«La seguridad encuentra su razón de ser en que hay que hacer las cosas bien y en que los servicios deben ser de calidad»

Bernardino Cortijo, vicepresidente de seguridad de Terra Lycos

Terra Lycos es uno de los macroportales y proveedores de acceso y servicios en la Red más importantes del mundo. Y también es una compañía que por razones de su naturaleza y volumen de operaciones electrónicas de clientes y usuarios, necesita dotarse de una seguridad TIC ciertamente sólida en su política y a la vanguardia tecnológica. SIC ha mantenido una entrevista con su vicepresidente de seguridad, Bernardino Cortijo, un extraordinario profesional cuyo reto consiste en conseguir que los clientes y usuarios del Grupo, puedan realizar sus actividades de información, de trabajo o de ocio, sintiéndose seguros.

– ¿Qué se entiende en Terra Lycos por seguridad de la información?

– Terra es una empresa en la que precisamente la información es uno de sus más grandes activos, por no decir el mayor. La protección de esa información resulta vital para la propia organización. Eso sí, le preciso que cuando menciono el término seguridad, no sólo me refiero a la seguridad en la faceta de protección de datos, sino también a la de la infraestructura TIC, a la gestión de los riesgos y a la continuidad de servicios.

– ¿De dónde depende jerárquicamente en Terra Lycos la función de seguridad de la información?

– Depende directamente del presidente de la compañía a efectos corporativos. Luego, en cada país en el que estamos implantados, y en cada línea de negocio, hay profesionales especializados en las distintas ramas de la seguridad TIC, siempre coordinados por el área corporativa.

– ¿Cómo está organizada la función de seguridad?

– En primer lugar, tenemos a los equipos que están coordinando y gestionando la seguridad del Grupo en el área corporativa, que es desde donde se emiten las políticas de seguridad, las normativas, y donde se elaboran los procedimientos y se lleva a efecto un control del cumplimiento de lo establecido; en segundo, existe el personal especializado adscrito a cada país en el que operamos en forma de unidad de negocio: Terra España, Terra Méjico, Terra Brasil, Terra Argentina, Lycos... En estas unidades de negocio de países, sí se diferencia lo que es la seguridad informática propiamente de otro tipo de seguridades que también dependen del área corporativa y que, en efecto, deben enmarcarse en el más amplio contexto de seguridad de la información.

Básicamente esta es la estructura; no obstante, hay una peculiaridad en Terra Lycos: que trabajamos en base a proyectos activos, que tienen una estructura horizontal. Le explico: en cada proyecto de seguridad que tenemos en curso –también en aquellos de negocio que la prudencia y el oficio nos indican que tienen una fuerte vinculación con la seguridad–, hay un responsable y un equipo de colaboradores de distinto nivel; pero, además, también participan expertos de otras áreas de la organización, que durante el tiempo de duración del proyecto, están adscritos al área de seguridad. Lo mismo ocurre en otros terrenos. Creo que es una manera muy eficaz de optimizar los medios y de fomentar el que nuestros equipos humanos den lo mejor de sí mismos.

– ¿Está satisfecho con la inversión que hace el Grupo en seguridad de la información?

– Sí, en la fase actual de trabajos, muy centrada en el asentamiento sólido de políticas de seguridad y en la apertura de proyectos muy específicos para controlar la protección de los datos, proteger las aplicaciones, dar valores añadidos a ciertas líneas de negocio... Tampoco somos más ambiciosos de lo que la dimensión de nuestra función justifica. Hoy, tenemos abiertos varios proyectos importantes, y todos están teniendo el apoyo de la compañía.

– De los proyectos a los que alude, ¿cuál le parece más significativo?

– Hay uno, de ámbito global, que consiste en conseguir optimizar la seguridad para el cliente. Con este proyecto, que tiene varias partes, se pretende que cuando el cliente entre –sea un usuario gratuito o de cualquier tipo de nivel de pago y de cualquier servicio– se sienta potencialmente seguro. Esto, dicho así parece estupendo, pero en realidad es algo muy complejo. Lo tenemos parametrizado, es decir, valorado según las técnicas estándar para saber hasta dónde podemos llegar en velocidad de la línea,

problemas que pueden causarse, continuidad de servicios, problemáticas de seguridad en el envío y recepción de correo-e (intrusiones en la intimidad, ataques con código malicoso...). También estamos intentando, en este contexto técnico, articular medidas que nos permitan facilitar los contenidos adecuados para los menores.

– ¿Tienen ustedes a *hackers* o fisgones trabajando en casa?

– No me gusta el término *hacker*, me suena a delincuente. En Terra Lycos disponemos de profesionales de la seguridad TIC que entienden muy bien las distintas áreas de especialización en su trabajo de tipo técnico, ya en el chequeo del estado de nuestras redes ya en otras facetas de investigación.

– ¿Le resulta complicado extender la política corporativa de seguridad al resto de entidades del Grupo en los países donde operan?

– Nunca es fácil. De momento no estamos teniendo mucho problema, a lo que nos ayuda el que las cosas se estén planteando en función de un beneficio para el usuario y el cliente. Algunas acciones obligadas de seguridad parece que no dan un beneficio inmediato, aunque con las cosas que están pasando hoy en día creo que dicho beneficio está a la vista.

– Hay quien cuenta que ustedes detectan cerca de medio millones de intentos de ataque al mes. ¿Le parece descabellado el cálculo?

– Yo no los he contado, desde luego. Obviamente, en los grandes portales, y también en las grandes empresas y administraciones con mucho volumen de transacciones en el contexto de la Red, pues se registran intentos de ataque. Pero conviene aquí precisar que muchos de estos intentos son de carácter sistemático y/o estadístico y no revisten mucha gravedad. Otros se realizan a conciencia y con mal sentido. Esta es una realidad, y para controlar el que este tipo de incidentes no se conviertan en causa grave de trastorno para la empresa estamos los profesionales de la seguridad.

– ¿Hasta qué punto confía en las herramientas tecnológicas de seguridad?

– La casa la hemos empezado por los cimientos: elaboración de política, normas y procedimientos basándonos en estándares: ISO 17799, método de análisis y gestión de riesgos Magerit, RFCs... Contamos, además, con la ventaja de nuestra fortísima relación con el Grupo Telefónica, que dispone de una dirección general de seguridad corporativa que, precisamente, desarrolla las normas globales y coordina las acciones que al respecto toman las empresas del Grupo. Después, y por sus peculiaridades, cada una adapta la normativa a su casuística.

Tras crear esa base de normativas adecuadas, hemos generado procedimientos para identificar productos. En última instancia, lo que pretendemos es que, se utilice el cortafuegos que se utilice, o el IDS, o la solución antivirus, o el sistema de alta disponibilidad y balanceo de carga tal o cual, como mínimo cumpla las especificaciones de seguridad que damos en la normativa y se adapte a los requisitos técnicos de nuestra infraestructura tecnológica.

En estos momentos estamos evaluando varios productos cortafuegos e IDS, entre otros. Y debido a nuestras peculiaridades, tamaño y política, no parece que vayamos a optar, en cada caso, por la herramienta de un solo fabricante, además de que no todo sirve para todo. Puede pasar que a los seis meses o al año, una herramienta implantada para cubrir una necesidad, ya no sea la mejor del mercado.

– ¿Y dónde quedan las personas?

– Con unos buenos profesionales, unos buenos procedimientos de trabajo y una buena normativa hemos resuelto, sin entrar en el capítulo de adquisición de herramientas tecnológicas de fabricante, un porcentaje elevadísimo de problemas de seguridad. Ahora bien, hay áreas que no pueden protegerse con procedimientos, y es completamente necesario hacerlo con herramientas.

Una apreciación: a las herramientas tecnológicas hay que sacarles el máximo partido, y para ello es necesario disponer de profesionales expertos en su configuración, administración y mantenimiento.

«La protección frente a instrusiones es importante en Terra Lycos, pero aún lo es más la disponibilidad de los servicios»

– ¿Qué opina acerca del Reglamento de medidas de seguridad y, en general, de la legislación sobre datos personales?

– Parto de la base de que haya Ley o no haya Ley, y de que haya Reglamento o no, la protección de los datos personales de los clientes y usuarios en algo importante en una empresa u organización, y más generalmente en la sociedad. Para cumplir con la legislación sobre protección de datos personales hay que hacer un importante esfuerzo, y yo lo tengo asumido. Sin embargo, quizá falte un punto más de celo en la aplicación de las leyes a aquellos terceros que probadamente acceden de forma no autorizada a esos datos personales.

– ¿Cuál le parece su reto profesional más importante, relativo a la seguridad, en Terra Lycos?

– Conseguir que los clientes y usuarios puedan realizar sus actividades de información, de trabajo, de ocio, sintiéndose seguros. ¿Cómo? Pues fortaleciendo las aplicaciones, controlando los accesos, la seguridad en las comunicaciones...

– ¿Es posible, sirviéndose de la seguridad, ofrecer valor añadido a las líneas de negocio?

– Hay pocas cosas de las que no se pueda hacer negocio. La seguridad surge como consecuencia de unas necesidades que hay que cubrir de modo obligatorio y por pura profesionalidad. Ahora bien, si por ejemplo a un señor, o a una familia, se le ofrecen diferentes niveles de equipamiento y de seguridad o de protección en función de lo que vayan a hacer, o a una empresa en función de las distintas necesidades de sus departamentos, pues la visión empieza a ser de negocio. Hay varias fórmulas. Terra está contemplando todo lo que pueda ser útil o necesario. Además, algunos de estos servicios hay que ofrecerlos en coordinación con empresas especializadas en seguridad: no vamos a inventar aquí un antivirus o un sistema de detección de intrusiones.

– ¿Va a crecer la inversión en seguridad TIC en todos los órdenes?

– Llevamos más de dos años creciendo a buen ritmo, y todo indica que vamos a seguir en esa línea. Creo que todavía tiene el ramo de seguridad un margen de crecimiento muy importante, aunque todo tiene un límite.

– ¿Ofrece actualmente la tecnología soluciones asumibles para las necesidades detectadas de seguridad en Terra Lycos?

– Queda mucho por hacer. La versión actualmente operativa de IP está un poco quemada. Debería haber cuanto antes un cambio. Por otra parte, el número de usuarios de servicios de web y de correo-e crece y crece, y en ocasiones, algunos sistemas cortafuegos son ineficaces frente al número tan elevado de llamadas que se realizan. Hay que trabajar mucho en todos los frentes, por ejemplo en los balanceadores de carga, a efectos de conjugar de forma óptima herramientas tecnológicas con distintos propósitos.

También es cierto que las empresas desarrolladoras de productos de seguridad -europeas y españolas, también- están trabajando mucho y muy bien, que todo hay que decirlo.

– ¿Dónde deja a los *hackers*? ¿Le parece que son personas que están ahí para divertirse? ¿Existen intrusos realmente peligrosos, los de verdad, aquellos que no son conocidos?

– No concibo, dentro de la ley, el entrar en un sistema ajeno. Cada persona, física o jurídica, tiene sus propiedades, sean electrónicas o no, y hay que respetarlas. En este mundo hay dos tipologías básicas: los curiosillos, generalmente universitarios, que no hacen mucho daño, y aquellos que van en serio a hacer daño a una persona, empresa o administración... Creo que las herramientas tecnológicas deben protegernos de sus ataques, e identificarlos.

– ¿Qué opinión le merece el proyecto de nuevo DNI?

– Estoy muy interesado. Creo que es necesario, porque debe haber un documento que nos garantice quiénes somos a través de los medios electrónicos. Debemos apoyar el proyecto de DNI Electrónico.

– Una última pregunta: ¿justifica la seguridad TIC en base al riesgo que suponen este tipo de amenazas en el contexto de la Red?

– La seguridad TIC, en el contexto de la seguridad de la información, encuentra su razón de ser en dos pilares: que hay que hacer las cosas bien, y que los servicios deben ser de calidad. El capítulo de la protección frente a instrusiones es importante en Terra Lycos, pero aún lo es más el de la disponibilidad de los servicios. n

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