gracias a lo cual hoy solo tenemos alrededor de un dos por ciento de falsas alarmas; casi todo lo que llega a la Policía es verdadero", concluye Cepeda.

En esta línea, Largacha apoya diciendo que "la bidireccionalidad que permite el sistema implantado y la CRA propia ha permitido que el importante problema de las falsas alarmas sea prácticamente inexistente en esta CRA".

De hecho, el pasado mes de mayo hizo dos años de la homologación de la CRA de Mapfre (hoy tiene más de

de 60 armados diarios desde el CCG (sin intervención humana).

Hasta la fecha, entre otras actuaciones, se han evitado más de 40 robos, se ha intervenido un atraco, se han tramitado tres inundaciones.

Investigación total

David Largacha especifica que, cuando hay algún problema, toda esta estrecha integración de sistemas y profesionales permite que se lleve a cabo una adecuada y oportuna respuesta e investigación de cada incidente.

Y es que, como defiende Joaquín Juárez, subdirector de Operaciones, "en Mapfre hay un muy alto nivel de

Según uno de los directivos de Mapfre, la seguridad no tiene que ser secreta, sino los procedimientos

2.500 oficinas conectadas) y no han tenido ni un apercebimiento por parte del Ministerio del Interior.

En lo relativo al diseño del sistema, hay numerosos aspectos destacables. Por un lado, la planificación de la instalaciones de Sistemas Electrónicos de Seguridad (SES) no se hace con instalación masiva de detectores o cámaras, sino más bien "mediante una asignación lógica de zonas, identificando los puntos vulnerables de cada área; un sistema racional, normalizado y estandarizado de implantación de SES", narra Joaquín Juárez, subdirector de Operaciones.

Pese a ello, Javier Cepeda hace notar y describe la complejidad de Mapfre, señalando que en alguno de sus edificios, hay instaladas 102 cámaras y 900 sensores. "El disponer de una CRA y de una herramienta como la que Sabia nos proporciona, nos da muchísima flexibilidad y posibilidad de identificación e implantación constante de mejoras", puntualiza Javier Cepeda.

Como indicadores más significativos, desde la CRA se gestionan más de 700 alarmas al mes y y una media

desarrollo e implementación tecnológica y un grupo de profesionales de excepción, como corresponde a una empresa con presencia en más de 42 países".

Este directivo, que viene de las Fuerzas Armadas, tiene una visión de la seguridad transparente: "La seguridad no tiene que ser secreta: secretos son los procedimientos".

Líneas de actuación y avance

Una de las líneas de actuación en las que están inmersos en la Dirección de Seguridad es la puesta en marcha de una plataforma criptográfica, infraestructura que proporciona servicios de firma electrónica, validación de firma y custodia de documento firmado, enfocada principalmente a optimizar los procesos existentes, tanto internos como externos, permitiendo la adaptación a la legislación vigente (Ley para el Impulso de la Sociedad de la Información -LISI-). Como primer hito, Mapfre ha conseguido ofrecer a sus clientes acceso (identificación) y contratación del alta (firma) a la Oficina Internet Mapfre mediante DNI electrónico y certificado de la Fábrica Nacional de Moneda y Timbre (FNMT). ■



Tx y ft: MOV.

En Mapfre han conseguido integrar la tradicional seguridad física, con la seguridad lógica dentro del Área de Seguridad y Medioambiente, bajo un subdirector general que reporta directamente al vicepresidente ejecutivo de la compañía. En concreto, usted es el responsable directo del área de Seguridad. ¿Cuándo deciden dar este importante paso hacia la integración total y gracias a qué y a quiénes ha sido posible?

Desde la concepción de un área específica de Seguridad en Mapfre, se apostó de forma clara e inequívoca por un enfoque integral de seguridad y así se plasmó en, el aquel entonces, tremendamente novedoso Plan Director de Seguridad de Mapfre. Hablamos del año 1996, en que ya se exponía, como primer criterio básico de actuación, el de la Seguridad Integral, además de, en consecuencia, atribuir responsabilidades, y competencias asociadas, en ambas áreas (física y lógica) al órgano recién creado.

En este sentido, entiendo que el mérito hay que atribuírselo a la organización en general y al vicepresidente y al subdirector general en particular, pues han sido quienes han impulsado y dirigido en primera persona este proyecto.

Por otro lado, desde un punto de vista táctico y operativo, la integración ha sido posible gracias a la flexibilidad y profesionalidad de las personas que componen la organización de Seguridad de Mapfre, que pese a provenir de culturas diferentes, han sabido identificar y aprovechar las sinergias existentes entre las distintas áreas de la Seguridad. Al final, ha sido la labor de todos ellos, la que ha hecho posible la implantación de

ENTREVISTA

Guillermo Llorente Director de Seguridad de Mapfre

"Cuando la falta de visión hace que el "cortoplacismo" se convierta en estrategia, se asumen riesgos inaceptables"

Llorente se caracteriza por hablar claro y alto sobre temas espinosos por los que hoy pasa la Seguridad. Sin querer sentar cátedra -como otros directivos prepotentes que, además, no tienen mucho qué contar-, uno no se cansa de escuchar la sencillez con que comparte el conocimiento este líder nato.

este enfoque integral, que es la seña de identidad, y de orgullo, de la Seguridad de Mapfre como organización.

Una de sus responsabilidades es la protección de activos, la protección de la información; y una empresa como Mapfre, en la que sus activos se basan precisamente en la información que manejan de sus clientes, pero también en el patrimonio y en la protección de datos de sus asegurados y sus empleados, es un objetivo harto "suculento". ¿Cuáles son los principales riesgos que sufren y las amenazas más habituales?

Como bien dice, para Mapfre la protección de su información, tanto la de sus clientes como la de sus empleados, es una necesidad crítica, pues de ella puede depender la existencia de la propia compañía y a ella dedicamos nuestros mayores esfuerzos.

Las amenazas y riesgos a los que nos enfrentamos en Mapfre son los mismos a los que puede enfrentarse cualquier compañía multinacional en la actualidad: robos, fraude, malware, pérdidas de datos, etc. La actual coyuntura está provocando un repunte en las actividades delictivas y esto nos hace estar más alerta si cabe, teniendo siempre presente, que estamos en una carrera de fondo, frente a un adversario global, que no duerme y que tiene, al menos, tantos medios como nosotros.

En cualquier caso, todos los que trabajamos en Mapfre, y en especial en Seguridad, no olvidamos, ni podemos permitirnos hacerlo, que el funcionamiento de Mapfre se basa en su prestigio y en la confianza que nos depositan nuestros clientes, por lo que en

justa compensación y reciprocidad, para Mapfre, el atender a sus compromisos con ellos, y la protección de sus datos es uno de éstos, constituye nuestra prioridad más absoluta y a la que dedicamos todos los medios necesarios para garantizar la adecuada protección de los mismos.

El plan director de seguridad que ustedes han definido, tiene como piedra angular lo que denominan Centro de Control General (CCG), en el que se encaja como un verdadero puzzle cuatro áreas: el Centro Operativo de Administración de usuarios (COAS), el Centro Operativo de Seguridad de la Información (COSI), el Sistema de Control de Accesos (SCA) y la Central Receptora de Alarmas (CRA). De nuevo, una muestra clara de que el mundo de la seguridad tradicional y el de la seguridad informática no solo pueden convivir, sino que deben convivir. Usted, que procede del Ejército (teniente coronel de infantería), ¿por qué cree que hay cierta reticencia entre ambos frentes, si me permite la expresión?

Personalmente -y es solo una opinión personal- creo que es un problema básicamente cultural y de desconocimiento, y tal vez, por ese desconocimiento de desconfianza mutua. La seguridad tradicional suele estar situada organizativamente cerca de la Alta Dirección y, desde esa posición, relativamente "cómoda", con un ámbito de actuación cercano y conocido, es reacia a abordar aspectos de índole tecnológica que, desde lejos y a primera vista, entiendo le puedan parecer verdaderos "arcanos", y cuya aportación de valor a su actividad diaria, tal vez no vean del todo clara.

Desde la perspectiva de la tradicionalmente llamada seguridad de la información, creo que pudiera haber cierta desconfianza frente a la integración de ambas áreas, por lo que entiendo puede ser percibido por algunos, como una posible pérdida de poder frente a la seguridad tradicional, por la posible ventaja que ésta tendría en la integración, al haber estado históricamente más cercana al Comité de Dirección.

Además, desde ese área de la seguridad lógica, asumo que puede ser difícil entender la complejidad y sofisticación de la seguridad tradicional, lo que hace que se puedan percibir sus actividades como de escaso valor añadido. A lo anterior, estimo que habría que añadir que este área de la seguridad lógica depende tradicionalmente de TI, por lo que creo son fácilmente comprensibles, las posibles y humanas reticencias por parte de los directivos del área de Tecnología, a que un área externa conozca lo "menos bueno" o "más vulnerable" que hay en su área de competencia.

Frente a esto, la realidad se impone tozudamente: la tecnología está presente en ambos mundos y el nivel de protección de un determinado activo lo da la suma ponderada de las medidas de protección que lo salvaguardan. Medios y medidas dispuestas o implantadas coordinadamente y de forma escalonada (multicapa) en todos los ámbitos (instalaciones, infraestructuras, aplicaciones, personas, etc.), y que, personalmente, sólo veo capaz de gestionar adecuadamente, desde una visión global.

Los "malos" buscan comprometer los activos, ya sea de forma física, tecnológica o mediante ingeniería social, y nosotros no podemos tratar estas cuestiones ni hacer frente a esta amenaza de forma aislada o fraccionada.

¿Cómo han abordado la resistencia al cambio que presentan algunos directivos y profesionales cuando hay un cambio estructural como este?

Como he comentado anteriormente, la realidad es que no hemos tenido cambio que gestionar; ya desde el principio se concibió un enfoque integral e integrador, que hemos sido capaces de llevar a una estrategia, visión y mensaje comunes, que creo todos los componentes del área de Seguridad hemos entendido e interiorizado.

Con este enfoque, desde las restantes áreas de Mapfre, se ha llegado a entender y asumir de manera natural que todos los aspectos relativos a Seguridad se tratan desde nuestra área, independientemente de la naturaleza de los mismos. Esto simplifica nuestra relación con la organización, aumentando tremendamente nuestra eficacia y eficiencia, con la consiguiente optimización de esfuerzos y costes.

Como bien sabe, hoy día una de las palabras que más se utiliza en las organizaciones es la de "líder", y comienza a instaurarse igualmente en el sector de la Seguridad. Sin embargo, parece que su uso indiscriminado, aplicado a cualquier tipo de dirección y persona, adolece su esencia más elemental. Siendo hombre cabal, como es usted, ¿Cómo debe ser un verdadero líder en Seguridad? ¿Son realmente necesarias tantas siglas o es más importante saber delegar en un buen equipo?

Gracias ante todo por lo de hombre cabal, pues es un adjetivo en nada desdeñable y que considero parte intrínseca a las cualidades que entiendo debe tener un buen líder. A este respecto, creo que la definición de líder de la Real Academia Española (RAE), como "Persona a la que un grupo sigue reconociéndola como jefe u orientadora", sintetiza la esencia de lo que debe ser un líder en Seguridad.

determinación extraordinaria", por ese punto de osadía y valor que creo se necesita en nuestro ámbito para afrontar y solventar problemas complejos, que en ocasiones nos corresponde "poner sobre la mesa"; problemas con múltiples derivaciones e implicaciones, y que es necesario afrontar asumiendo riesgos, pero siempre tras haber tratado (conseguirlo no siempre es posible) de identificarlos y evaluarlos.

Usted es uno de esos líderes que delega en un importante y preparado equipo de profesionales. ¿Qué supone para usted "su gente"?

Disponer de un equipo de personas con criterio, autonomía, ilusión y compromiso, es fundamental, y en este sentido, yo me considero tremendamente afortunado. Creo sinceramente que ha sido una de las partes más satisfactorias de esta etapa de actividad profesional en Mapfre.

■ ■ "El nivel de protección de un activo lo da la suma ponderada de las medidas que lo salvaguardan" ■ ■

Bajo mi punto de vista, y de lo que a mi me enseñaron, el líder debe aspirar a contar no sólo con el poder (la Potestas), sino también con la autoridad (la Auctoritas) necesarias para guiar y sacar el máximo partido del grupo de profesionales a su cargo, que en un caso como el de Mapfre, implica personas con distinta formación, experiencia, trayectoria, visión, etc. Personas con capacidades distintas, pero todas ellas necesarias para dar respuesta a unas necesidades de seguridad muy complejas como lógicamente corresponde a una gran empresa multinacional como es Mapfre.

Aquí aparece también otra característica que creo clave para un líder, que es la capacidad de Dirección, entendida esta, como la capacidad para analizar situaciones, identificar objetivos, definir estrategias y asignar medios y misiones a sus colaboradores, asegurando la necesaria coordinación entre ellos, a fin de lograrla orientación a la que hace referencia la definición. Todo ello, a la vez que establece los mecanismos necesarios que le permitan reevaluar permanentemente ese escenario a fin de identificar la necesidad de introducir suaves cambios o, Dios no lo quiera, golpes fuertes de timón.

Otra definición de líder con la que, en parte, me gusta sentirme identificado, es la de "persona ordinaria con una

Yo no concibo el día a día sin mi equipo: son ellos los que hacen girar la rueda, y me satisface reconocer que tengo la suerte de aprender algo todos los días, tanto profesional como personalmente. En este sentido, una de las tareas a las que me dedico con más ahínco, y que considero como una obligación personal, es la de "vender" el trabajo que hacen, para que la organización se sienta tan orgullosa de ellos como lo estoy yo mismo.

En todo el proceso y proyecto del CCG, Mapfre ha trabajado mano a mano con la empresa Sabia. ¿Cómo es la relación con este socio? ¿Tienen pensado poder comercializar de algún modo, y en un futuro, el modelo que se está implantando en la compañía aseguradora?

Con Sabia hemos llegado a la esencia de lo que es tener un socio y no un proveedor, con todo lo que ello implica. Una relación entre partes que quieren tratarse como iguales siempre parece más complicada para el supuesto cliente; pero he de decir que, en este caso particular, estamos más que satisfechos del trabajo que hemos realizado conjuntamente, y que nos ha permitido llevar a Mapfre a niveles que consideramos absolutamente vanguardistas en aspectos relativos a la gestión operativa de la Seguridad.



Ana Borredá, directora de RED SEGURIDAD, charla con Guillermo Llorente, director de Seguridad de Mapfre, en la visita que la revista realizó a las instalaciones de la compañía.

En este campo, nosotros tenemos un acuerdo a largo plazo con ellos, que define la forma de colaboración y aportación de cada uno a este proyecto conjunto, por el que nos comprometemos a darnos ese apoyo mutuo que garantice el beneficio común. Beneficio que se traduce, como fruto de ese acuerdo, en unos productos y desarrollos de muy alta calidad y tecnología, que Mapfre utiliza en sus instalaciones y que Sabia puede comercializar sin restricción alguna.

¿Con qué otros partners trabaja Mapfre en todas las áreas de seguridad?

La vocación de Mapfre como empresa global es la de trabajar con proveedores de máximo nivel y solvencia, líderes en su campo o actividad y con un ámbito de actuación internacional. Desde el punto de vista de Seguridad, nosotros buscamos siempre la mejor solución en cada materia (el *best of breed* que tanto citan algunos), para cada uno de los aspectos que entran en nuestro ámbito de competencia, frente a otras aproximaciones basadas en "soluciones para todo" de proveedores de amplio espectro.

¿A qué debe "tener miedo" una organización actualmente?

Si hablamos en general, yo citaría, como principal amenaza, a sí misma. Cuando la falta de visión, hace que el "cortoplacismo" se convierta en estrategia, se asumen riesgos inaceptables y las consecuencias, si no se manifiestan de inmediato, seguro que aparecerán en poco tiempo. Eso es aplicable a todos los ámbitos, no solamente al de la Seguridad, con resultados que desgraciadamente hemos venido

observando en los últimos tiempos en compañías de primer nivel.

Cuando una empresa se comporta con la debida prudencia, teniendo como *leitmotiv* el análisis y la gestión prudente de los riesgos, y haciendo los "deberes" día a día, aunque no este fijada (como pasa en Seguridad) la "fecha del examen", puede tener que enfrentarse a amenazas tremendamente complicadas, pero lo hará sin miedo, con la conciencia muy tranquila y con la seguridad de que, aunque siempre habrá tiempos difíciles, el "barco" capeará el temporal y llegará a buen puerto.

Creo que asumir esa política y esa forma de actuación, es el secreto del éxito Mapfre y el criterio a seguir también en el área de Seguridad.

Además de ese CCG del que antes hablábamos, ¿podría usted citarnos algún otro ejemplo o resultado de esa integración de las distintas seguridades tradicionales y las ventajas obtenidas?

Ejemplos hay muchos, pero uno con gran visibilidad e impacto en la organización, y con el que estamos muy ilusionados, es el de la implantación de una credencial única de identificación que integre y recoja las posibilidades o habilitaciones de acceso, tanto a las aplicaciones y sistemas, como a los edificios o zonas restringidas de los mismos.

Las ventajas de un sistema único y centralizado de acceso, creo son evidentes. En primer lugar, por lo que supone de simplificación y normalización de los distintos procesos y sistemas de acceso (en Mapfre hay más de 4.000 oficinas y edificios y más de 200 aplicaciones corporativas), con lo que conlleva de aumento de la eficiencia y reducción de costes. Pero por otro lado, no menos importante, porque la confrontación y cruce de la información obtenida permite la identificación y trazabilidad de todos los

accesos, y la detección de incidentes, que de otro modo pasarían inadvertidos (cuando por ejemplo, quien se "logea" en un equipo no es quien accedió a la ubicación o sala donde este se encuentra).

Tras finalizar esta etapa, ¿qué otras fases tienen previstas en la Dirección de Seguridad?

En primer lugar, estamos trabajando en tratar de alinear, más claramente si cabe, los objetivos de seguridad con los objetivos estratégicos de negocio de la compañía; el resultado de este alineamiento marcará las líneas de actuación para los próximos ejercicios.

Independientemente de lo anterior, seguiremos apostando por mejorar la gestión operativa, optimizando y automatizando procesos en la medida de lo posible.

Por otro lado, queremos continuar potenciando nuestro enfoque de "seguridad desde el principio", incorporando requisitos de seguridad en tiempo de diseño en todos nuestros ámbitos de actuación, ya sea en el desarrollo de nuevas aplicaciones o sistemas o en la construcción de nuevos edificios.

De manera adicional, pretendemos continuar homologando y "paquetizando" nuestras soluciones para trasladarlas al ámbito internacional, aprovechando acuerdos marco corporativos y el know-how obtenido en nuestra práctica nacional.

¿Qué les diría a los directivos de áreas de seguridad física, seguridad TIC, normativa, recursos humanos, etc., que prefieren aún llevar sus campos de manera independiente y como departamentos aislados?

Las organizaciones son tremendamente complejas y pensar que una receta vale para todos es trivializar la cuestión, por lo que creo que no soy quién para dar consejos en esta materia a nadie. Por eso, yo sólo puedo referirle lo que estimo son las bondades de nuestro enfoque, las razones que nos han llevado a asumirlo, y afrontar un debate conceptual al respecto, parte de lo cual, espero haber logrado a lo largo de esta entrevista.

En cualquier caso, si un compañero me pidiera consejo sobre cómo avanzar en un posible proceso de integración, posiblemente le contestaría diciendo que considero que disponer de un Comité Operativo de Seguridad en el que se sienten todas las áreas que antes has mencionado, pudiera ser algo no excesivamente difícil de lograr, del que pueden extraerse beneficios tangibles a corto plazo y que puede ser el primer paso para ir acercando posturas, mejorando el conocimiento mutuo y evitando recelos. ■