«No hay seguridad sin calidad, y ambas debemos de medirlas de forma permanente»

Francisco Javier García Carmona, director de Seguridad de la Información y Comunicaciones de Iberdrola

Lograr la creación de un entorno que permita disparar el proceso de mejora continua de la calidad de la seguridad de la información y las comunicaciones en una empresa no es algo que pueda conseguirse exclusivamente con la implantación de herramientas tecnológicas. Se necesita planificación, organización, disciplina, formación y colaboración interdepartamental. Esta es una de las conclusiones que pueden sacarse de la presente entrevista, realizada a Francisco Javier García Carmona, director de Seguridad de la Información y Comunicaciones de Iberdrola.

– ¿Qué se entiende en Iberdrola por seguridad de la información en su relación con las tecnologías y sistemas de la información y comunicaciones?

– En el Grupo Iberdrola se está instaurando actualmente una nueva cultura empresarial en la que ocupa un lugar relevante la protección de la información y de las comunicaciones, entendida como algo que va más allá de lo que hasta ahora se venía entendiendo como la protección de los sistemas de información tecnológicos o seguridad informática.

En Iberdrola hablamos de proteger la información independientemente del modo en que ésta se pueda manifestar: de lo que hablemos, de lo que escribamos, de lo que comuniquemos..., y del medio en que se pueda soportar: papel, telemático...

– ¿Qué se valora más en Iberdrola, la disponibilidad, la integridad o la confidencialidad?

– No podemos priorizar en este sentido. Nosotros tenemos dos tipos de clientes, internos y externos. La disponibilidad, en relación con los segundos, tiene un gran peso específico. En lo referente a la integridad, qué le voy a decir cuando tratamos datos, no ya sólo de carácter personal, que están regulados por una Ley cuyo cumplimiento tiene mucha importancia en nuestra organización, sino datos de características de suministros, bancarios, domiciliarios, datos de personas jurídicas... La integridad de esta información resulta esencial.

En lo que concierne a la confidencialidad, creo que hoy, la liberalización del mercado va a hacer que en las compañías tengamos que velar mucho más por nuestros activos de información, en el sentido de que va a entrar en escena una agresividad comercial que antes no existía, y que puede dar lugar a la aparición de un riesgo potencial de salida de información de las organizaciones.

– En materia de datos de carácter personal, ¿cuáles son las especiales casuísticas de Iberdrola?

– Las grandes compañías compartimos en este sentido la misma problemática, y estamos concernidas por el mismo tipo de incidencias. Hablamos de datos que pueden definir una serie de perfiles del usuario, lo que la Ley de Protección de Datos y el Reglamento de medidas recogen con acierto.

La protección de los datos personales en Iberdrola se entiende como un valor añadido en el contexto del servicio a los clientes, además de los aspectos de eficacia y eficiencia.

La responsabilidad de tipo legal en lo que se refiere al tratamiento de datos, especialmente el de los datos personales, trasciende el perímetro del Departamento de Seguridad Corporativa, encontrándose al más alto nivel de la organización. En función de este modelo de responsabilidades estamos ejecutando el proyecto de adaptación a las medidas de nivel alto del Reglamento. Esto le da una idea de la importancia que

tiene para nosotros.

– ¿Qué modelo de dependencia jerárquica de la función de seguridad de la información se ha implantado en Iberdrola?

– Nuestra Unidad de Seguridad de la Información y Comunicaciones es una de las que conforman el Departamento de Seguridad Corporativa, junto a las de Seguridad Patrimonial, Procedimientos y Calidad (y Planes de Emergencia y Evacuación), e Internacional. El departamento de Seguridad Corporativa está encuadrado en la Dirección General de Medios.

– Comentaba antes que el concepto de seguridad de la información en Iberdrola es más amplio que el que se circunscribe específicamente a la seguridad en sistemas tecnológicos. ¿Cómo aplican tan amplio concepto en la organización?

– Desde la matriz, es decir, desde Iberdrola, S.A., damos cobertura al resto de las, digamos, "Iberdrolas" y a las compañías que componen el Grupo Industrial. Para que nos hagamos una idea, la primera línea está compuesta por siete compañías, y con el resto del Grupo con más de 250 (llegamos hasta las 253). ¿Cuántas personas damos cobertura a este universo desde la Unidad de Seguridad de Sistemas de información y Comunicaciones? Pues actualmente diez profesionales, especializados en distintas áreas: normativa legal, procedimentación y documentación.

– ¿Cuáles son sus principales retos como director de Seguridad de la Información y Comunicaciones de una compañía como Iberdrola?

– Poder tener una participación activa, colaborando en la creación de ese valor añadido en los servicios que ofrece Iberdrola, a través de la difusión del concepto amplio de protección de la información entre las Unidades de Negocio de la compañía y entre el Grupo Industrial. Lo que estamos haciendo actualmente es desarrollar un Plan Director de Seguridad para toda la Corporación, dividido en dos fases, una primera para las empresas "Iberdrola", y una segunda, dirigida al Grupo Industrial.

– ¿En qué fase de desarrollo del Plan Director de Seguridad se encuentran?

– Estamos definiendo un modelo funcional y jerárquico, en el que van a tener un papel determinante todos los responsables de los activos de información de la compañía. Nuestra Unidad es un medio y una guía, con la misión de ayudar a asegurar su modelo de negocio. Habrá aspectos que serán de carácter más impositivo, basados en normas y procedimientos; pero, como digo, los responsables de los activos de información van a tener un gran protagonismo en el modelo organizativo y jerárquico del Plan Director de Seguridad.

Fuera ya de esta faceta de planificación, el Plan Director de Seguridad también contiene el consiguiente epígrafe de desarrollo de medidas organizativas y técnicas.

Conviene añadir que, además de la Unidad de Seguridad, con diez profesionales, Iberdrola cuenta cuenta con el resto de su organización para la implantación de medidas técnicas, y administración y gestión de seguridad. Aquí tiene un papel determinante el área de Sistemas, además de los responsables de los activos de información. Nosotros marcaremos los conceptos, la tecnología y las herramientas, y procedimentaremos cómo y de qué manera se tienen que administrar, gestionar y operar para que los grupos específicos del área de Sistemas puedan llevar a cabo la operación de las mismas. Cualquier tipo de modificación o de incidencia que no se pueda recoger dentro de un procedimiento, nos deberá ser remitida, nosotros la estudiaremos, la procedimentaremos y el producto de nuestro trabajo lo difundiremos entre los interesados.

"Los responsables de los activos de información van a tener un gran protagonismo en el modelo organizativo y jerárquico del Plan Director de Seguridad"

– ¿Se están basando en normas internacionales?

– Estamos intentando llevar a la práctica el binomio calidad-seguridad, por lo que nos basamos en normas ISO y en la BS-7799, y en las normas UNE de AENOR. Nuestro objetivo es implantar un sistema de calidad dentro de seguridad.

– ¿Podría mencionar algunos proyectos en el marco del Plan Director de Seguridad?

Los proyectos, para este año en curso, y en el contexto del Plan Director de Seguridad, los tenemos clasificados en tres grandes grupos. El primero corresponde a la protección de nuestra plataforma de cliente. Aquí estamos trabajando en la incorporación de herramientas que permitan hacer un uso más racional del PC. No vamos a restar funcionalidad al puesto; ahora bien, lo que no necesite el usuario para realizar su trabajo, será suprimido. Estamos ya construyendo los primeros prototipos con herramientas tecnológicas de seguridad interesantes, de tal suerte que vamos a poder tener un PC con las máximas funcionalidades en un momento determinado, o convertirlo en un terminal "tonto". Este proyecto va a tener un gran impacto en la cultura de Iberdrola, y a efectos cuantitativos va a afectar aproximadamente a 10.500 usuarios de plantilla, así como a los colaboradores.

El segundo grupo se centra en la protección de las comunicaciones, incluyendo las de voz. Al respecto le diré que tenemos un entorno de comunicaciones muy heterogéneo, disperso geográficamente y con localizaciones también fuera de las fronteras de nuestro país. Disponemos de una red de 9.500 kilómetros de fibra óptica dentro de la organización, y además prestamos servicios de transporte a terceros.

El tercer grupo no es puramente tecnológico, pero consideramos que tiene el mismo peso que los anteriores: la formación y la divulgación de la cultura de seguridad. Si el usuario empieza a valorar la información que trata y a utilizar adecuadamente los medios tecnológicos puestos a su disposición para ello: PCs, soportes..., se evitarán muchos problemas. La verdad es que algunas medidas técnicas de protección, en muchas ocasiones –no en todas, por supuesto– hay que tomarlas por la falta de disciplina de los usuarios.

– ¿Tienen ustedes algún proyecto enfocado a la administración centralizada de la seguridad en el entorno tecnológico heterogéneo de Iberdrola?

– En el Plan Director de Seguridad, y dentro del apartado de medidas organizativas y técnicas, se recoge precisamente el poder disponer de un repositorio de los perfiles operativos/funcionales y de seguridad de los usuarios. Por otra parte, estamos actualmente en un proyecto corporativo muy importante de cambio de la plataforma de puesto básico de trabajo. Se recoge en el marco de esta iniciativa el disponer de un Directorio Activo, conjuntamente con herramientas de gestión y administración centralizada, las cuales son imprescindibles para el desarrollo de nuestra función.

– ¿Qué importancia dan en Iberdrola a las incidencias por código malicioso?

– Queremos poner en práctica el concepto de seguridad planificada, y en este contexto, no

sólo se pretende corregir la incidencia, sino analizar el cómo, el por qué, el cuándo y el por dónde. Esto nos va a permitir el establecimiento de acciones de carácter preventivo, y en algún caso de carácter predictivo, con las medidas de tipo organizativo y/o técnico.

– Interesante lo de seguridad planificada. La verdad es que para solucionar los problemas hay que localizarlos y conocerlos con el debido detalle…

– La intención es llevar una gestión centralizada de todo lo que concierne a seguridad técnica y, además, ser racionales a la hora de disponer de información sobre lo que pasa; queremos ir teniendo la imprescindible e ir dimensionando controles con el punto justo de granuralidad. Vamos a incorporar para ello nuevas herramientas.

– En su opinión, ¿están los fabricantes de herramientas tecnológicas de seguridad a la altura de las diversas necesidad de Iberdrola en esta materia?

– Lo que se espera siempre de cualquier herramienta tecnológica de seguridad es la solución a todos los problemas. Pero eso no existe, por lo que al final, las organizaciones deben ser capaces de componer un entorno de seguridad técnico coherente basado en un conjunto de herramientas sabiamente combinadas. En contestación directa a su pregunta le diré que cada uno en su parcela, sí.

– ¿Y los fabricantes españoles?

– La respuesta es la misma: cada uno es su parcela, sí. No hay demasiadas empresas españolas que desarrollen herramientas tecnológicas de seguridad, y es una pena, porque mi experiencia profesional al otro lado de la barrera, es decir, en el de la oferta, fue muy positiva: existen pocas compañías, pero con una capacidad y con un potencial elevadísimos.

El problema es que muchos todavía piensan que lo de fuera es lo mejor, y, en consecuencia, se potencian poco los desarrollos tecnológicos en seguridad realizados por firmas españolas. Creo que podemos decir con la cabeza bien alta que estamos en esta materia a la altura de cualquier fabricante multinacional, y en algunos desarrollos, por encima. Además, las empresas españolas son más flexibles que los grandes fabricantes, y pueden personalizar muy detalladamente sus productos y servicios profesionales. Las grandes compañías, por aquello de que tenemos mayor peso en el mercado, hemos de apoyar a los fabricantes españoles de herramientas de seguridad. Desde luego, en Iberdrola daremos prioridad a los de 'aquí', en la medida en que dispongan de soluciones tecnológicas para cubrir nuestras expectativas de protección de la información y las comunicaciones. Los productos pueden ser más o menos buenos, pero el elemento que va a dar más juego es el soporte que sobre ellos se tenga con el binomio integrador-fabricante.

– ¿Faltan o sobran en España buenas compañías integradoras con equipos de expertos en seguridad técnica?

– Es bueno que las empresas se hayan dado cuenta de que en general los productos, por sí mismos, no tienen vida, no tienen valor. El valor lo da quien pueda aportarlo, no sólo con el soporte –como antes he apuntado– sino además con la posibilidad de realizar labores de integración en el contexto del 'puzzle' de seguridad adecuado a las características de seguridad de cada organización. Conseguir la interoperabilidad de las distintas tecnologías y herramientas constituye la labor del integrador.

"Las organizaciones deben ser capaces de componer un entorno de seguridad técnico coherente basado en un conjunto de herramientas sabiamente combinadas"

El trabajo de nuestra Unidad, se centra en planificar, organizar y dirigir: no podemos crear unas macro-estructuras departamentales para tener un gran *know how*, unas grandes capacidades de integración. Para eso hay que confiar en compañías integradoras. Están apareciendo firmas con este perfil y con experiencia en la materia, lo que nos va a ayudar a ser más ágiles y rápidos en la consecución de nuestros objetivos de seguridad.

– ¿El peligro, en lo que a inseguridad se refiere, viene de dentro o de fuera de las organizaciones?

– Los problemas de seguridad no vienen de fuera, sino de dentro de las organizaciones. Se ha inflado eso de que el lobo feroz está en Internet. Entiéndame: no es que no sea cierto, porque nuestro indicadores sí lo marcan con claridad, pero la situación real es que en un 75% o un 80% de los informes de auditorías y de diferentes Certs que recibimos se deduce que los problemas se localizan en el interior de las empresas. También hay que reseñar que la mayor parte de éstos no se generan de forma intencionada, sino accidental, precisamente porque el acceso a los sistemas se hace a través de plataforma PC, que no está pensada para la seguridad.

Por eso en Iberdrola damos tanta importancia a la 'securización' de la plataforma cliente, a efectos, entre otros, de intentar reducir drásticamente el porcentaje de problemas de seguridad originados en la misma, que es la más vulnerable de todas, ya que en grandes sistemas y en entornos Unix, el escenario de riesgo está más controlado.

– ¿Destina Iberdrola suficiente dinero a la seguridad de la información?

– Desde el momento en que nos hemos constituido como Unidad, mi respuesta es sí. La sensibilidad de la nueva Dirección de Iberdrola ha hecho muy factible el que se pueda contar con un presupuesto pensamos que adecuado para los objetivos que este año se tienen fijados.

– ¿Qué opina de la legislación española sobre protección de datos personales?

– El objetivo que tiene la Ley, su espíritu, está bien claro; el Reglamento de medidas es más ambiguo, quizá porque los expertos que lo redactaron no identificaron algunos problemas tecnológicos, funcionales y económicos derivados de su cumplimiento.

– Auditoría obligatoria del Reglamento a partir del nivel medio. ¿Están ustedes en ello?

– Uno de los asuntos recogidos en el Plan Director de Seguridad es, precisamente, el concerniente a los Planes de Auditoría. Vamos a crear un grupo, integrado no sólo por componentes de nuestra Unidad, sino también de otras unidades departamentales, los propietarios de los activos de información. En una primera fase, el mandato reglamentario lo estamos cumpliendo con una auditoría interna, que será completada más adelante con otra basada en recursos externos.

– ¿Seguridad vs. calidad?

– No hay seguridad sin calidad, y ambas debemos de medirlas de forma permanente. Precisamente el epígrafe de la auditoría está enmarcado en el plan de seguimiento de la calidad de la seguridad. Si somos capaces de establecer un modelo de seguimiento, entonces la auditoría interna la vamos a estar realizando de forma 'permanente'. Por lo tanto, el proceso puro y duro de auditar un área o una unidad o un bloque de información, no va a requerir una acción especial. La auditoría interna va a ser continua, y lo que haremos es circunscribirnos a la que por imperativo legal se nos pueda exigir, como se recoge dentro de la Ley de Protección de Datos. n

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