"Este año daremos un paso decisivo con el desarrollo del Plan Director de Seguridad Informática"

Pablo Monteagudo Ferrero, Seguridad Lógica Corporativa de Repsol-YPF

No todas las compañías disponen de la misma organización de seguridad TIC. En la presente entrevista, Pablo Monteagudo, miembro del Grupo de Seguridad Lógica Corporativa de Repsol-YPF, profundiza en el modelo vigente en su entidad, al tiempo que deja traslucir algunos de los proyectos que se están acometiendo y otros que se acometerán tras el desarrollo del Plan Director de Seguridad TIC de la multinacional española.

– ¿Cómo se articula en Repsol-YPF la administración y gestión de la seguridad informática?

– La responsabilidad específica recae en el Grupo de Seguridad Lógica, creado hace aproximadamente unos seis años e integrado actualmente por unos treinta profesionales especializados en las distintas áreas que conforman la protección técnica de la información y de los sistemas que la tratan, distribuidos en estructuras gemelas en las sedes de Buenos Aires y Madrid que atienden a Latinoamérica y Europa y resto del mundo, respectivamente.

– ¿De dónde depende el Grupo?

– Está integrado en el Departamento de Seguridad y Proyectos de Infraestructuras, que a su vez se encuadra en la Dirección de Soporte. Dicha Dirección pertenece a la Unidad de Servicios de Sistemas de Información.

– ¿Qué funciones específicas tiene encomendadas el Grupo?

– El Grupo de Seguridad Lógica tiene encomendadas las funciones de aplicación de la Política de Seguridad Informática definida por el Grupo Repsol-YPF, custodia las contraseñas de administración de todos los sistemas (centrales, distribuidos y de redes), ejecuta las operaciones de alta y baja de usuarios, opera las herramientas de administración de la seguridad, vigila la delegación de las funciones que se consideren, supervisa la seguridad de toda la red informática, estudia e implementa acciones de mejora de la seguridad, elabora informes sobre debilidades e intentos de violación, y define las normas y procedimientos de la seguridad informática.

– ¿Tienen alguna formación específica previa los profesionales que hoy conforman el Grupo de Seguridad Lógica?

– Su formación corresponde a la de técnicos de sistemas especializados en las distintas disciplinas de seguridad. Mediante una formación muy cuidada y la práctica diaria, han ido adquiriendo una notable experiencia en los distintos frentes de la protección de los sistemas de información y las comunicaciones.

– ¿Qué importancia dan en el contexto actual al epígrafe de formación?

– La formación, extraordinariamente importante en todo ámbito, sufre especialmente los efectos de las reducciones de presupuestos, cuando acontecen. Nosotros, en el Grupo de Seguridad Lógica, procuramos asistir a cursos y congresos de seguridad, y fomentamos el que compañeros de otras áreas de Sistemas de Información de Repsol-YPF también lo hagan. Obviamente, dedicamos la debida atención a la formación en la administración y gestión de herramientas tecnológicas de fabricantes, así como en estar al día de las novedades que se producen en este ámbito.

– Pregunta obligada: ¿están satisfechos con el presupuesto de que disponen para cumplir con sus cometidos?

– Por mucho dinero que se presupueste, si no se cuenta con recursos humanos suficientes resulta francamente difícil cubrir todas las facetas de seguridad TIC que requiere una multinacional del calado de Repsol-YPF; en consecuencia, y aparte de que sea más que recomendable incrementar el presupuesto, consideramos necesario aumentar la plantilla con unos diez técnicos más.

– ¿Cuáles son hoy sus prioridades en materia de seguridad técnica?

– Mantener y perfeccionar el nivel de seguridad especialmente en comunicaciones, por ser el área más

vulnerable hoy en cualquier organización. Las necesidades en este epígrafe están experimentando un crecimiento constante, tanto por la demanda interna como por las solicitudes de interconexión de terceros.

– ¿Qué proyectos están acometiendo actualmente?

– Tenemos varios frentes abiertos. Uno está asociado a la aplicación interna de firma electrónica, usando una PKI propia basada en certificados de Entrust y Microsoft. Igualmente, estamos trabajando con la FNMT-RCM para establecer una confianza que nos permita en el futuro abrirnos a contratistas y clientes. Por otra parte, hay una iniciativa relativa al *single sign on*, que cuando culmine afectará a cerca de 20.000 usuarios. Tambien cabe citar el uso de los cortafuegos personales, la interrelación entre el Directorio Activo y las aplicaciones, y la adecuación a los roles de usuarios.

– ¿En qué medida les preocupa la prevención y detección de ataques, y el conocimiento permanente de la fortaleza de sus sistemas?

– Esta es una preocupación constante de todo profesional de la seguridad que se precie. Dentro del Grupo de Seguridad Lógica tenemos un equipo específico dedicado a estos menesteres: análisis de incidencias, simulaciones, descubrimiento de agujeros de seguridad, seguimiento de informes sobre vulnerabilidades, actualizaciones... Aquí no puede haber relajación, ya que esta faceta de la protección de sistemas es muy dinámica.

Reconozco que mantener debidamente actualizados en materia de seguridad los cientos de servidores distribuidos de que disponemos, se está convirtiendo en una actividad crítica y muy laboriosa.

– ¿Se apoyan en herramientas técnicas de fabricantes para cubrir los frentes de seguridad TIC?

– Sí, por supuesto. En líneas generales, los fabricantes están desarrollando productos aceptables que nos sirven como base para diseñar nuestra estrategia de protección. Además, en Repsol YPF no queremos desarrollar herramientas técnicas internamente. No es nuestro negocio, y preferimos adaptarnos a los estándares existentes para evitar problemas de compatibilidad con terceros.

No obstante, quisiera añadir que un requisito indispensable para Repsol YPF es que las distintas herramientas técnicas de protección: antivirus, IDS, cortafuegos..., puedan gestionarse y administrarse de forma centralizada. Aquí los fabricantes han empezado a proporcionar soluciones hace relativamente poco tiempo.

– ¿Tiene el Grupo de Seguridad Lógica facultades de prescripción tecnológica a la hora de adquirir herramientas técnicas?

– Siempre emitimos nuestra opinión, y normalmente la sacamos adelante, pero en estrecha colaboración con el área solicitante.

– ¿Tienen solucionado el problema del control del uso que los usuarios dan a los recursos informáticos y telemáticos que Repsol YPF pone a su disposición para trabajar?

– Existe una normativa específica vigente desde hace cinco años. No se expresan prohibiciones taxativas, sino que se ha optado por hacer un llamamiento, mediante recomendaciones, al uso responsable de los medios y recursos. No obstante lo dicho, y debido a la rapidez con la que cambia el escenario tecnológico en los ámbitos de trabajo, vamos a abrir un proceso de puesta al día de la normativa antedicha, y no se descarta el uso de herramientas técnicas para poder implantar controles razonables y eficaces.

– ¿Han tenido incidentes de seguridad destacables?

– Hemos registrado algún incidente puntual y muy localizado por virus informático, que no tuvo mayores consecuencias, como puede ser el caso de SQL Slammer o el Bug Bear.

– ¿Tiene Repsol-YPF una política de seguridad TIC debidamente formalizada?

– Desde primeros de este año disponemos de una política aprobada al más alto nivel. Hasta esa fecha, dicha política existía y se cumplía, pero no estaba aprobada oficialmente, lo cual nos generaba algún que otro problema con los auditores, ya que nos exigían la pertinente formalización.

"Mantener debidamente actualizados en materia de seguridad los cientos de servidores distribuidos de que disponemos, se está convirtiendo en una actividad crítica y extremadamente laboriosa"

Este paso ha sido decisivo para nosotros. Ahora vamos a dar otro: el desarrollo de un Plan Director de Seguridad, en el que se contempla la creación de un Cuadro de Mando de Seguridad TIC en el que ya estamos trabajando en colaboración con colegas de otras compañías. También en el Plan se van a contemplar otras iniciativas, entre las que se encuentra un proyecto de concienciación de usuarios finales y otros asuntos por determinar o retomar, entre los que quizás podríamos mencionar el de la gestión de usuarios. Al respecto de este asunto, tenemos implantada la entrada única para los usuarios que acceden a nuestros distintos sistemas SAP, basada en *ticket* de Kerberos.

– ¿Les está resultando complicada la definición de indicadores para el cuadro de mando?

– En absoluto. Los indicadores básicos ya están definidos, así como las variables que los conforman. Tenemos el compromiso de presentar el resultado de la recopilación de los datos necesarios. Es más que posible que surjan nuevos indicadores y variables como consecuencia del ajuste del cuadro a las Políticas y Normas de Seguridad vigentes en la compañía.

– ¿En qué medida les ha ayudado a ir cumpliendo objetivos de seguridad la legislación sobre protección de datos de carácter personal?

– La existencia de una ley orgánica y de un reglamento de medidas de seguridad, que son piezas de obligado cumplimiento, han conseguido –como no podía ser de otra manera– vencer posibles resistencias internas. Hemos estado trabajando los ultimos años para adaptarnos a la legislación, y los propios clientes internos son ahora los primeros que procuran informarse acerca de los requisitos que pudiera imponer la LOPD sobre sus iniciativas. No obstante lo dicho, disponemos de controles, que se ejecutan al inicio de cualquier proyecto y antes de su paso a producción, cuya finalidad es determinar si ese archivo, fichero, base de datos, servicio o aplicación está afectado por la ley y el reglamento, y si lo está, en qué niveles. Al inicio del proyecto se establecen los requisitos de protección de datos personales que hay que cumplir, pero como normalmente los proyectos se alargan en el tiempo y sufren cambios en su desarrollo, antes de su paso a producción, verificamos mediante un test si cumple los requisitos establecidos al principio o si, por las razones que fuere, éstos han cambiado y requieren una readaptación a la normativa vigente.

– ¿Interviene Seguridad Lógica en el desarrollo de servicios y aplicaciones?

– Antaño había una relación informal entre el desarrollador y Seguridad Lógica, pero hoy existen ya una normativa y unos procedimientos que nos permiten fijar, desde que una iniciativa empieza hasta que termina, distintos hitos en los que es menester nuestra intervención.

– ¿Y qué opinan de esta intervención los colegas internos de sistemas de información?

– Al principio pensaban que eramos una especie de china en el zapato, pero con el paso del tiempo las cosas han ido cambiando, y ahora demandan activamente nuestra colaboración, entre otras razones porque también van siendo sufridores de los rigores de la demanda de seguridad de la información por parte de los clientes internos.

– En su opinión, ¿de dónde debería depender la función de seguridad de la información en una organización?

– El núcleo decisor del que emanan las directrices no debería depender directamente del departamento de Sistemas de Información. Ahora bien, es una realidad que la función de seguridad técnica debe ejercerse permanentemente sobre cada uno de los sistemas existentes.

– Una última pregunta: ¿tiene futuro en las empresas esto de la seguridad TIC?

– Sí, por supuesto. Estará sometida, como todo, a ciclos, y llegará un momento en el que se convertirá en algo cotidiano y dejará de estar tan en primer plano como en la actualidad, y lo más importante es que está siendo cada vez más necesaria y, en el futuro inmediato, se constituirá en una pieza natural de todo sistema implantado. ■

Texto: **José de la Peña Muñoz**
Fotografía: **Jesús A. de Lucas**