# «Los servicios de seguridad de la información son absolutamente necesarios en cualquier organización gestionada de forma responsable»

## Ramón Montes, coordinador de Seguridad Informática de Endesa

En la presente entrevista, Ramón Montes, coordinador de seguridad informática de Endesa, explica la concepción que en esta entidad se tiene de la seguridad de la información y de la seguridad informática, y el modelo de organización que las soporta. Igualmente comenta algunos de los proyectos de protección tecnológica que se están llevando a efecto o que se tiene previsto abordar, y que se incluyen en el Plan Director de Seguridad Informática diseñado por esta compañía para el trienio 2002-2004.

**– ¿Cómo se organiza la seguridad de la información en Endesa?**

– En 1998 se constituyó en Endesa un Comité de Seguridad de la Información, que es el órgano del que emanan las normas corporativas de seguridad de la información. En el año 2000, dicho Comité decidió crear una unidad específicamente dedicada a la coordinación en materia de seguridad informática. Hasta ese momento, la función no estaba definida y los trabajos específicos se acometían proyecto a proyecto. La unidad de Coordinación de Seguridad Informática cumple con su cometido de una manera estable desde mediados del año 2001, y aunque encuadrada en la dirección de Sistemas de Información y Telecomunicaciones, está coordinada funcionalmente desde Seguridad de la Información.

**– ¿Cada cuánto tiempo se reúne el Comité de Seguridad de la Información?**

– Se convoca una reunión cada 2 ó 3 meses, salvo que exista un motivo que justifique una reunión digamos extraordinaria. La verdad es que la existencia de una organización de seguridad de la información en cualquier empresa es fundamental, ya que sin ella, la seguridad informática debería estar siempre luchando para hacer un despliegue de todas las medidas que realmente se necesitan. Nosotros, en la unidad de Coordinación de Seguridad Informática, somos expertos en identificar esas medidas, pero en virtud de lo que nos demanden los propietarios de la información. La seguridad, créame, no puede empezar y terminar en el área de sistemas de información.

**– No obstante, es innegable el creciente papel de la tecnología en la seguridad de la información…**

– El protagonismo de los sistemas tecnológicos en el tratamiento de la información crece día a día. Si queremos proteger la información, uno de los objetivos clave es crear entornos tecnológicos razonablemente seguros. Obviamente, la tecnología es necesaria para llevar a cabo prácticamente cualquier proyecto de seguridad informática; pero no es suficiente. No se trata de disponer de herramientas tecnológicas, sino de implantarlas e integrarlas en la justa medida en que ayuden a solucionar los problemas de seguridad inherentes a los sistemas de negocio.

**– ¿Cuál es el grado de profundidad al que llega la unidad de Coordinación de Seguridad Informática en el cumplimiento de las funciones que tiene asignadas?**

– Nuestra misión es aportar soluciones de seguridad a los sistemas de negocio de Endesa mediante la creación de políticas y normas, la elaboración de procedimientos y la aportación de servicios de seguridad informática acordes con la política de seguridad de la información existente. Nosotros coordinamos, pero no asumimos funciones de gestión y operación.

**– ¿Cómo percibe la alta dirección el trabajo que ustedes realizan? ¿Entiende la diferencia entre la seguridad de la información y la**

**seguridad informática?**

– Como he dejado apuntado, disponemos de una organización enfocada a mantener y acrecentar una cultura de seguridad en la entidad. Prácticamente toda nuestra alta dirección tiene representación en el Comité de Seguridad de la Información, desde el que trasciende que la seguridad es responsabilidad de todos. Quizás lo más difícil de hallar sea el punto óptimo de equilibrio entre las medidas de protección y la comodidad y funcionalidad en el trabajo.

**– Probablemente la legislación sobre protección de datos personales haya ayudado a concienciar todavía más a la alta dirección en materia específica de seguridad informática…**

– Sí, qué duda cabe. La existencia de la legislación sobre tratamiento de datos de carácter personal ha sido un factor determinante en la toma de conciencia por la alta dirección de las necesidades de proteger la información. Si nos referimos concretamente a la seguridad informática, pues parece claro que la existencia del Reglamento de medidas de seguridad no deja lugar a dudas sobre lo que hay que hacer a efectos técnicos y de organización para respetar los derechos de los ciudadanos. En los últimos años hemos venido trabajando muy seriamente para adaptarnos a lo que en esta pieza legal se indica. Pero claro, no todos los datos son personales. Hay activos de información estratégicos de negocio que para Endesa tienen la misma importancia a los efectos de seguridad de la información y de seguridad informática, que la que el legislador dio en la LOPD a los datos de carácter personal.

**– ¿Qué les preocupa más en Endesa, la confidencialidad, la integridad o la disponibilidad de los datos de negocio?**

– Disponemos de una serie de procedimientos de seguridad de la información que informan sobre cómo identificar y clasificar nuestros activos de información en base a los paradigmas de la seguridad, tanto uno por uno como en conjunto. En función de los tipos y procesos de negocio, el peso de cada uno varía. Por ejemplo, en una actividad basada en transacciones en tiempo real quizás prepondere la disponibilidad, sin obviar la integridad y la confidencialidad de la información.

**– ¿Tienen plan director de seguridad?**

– La unidad de Coordinación Informática, como he comentado, empezó a operar en 2001, y uno de las primeros proyectos que llevamos a efecto fue el diseño de un plan director de seguridad informática a tres años, 2002-2004. Dicho plan, aunque partió de seguridad informática, alcanza objetivos más amplios de seguridad de la información.

En 2001 arrancamos un proyecto, llamado Confía, que engloba todas las iniciativas de seguridad de la información. El plan director de seguridad informática antes aludido forma parte de Confía. El año pasado, tras una reorganización interna en nuestra Dirección, definimos un Plan Director de Sistemas de Información y Telecomunicaciones. Dentro de este Plan se encuentra un nuevo Plan Director de Seguridad Informática, basado en el diseñado para el trienio 2002-2004, aunque adaptado a la estructura actual.

**– ¿Cuáles son los fundamentos de la estrategia global en seguridad informática de Endesa?**

– Tres: el cumplimiento de las directrices que emanan de nuestro Comité de Seguridad de la Información, el cumplimiento de la legislación vigente y el cumplimiento de normas internacionales.

***"Ni creo que los sistemas lleguen a ser tan seguros que sea innecesaria la existencia de profesionales especializados en su gestión, ni me parece razonable que se pueda pensar que la seguridad no es importante para un sistema"***

Hemos planificado para el próximo año iniciar los pasos para implantar la ISO 17799, ya que permite sistematizar la seguridad informática de un modo muy completo.

**– ¿Le parece adecuado el presupuesto que destina Endesa a proteger la información que se trata en sus sistemas de información tecnológicos?**

– Endesa está realizando un importante esfuerzo para dotar a Seguridad de la Información de un presupuesto adecuado. En cualquier caso, siempre tenemos muy en cuenta el valor de los activos a proteger y los costes de protección.

**– ¿Qué proyectos de seguridad están desarrollando actualmente?**

– Hay varios. Uno de ellos de especial significancia, ya que su finalidad es solucionar la problemática que plantea la gestión de usuarios y perfiles y el acceso a la información. Este proyecto lo iniciamos en junio de 2002, basándonos en tecnología de BMC Software y de Netegrity y con la participación de SIA, como integrador. Le concedemos mucha importancia, ya que nos va a permitir implantar unas políticas muy afinadas para proteger el acceso a la información y facilitar al usuario final el proceso de identificación y autenticación en los sistemas de información. Primero vamos a sincronizar las contraseñas y después vamos a poder dar entrada única.

**– ¿A cuántos usuarios, sistemas y aplicaciones afecta?**

– Una de las primeras preguntas que nos tuvimos que contestar antes de empezar con la iniciativa fue la alusiva a cómo íbamos a encarar su despliegue. El proyecto afecta a los empleados de Endesa y al personal subcontratado y en externalización. Hablamos de 15.000 usuarios en total. El proyecto tiene dos fases, en lo referente al despliegue de sistemas que vamos a incorporar al mismo. En la primera, vamos a incluir unas doce aplicaciones web y de cliente-servidor las seis o siete más importantes por afectar a un mayor número de usuarios: Windows 2000, correo electrónico, partes de trabajo... También incluiremos otras aplicaciones más específicas, como la que soporta nuestro sistema comercial-facturación, al que acceden unos 5.000 usuarios, el sistema económico-financiero, al que acceden una cantidad similar de personas; en una segunda fase, que se va a solapar en su inicio con la finalización de la primera, vamos a incluir la totalidad de sistemas y aplicaciones de Endesa.

Tenemos otro proyecto, que iniciamos en octubre de 2002 y al que llamamos Entorno Corporativo Seguro, destinado globalmente a la mejora continua de nuestra seguridad perimetral, incluyendo la renovación del parque de sistemas cortafuegos, la detección de ataques (IDS), el análisis y corrección de vulnerabilidades y el fortalecimiento del sistema antivirus.

En realidad se trata de varios subproyectos en los que utilizamos tecnologías de ISS, de Check Point, de Network Associates y la colaboración de integradores como Realsec y Davinci. Para Endesa resulta vital tanto detectar ataques, internos o externos, como asegurarse técnicamente de que no es débil ante dichos ataques.

**– ¿Qué tipo de atacante externo es el que realmente les preocupa?**

– Aunque la liberalización del mercado eléctrico pueda propiciar fenómenos de sustracción de información, en realidad no discriminamos en ese sentido: cualquier atacante es peligroso, ya sea su fin el divertimento, la notoriedad, el espionaje industrial o cualquier otro motivo.

**– ¿Podría mencionar otros proyectos?**

– Tenemos uno dedicado a la seguridad en el ciclo de vida de los sistemas; se trata de, tras estudiar los procesos y los activos de información involucrados en los mismos, identificar en cada uno de esos procesos las medidas de seguridad y estándares que deben de adoptarse para alcanzar los niveles de seguridad necesarios. Para empezar lo estamos haciendo de la mano de los nuevos proyectos de negocio, pero con la idea de desarrollar la iniciativa a efectos globales en un futuro cercano.

Asimismo, tenemos previsto reforzar nuestra estrategia en Planes de Continuidad de los Sistemas de Negocio.

**– ¿Cómo se valora en Endesa el problema de seguridad que acarrea el ataque mediante virus informáticos y otros códigos maliciosos, en muchas ocasiones indiscriminados?**

– La defensa frente a virus informáticos se abordó en Endesa hace ya muchos años. Es un asunto en el que no conviene relajarse y que, además, requiere ajustar permanentemente las políticas de prevención y corrección. Disponemos de un antivirus corporativo potente y con unas políticas de actualización muy estrictas de despliegue inmediato, lo que hasta el momento nos ha dado resultado. Sin embargo, y como antes he apuntado, vamos a fortalecer aún más el sistema, analizando otras alternativas distintas al modelo tradicional correctivo.

**– ¿Cree que la industria desarrolladora de herramientas de seguridad está a la altura de la demanda corporativa?**

– Creo que los fabricantes están haciendo buenos trabajos en general, suministrando tecnologías sobre las que pueden implementarse buenas soluciones de seguridad.

**– ¿Y qué opina de los integradores?**

– Como este es un buen momento para la seguridad técnica, lo cierto es que proliferan como setas. Hay demasiados, y todos dicen tener muchísima experiencia en el despliegue de proyectos. La verdad, creo que ese mercado va a tener que redimensionarse y al final permanecerán sólo los más competitivos, que los hay.

**– ¿Cree usted que esto de la seguridad informática tiene futuro profesional?**

– Los servicios de seguridad de la información son absolutamente necesarios en cualquier organización gestionada de forma responsable. La seguridad informática es una función inherente al propio funcionamiento de los sistemas, que cada vez son más abiertos y demandan una mayor protección. Ni creo que los sistemas lleguen a ser tan seguros que sea innecesaria la existencia de profesionales especializados en su gestión, ni me parece razonable que se pueda pensar que la seguridad no es importante para un sistema.

**– ¿Qué opina de la firma electrónica?**

– Hace años que apostamos por el uso de esa tecnología para nuestra iniciativa *e-business*, que nació con la finalidad de proporcionar soluciones de negocio entre terceros. Este escenario requería el uso de mecanismos de seguridad basados en criptografía de clave pública y PKI, por lo que en el año 2000 iniciamos un proyecto piloto de la mano de SIA, y tras algunos meses conseguimos disponer de una infraestructura estable, materializada en una CA (autoridad de certificación) con la marca registrada e-certeza.

***"Hay activos de información estratégicos de negocio que para Endesa tienen la misma importancia a los efectos de seguridad de la información y de seguridad informática, que la que el legislador dio en la LOPD a los datos de carácter personal"***

Esta infraestructura tiene, potencialmente, la capacidad para compartir soluciones de certificación digital entre las comercializadoras y distribuidoras del sector energético.

Para agentes internos, en la actualidad estamos inmersos en el desarrollo de una serie de servicios basados en tecnología PKI. Al respecto estamos iniciando un piloto para usuarios específicos, como nuestra alta dirección y otros colectivos sensibles, a quienes vamos a proporcionar servicios de autenticación, integridad y confidencialidad en correo electrónico, escritorio, etc.

Por otra parte hay aplicaciones web en el área comercial, como por ejemplo la de gestor de relaciones entre agentes comerciales y distribuidoras que, con motivo del nuevo mercado liberalizado de la energía, necesitan la aplicación de mecanismos criptográficos para disponer de los servicios de seguridad indispensables.

**– ¿Disponen de cuadro de mando de seguridad informática?**

– Tenemos una visión de la gestión de la seguridad muy cercana a lo que es la gestión de un sistema cualquiera. Digamos que el de seguridad es un sistema más. Así pues, de la misma forma que no vemos la gestión de un sistema sin cuadros de mando, tampoco lo vemos en seguridad, por lo que en cada uno de los proyectos que estamos desarrollando siempre hay una parte dedicada a este epígrafe, al igual que siempre hay otra dedicada a la auditoría y al control.

Al final de lo que se trata es de controlar globalmente todo el sistema de seguridad informática. Para Endesa, y a tal fin, es muy importante la integración del cuadro de mando con la auditoría y el control. En este sentido, uno de los proyectos incluidos en el Plan Director de Sistemas de Información y Telecomunicaciones es lo que nosotros hemos denominado Plan Integral de Gestión de la Seguridad, que incluye esos cuadros de mando y toda la supervisión del sistema como tal.

**– ¿Se encuentra con muchas barreras en su labor de coordinación de Seguridad Informática?**

– Ha ayudado mucho el que Endesa disponga de una organización de seguridad de la información que desarrolla toda una serie de roles que considero indispensables para mitigar muchos problemas que pudieran presentarse en el desarrollo de nuestra función.

En el terreno técnico, lo que intentamos es tener un modelo de relaciones que permita el que dentro de la propia organización de la dirección de Sistemas de Información y Telecomunicaciones todos participemos de los mismos objetivos.

**– ¿Podrían desarrollarse aplicaciones sin contemplar las medidas de seguridad informática adecuadas?**

– No en nuestra organización; este particular está ya contemplado en la propia metodología de desarrollo de sistemas. El actual modelo de relación al que antes aludía propicia que los proyectos entren por donde corresponde, es decir por consultoría interna, que está directamente en contacto con el cliente interno. De ahí emana la organización del proyecto, la cual tiene en cuenta a todas las partes que han de participar, incluida la de seguridad informática.

Aclaro que Seguridad Informática está organizada internamente como un servicio horizontal para el resto de nuestra Dirección en cada uno de sus proyectos.

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