economistas
Consejo General
RASI
Asesores de Gobierno y Sistemas de la Información
Σ economistas y titulados mercantiles

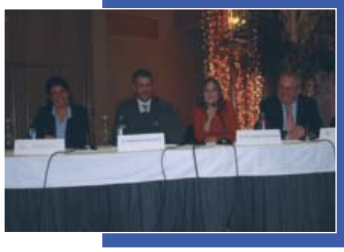
Enero 2014

actualidad RASI

REVISTA RASI · Asesores de Gobierno y Sistemas de la Información

Contenido

Presentación de RASI-CGE



El pasado 29 de Octubre tuvo lugar la Presentación de RASI-CGE en Vigo a cargo de (…)

Página 28

Consejo Editorial

ENTREVISTA

Página 3

¿Qué podría decirles a los que siguen pensando que las redes sociales son algo pasajero?

Le diría principalmente que hay multitud de estudios que revelan el hecho de que los usuarios de internet pasan un alto porcentaje de su (…)

Daniel Marote Escobar

Tribunas de opinión

Las tecnologías de la información: un ACTIVO para las empresas

Josep Puigvert Ibars

En adelante nos referiremos con el anglicismo Workplace al conjunto de Dispositivos, Sistema Operativo, Configuraciones (…) Página 6

Social Media Marketing: ¿Truco o trato?

Esteban García Pérez

Hace solo unas pocas semanas hemos celebrado la tradicional fiesta del día de Todos los Santos y, nos guste o no, lo cierto es que esta (…) Página 11

Gestión de la información basada en una estrategia de riesgo para pymes

Yazomary García García

Actualmente las empresas en Europa están esforzándose más por la gestión de la información, tomando en consideración los niveles de riesgo (…) Página 14

Cómo afecta la zona única de pagos en euros –SEPA– a la empresa

Joaquim Altafaja Diví, CISA, CISM, CGEIT

Con la publicación el pasado 30 de marzo de 2012 del Reglamento UE 260/2012, Reglamento directamente aplicable en todos los Estados (…) Página 15

El efecto contable que debería tener la inseguridad informática

Antonio Ramos

No obstante, identificar el nivel óptimo de protección no es trivial y siempre se producen tensiones entre las áreas de seguridad (…) Página 20

Auditorías de Seguridad. Necesarias por defecto

Daniel Calvo Castro

Compañías de todos los tamaños adoptan hoy en día nuevas tecnologías como el cloud computing, virtualización, o el conocido "BYOD" (…) Página 22

El cambio tecnológico, si no trae consigo un cambio de pensamiento, deja increíbles potenciales aparcados en los márgenes.

«Sin colaboración no hay innovación» es un lema 2.0 que nos recuerda cómo el cambio tecnológico, si no trae consigo un cambio de pensamiento, deja increíbles potenciales aparcados en los márgenes. Es difícil cambiar el enfoque, intentar mirar desde otro punto de vista, replantearse las estructuras. No obstante, la tecnología nos da esa oportunidad. Hablan los expertos de que el futuro estará en los liderazgos colaborativos, en un mundo *groundswell* –el de una sociedad civil organizada donde la generación de redes será la llave para sustentar el cambio– en el que pasar de la potencia al acto sea más una cuestión ética que técnica.

Tecnología para el Cambio

Elisa G. McCausland
Entorno Digital
Unión Profesional

La cultura de la tecnología y la innovación es la cultura del cambio, no solo de la adaptación. Este giro adaptado al mundo profesional redunda en un cumplimiento de los objetivos, donde las ideas y las herramientas tecnológicas tienen, más que nunca y combinadas, un papel clave. Así lo ha entiende la "revista RASI", una publicación consciente de la importancia de la cultura de la tecnología y la innovación para el entorno profesional. Porque es importante saber cómo utilizar las herramientas, cómo hacerlas parte de la organización, del despacho profesional, de ti mismo. En la era de la imagen de marca constante, del «ser en Internet», los profesionales no pueden perder comba ante propuestas tan interesantes como la idea del despacho 2.0, con la capacidad de establecer lazos colaborativos desde cualquier dispositivo móvil y generar tus propias estrategias para adaptarse a un mercado en constante cambio.

Es por esto que la labor de la "revista RASI" es tan importante. Saber qué está por venir, cómo establecer una estrategia digital, qué es importante tener en cuenta en materia de protección de datos o cuáles son las redes sociales que asegurarán nuestra imagen de marca en la arena 2.0 pudo ser tendencia hace un lustro, pero ahora es norma. De ahí que el apoyo a todos los nuevos profesionales de estas áreas, que en lo participativo y multidisciplinar están encontrando un nicho significativo para crecer, sean el futuro de una economía pensada por y para la eficiencia, tecnología mediante.

Pensar en abierto –lo económico, lo tecnológico, lo social– y compartir. Este es el objetivo de esta revista. En abierto, porque la porosidad es importante en los tiempos del 2.0. La idea de compartir como principio capital que la atraviesa, sobre todo, en un contexto de cambio donde los medios se readaptan, buscan fórmulas nuevas, se transforman continuamente para ofrecer ideas, argumentos, soluciones. Para abrir nuevos caminos, dentro y fuera de la Red.

REDES SOCIALES

Daniel Marote Escobar
CEO · Hydra Social Media

No existen fórmulas milagrosas para conseguir nuevos clientes en un escenario en que la competencia es feroz, pero el sentido común nos dice que la combinación de elementos entrelazados seguramente sea la correcta, y el uso de redes sociales puede ser una de ella.

¿Qué podría decirles a los que siguen pensando que las redes sociales son algo pasajero?

Le diría principalmente que hay multitud de estudios que revelan el hecho de que los usuarios de internet pasan un alto porcentaje de su tiempo en internet en redes sociales.

Y eso es algo que, indudablemente afecta a la publicidad, porque el ocio es cada vez más digital, y no únicamente es algo que tengan que tener en cuenta marcas con un público joven.

Si mis clientes no usan redes sociales ¿Por qué debería hacerlo yo?

La tendencia nos dice que si no usan redes sociales, las usarán, y es de sentido común estar preparado para ello.

Se sabe, como decíamos, que la mayor parte de los internautas usan redes sociales.

De hecho, la edad ya no se considera como el factor clave en el uso de redes sociales. Se sabe que el 40% de los usuarios de redes sociales tienen una edad media de 33 años y que, de ellos, el 43% son mayores de 36 años. De esto podemos inferir que las redes sociales ya forman parte intrínseca del día a día de las personas y que están aquí para quedarse.

¿Debemos hacer caso a los que dicen que Facebook está en vías de desaparición?

Siendo sincero, no sabemos qué canales permanecerán. Tenemos ejemplos como Tuenti, que ha posicionado su modelo de negocio como operadora móvil, dejando de lado su monetización como red social, algo que siempre ha sido bastante complicado para este caso concreto, y que ha derivado en la pérdida de casi el 58% de sus usuarios.

Sabemos también, sin embargo, que redes como Twitter están sufriendo un crecimiento imparable.

¿Podemos afirmar que las redes sociales son útiles para reforzar las ventas?

La respuesta es un sí. La clave está en dejar de actuar como empresas o corporaciones y ser conscientes de que esas empresas están formadas por personas. La imagen que una marca desprenda, sea cual sea su actividad, es esencial.

En ese sentido ¿Qué implica tener una gran comunidad en tus redes sociales?

Una gran comunidad de usuario, de "me gusta" en tu página profesional, siempre es bueno porque tus mensajes, a priori, pueden llegar a más gente. Sin embargo, normalmente tendemos a la personalización, es decir, no basta con tener una gran comunidad, lo mejor es siempre tener al público adecuado, de manera que tu mensajes lleguen de manera más profunda. Una gran comunidad implica un gran nivel de conversación, y gracias a ello podremos conocer mejor a nuestros clientes.

¿En qué puede ayudar el social media a los despachos profesionales?

En realidad, y volviendo a lo que decíamos arriba, el social media puede ayudar a conectar personas. No hablamos ya de marcas, sino de usuarios.

Con todo, y desde un punto de vista más concreto, el social media otorga una serie de oportunidades a cualquier negocio que esté dispuesto a abrazar los postulados de las web 2.0.

Por un lado tenemos oportunidades desde una perspectiva más estratégica, ya que podemos vislumbrar tres puntos clave: en primer lugar la **diferenciación respecto a nuestros competidores,** en segundo lugar la posibilidad de implementar nuestro branding o **imagen de marca en una posición de igual a igual respecto a empresas más grandes** o incluso multinacionales y en tercer lugar, nos permite realizar un **estudio de la competencia de manera eficaz y concreta.**

Tenemos, además, **oportunidades en el ámbito comercial.** Sabemos que no existen fórmulas milagrosas para conseguir nuevos clientes en un escenario en que la competencia es feroz, pero el sentido común nos dice que la combinación de elementos entrelazados seguramente sea la correcta, y el uso de redes sociales puede ser una de ellas con un objetivo claro: crear una comunidad de prescriptores que establezcan dinámicas de recomendaciones de boca a boca.

Otro elemento importante a valorar está en el ámbito de los **recursos humanos.** Sabemos que los modelos de contratación han cambiado, y que ahora son los empleados más cualificados los que eligen la empresa en la que quieren trabajar y en ese sentido la reputación de marca es esencial, así como el uso de canales específicos como Linkedin.

La web 2.0 implica, ante todo, democratización. Lo importante es la creatividad en los contenidos, y la poca inversión que ello pueda llegar a suponer.

¿Es necesario tener un gran volumen de negocio para estar en redes sociales?

La web 2.0 implica, ante todo, democratización. Lo importante es la creatividad en los contenidos, y la poca inversión que ello pueda llegar a suponer.

¿Qué redes sociales debería usar un despacho profesional?

Siempre dependerá de la empresa en concreto, de sus necesidades específicas, pero Facebook –al ser la red social mayoritaria– resulta esencial. También Twitter por una cuestión reputacional y, desde luego, Linkedin, por cuestiones de profesionalidad tanto de los empleados del despacho como de sus clientes, proveedores, etc.

Nosotros siempre recomendamos a nuestros clientes una mínima inversión en Twitter, básicamente, como una de las redes sociales con mayor potencial de conversaciones.

¿Vale la pena el riesgo de someterse a las críticas de tus clientes en redes sociales?

Una de las reglas de las relaciones públicas es que en muy pocas ocasiones el silencio es una opción. Siempre mejor controlar los mensajes y, además, un canal de redes sociales te permitirá siempre una relación más estrecha con tus clientes potenciales o actuales y en eso se basará el "boca/oreja" del éxito de tu despacho.

¿Qué presupuesto debo dedicar a social media marketing?

Eso siempre dependerá, por supuesto, de su presupuesto general anual destinado a publicidad, pero lo que hay que tener claro es que siempre es muy recomendable una inversión en publicidad específica en según qué canales, además, por supuesto, de una inversión en desarrollar de manera profesional la gestión de comunidades.

¿Es entonces realmente rentable el marketing en redes sociales?

En el caso de las empresas de servicios, que venden intangibles, como es el caso de un despacho profesional, el uso de redes sociales se rentabiliza a medio plazo, como una perspectiva de reputación de marca, pero es bastante factible, con todo, el cerrar tratos de una manera más instantánea teniendo en cuenta la rapidez de los mensajes.

¿Cómo se rentabiliza entonces una comunidad de usuarios?

Una comunidad de usuarios se rentabiliza teniendo en cuenta el valor de las recomendaciones de esos usuarios. Internet es la primera fuente de información a la hora de documentarse sobre una empresa. Si tus usuarios hablan bien de ti, lo harán en internet y tus clientes potenciales verán todos esos comentarios.

¿Qué podría decirnos como conclusión?

La mayor recomendación que podamos darle a un despacho profesional es que mire a su alrededor y vea cómo es posible construir una imagen de marca sólida con los recursos a su alcance a través de redes sociales.

Es importante ser valiente e innovador, que se tenga un espíritu curioso y se vea de qué manera podemos aportar valor a nuestro negocio, fuera de la zona de confort.

Siempre puede solicitar ayuda si lo considera necesario, nosotros siempre estamos encantados de echar una mano a quien se vea en la necesidad de iniciar nuevas aventuras empresariales.

Las tecnologías de la información: un ACTIVO para las empresas

Utilizadas eficientemente las TI permiten obtener ventajas competitivas.

La ecuación que recae en los departamentos de TI, es cada vez más compleja, hay que reducir los costes y a la vez tienen que ser catalizadores de la innovación para aportar más valor al negocio.

Josep Puigvert Ibars
Miembro del Consejo Directivo de RASI-CGE
CEO en ClaverTask

Nueva concepción del Workplace

En adelante nos referiremos con el anglicismo **Workplace** al conjunto de Dispositivos, Sistema Operativo, Configuraciones y herramienta que facilitan al usuario el acceso a las Aplicaciones y Datos necesarios para realizar su trabajo.

La hoja de ruta del entorno de puesto de trabajo no volverá a ser nunca más única y monolítica, la época de "café para todos" ya pasó a la historia, la "Consumerización" se incorporará a las empresas y traerá inconvenientes, pero sobretodo beneficios.

A este nuevo escenario del entorno de puesto de trabajo, se le llama la "era post PC" y a diferencia de anteriores evoluciones en la que un dispositivo sustituía a otro (PC sustituyó al terminal VT-220), en este caso los Dispositivos Móviles no sustituyen al PC, se añaden al ecosistema.

Otra peculiaridad de este fenómeno es que, así como la incorporación del PC al mundo TIC se hizo de la mano del sector informático, los dispositivos Móviles, lo han hecho de la mano del usuario, de ahí que no sea una incorporación "controlada".

La "consumerización" cuya expresión más concreta referida al entorno corporativo es el BYOD *(Tráete tu dispositivo al trabajo),* se va poco a poco incorporando a las empresas y ese hecho va a plantear nuevos retos. A su vez, una nueva generación –joven y tecnológicamente muy preparada– se incorpora al mundo laboral con una "experiencia de usuario" en relación a la tecnología informática muy superior a la que se pueda encontrar en la plataforma corporativa que le proporciona la empresa; es por eso que el nuevo usuario quiere ahora utilizar su dispositivo de elección (tablets, smartphones, …) para conectarse a la red corporativa de la empresa en la que trabaja. Y eso no nos debe extrañar, igual que no nos extraña que casi nadie utilice la pluma o el bolígrafo que le proporciona la empresa, cada uno se compra y utiliza aquel que le va mejor para hacer su trabajo.

La irrupción de los dispositivos móviles ha trastocado el ecosistema Workplace.

Esta irrupción de elementos nuevos y extraños en un entorno ya establecido y controlado, ya sucedió en otras épocas. Recordemos la época en que el entorno del puesto de trabajo estaba conformado por terminales "tontos" como el VT-220 para sistemas Unix y el IBM-3270 para los HOST IBM y aparecieron los PC's , fue toda una revolución. Los responsables de seguridad y los directores de Informática, en general, pusieron el grito en el cielo, argumentando que si se "liberaba" el acceso a los sistemas a través de la microinformática sería el caos y la pérdida del control de los sistemas y los datos corporativos.

Algo similar está ocurriendo hoy día con la aparición de los Smartphone y los Tablets. En el 2011, cuando empezó el fenómeno de la "Consumerización", si le

hablabas a un Director de Sistemas de incorporar al Workplace estos dispositivos, le cambiaba el semblante como si hubieras mentado a la bicha. Y es una pena, porque al final, antes de dos años, esa integración habrá sido total y se habrán perdido 4 años de beneficios para la empresa, que es lo realmente importante. En general, y en nuestro entorno principalmente, de las tendencias es mejor beneficiarse que oponerse.

Incluso, las empresas más aperturistas en la incorporación de este fenómeno, lo han hecho de forma muy controlada, homologando unos dispositivos concretos a los que se les permitía el acceso. Siendo más positiva esta estrategia, tampoco le vemos sentido a esta fase intermedia, puesto que precisamente este fenómeno se caracteriza precisamente por la **diversidad**. Volvemos otra vez a aplicar pautas aprendidas que nos resolvieron problemas en el pasado para afrontar problemas nuevos, y eso no suele funcionar.

¡No se puede "plataformar" el futuro!

Para controlar los Dispositivos Móviles aplicamos soluciones del mundo de los PC's, y eso no sirve. En este nuevo entorno no debemos controlar el Dispositivo ni el Sistema Operativo ni las Aplicaciones, sino únicamente asegurarnos de que cumple las reglas establecidas por la empresa para conectarse a sus Sistemas.

Es importante no poner prohibiciones en el uso, ni intentar frenar la entrada de estos dispositivos a nuevos usos y roles de usuario, sino incorporar normas y medidas de seguridad apropiadas, para buscar el equilibrio entre un puesto de trabajo seguro y usable.

Hay que perder ese vértigo infundado a los "invasores" de nuestra "estabilidad". Por suerte hay soluciones de sobra para gestionar, controlar y asegurar los Dispositivos Móviles. Las soluciones **MDM (Mobile Device Management)** que existen hoy en día permiten precisamente esa dualidad, en parte contradictoria, de que el usuario pueda hacer lo que quiera con su dispositivo y, al mismo tiempo, la seguridad de los sistemas y la información de la empresa estén a buen recaudo. Porque básicamente la estrategia a seguir con los dispositivos es "en la calle haz lo que quieras, pero cuando entres en mi casa, las normas las pongo yo"; es decir, utiliza el dispositivo para tus cosas, pero cuando te conectes a los sistemas de la empresa deberás cumplir unas condiciones que se establecen mediante políticas de seguridad. Al igual que las soluciones MDM nos permiten establecer las políticas de seguridad, las configuraciones y gestión de aplicaciones en los Dispositivos Móviles, existen soluciones que permiten acceder a la información (ficheros, documentos, etc.) de la organización de forma segura. La solución de Novell, Filr es un ejemplo de cómo compartir la información corporativa de la misma manera que se hace con los puestos clásicos, PC's y Portátiles, añadiendo una capa de gestión para que esa misma información y en las mismas condiciones sea accesible desde los Dispositivos Móviles.

Esta afluencia de nuevos sistemas móviles, origina una gran diversidad de dispositivos a gestionar, y entraña no pocos retos en términos de seguridad y compatibilidad de aplicaciones. A ello hay que sumar la imparable tendencia en términos de virtualización que las empresas están acometiendo, lo que todo unido provoca una gran complejidad de gestión y aprovisionamiento para aquellas entidades que asuman el reto de la nueva diversidad.

Una solución de Workplace contemporánea deberá integrar todas aquellas tecnologías que aporten valor, que resuelvan alguna problemática o que aporten alguna funcionalidad de valor para la compañía

Y no es cuestión de escoger una de ellas, en muchos casos habrá que incluir en nuestra plataforma de puesto de trabajo más de una o todas ellas. Y no debería ser un inconveniente incluirlas, si ello aporta valor, al fin y al cabo son "herramientas" y la evolución de la raza humana lo ha demostrado, la perfección de las herramientas le ha permitido mejorar el desarrollo de tareas que sin ellas hubiera sido imposible o, al menos, mucho más complicado

La concepción del puesto de trabajo de hoy en día y los próximos años, pasa por dar cabida a todas estas tecnologías en base a los requerimientos funcionales reales del empleado y el valor que nos aporta.

No se trata de ELEGIR la tecnología… … se trata de elegir la forma de GESTIONARLA…

Una vez más no se trata de escoger entre blanco o negro, las tecnologías no son buenas ni malas, depende del uso que se haga de ellas. Normalmente cada una de ellas resuelve una necesidad o proporciona una funcionalidad, pero nunca ninguna tecnología resolverá todas las problemáticas relativas al entorno de la plataforma del puesto de trabajo.

Tampoco se trata de polemizar sobre si es mejor virtualizar el puesto de trabajo, utilizar un puesto de trabajo ligero, utilizar un puesto de trabajo tradicional, la utilización de estrategias de virtualización de aplicaciones, puestos de trabajo fijos, móviles, uso de dispositivos diversos, etc. Todas estas tecnologías resuelven de forma eficaz determinadas problemáticas y aportan determinadas funcionalidades, por lo tanto es bueno que formen parte del Workplace de la empresa.

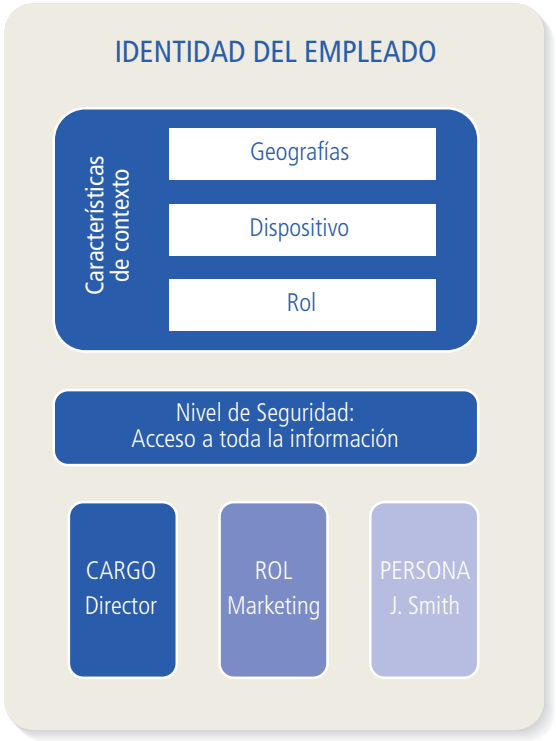
El inconveniente está en que cuantas más tecnología incorporemos, más compleja será la gestión y, por lo tanto, su coste y como ya hemos dicho que el reto está en proporcionar el mejor entorno productivo al usuario, reduciendo el coste de gestión, deberemos buscar alguna solución que compatibilice ese desafío de **más por menos.**

También en este sector influyen los efectos derivados de la ley del péndulo y, en los últimos tiempos, le ha tocado a la Plataforma PC pasar a un segundo plano (en adelante nos referiremos con el término **"Plataforma PC"** a la plataforma tradicional, basada en un PC o portátil, con su SO, aplicaciones y configuraciones) en contraposición a las Plataformas Virtualizadas (VDI, RDP/TS). Creemos que la Plataforma PC sigue siendo vigente y si la sometemos a un proceso de racionalización, optimización y autogestión, podemos reducir su TCO hasta el punto de ser equiparable con el TCO (Total Cost of OwnerShip) de las Plataformas Virtualizadas.

La Plataforma PC sigue teniendo vigencia. Las consultoras coinciden en que un puesto de trabajo bien gestionado puede reducir el TCO hasta en un 36% y reducir el diferencial de TCO con las Plataformas Virtualizadas en menos de un 2%. Por lo tanto, teniendo en cuenta estos parámetros y otros como los costes de transformación, compatibilidad, etc., ambas tecnologías deberán coexistir en las organizaciones.

Las herramientas disponibles actualmente para modelar la Plataforma PC, permiten alcanzar un nivel muy elevado de automatización de los procesos de gestión, administración y provisión, consiguiendo reducir considerablemente los costes de gestión. La razón de la anterior afirmación es que la solución de Plataforma PC debe disponer de los mecanismos automatizados, instalación, re-instalación, gestión y provisión que le hagan equiparable en costes de gestión a las plataformas virtualizadas:

- "Master" Unificado. Utilizando las tecnologías más actuales para la creación de imágenes de instalación conseguimos crear un único "master" con la suficiente lógica para que contemple todos los modelos de equipos de nuestra organización y aquellas aplicaciones y configuraciones que sean comunes a todos los usuarios.
- Aprovisionamiento Automático de Aplicaciones. Con el punto anterior tendríamos instalado un equipo con



las aplicaciones comunes a la organización. Normalmente las organizaciones hacen uso de un número considerable de aplicaciones y muchas de ellas usadas por muy pocos usuarios. Para resolver esta problemática, **deberemos disponer de un sistema de "Aprovisionamiento Automático de Aplicaciones"** que sea capaz de mantener un modelo de datos con el inventario de las aplicaciones de la organización y su asignación a cada usuario de forma que sea capaz de distribuir las aplicaciones específicas de cada usuario. De forma que, en el caso de una reinstalación, finalizada la fase de instalación de la Plataforma Base Común, se obtienen las aplicaciones que corresponden a ese usuario y desencadena la instalación automática de las mismas.

- Instalación/re-Instalación Automática y desatendida de cualquier puesto de la organización independientemente del hardware, aplicaciones o configuraciones que corresponda por el desempeño a al que está destinado.

  Disponer de un sistema que permite re-instalar cualquier puesto de la organización de forma automática y desatendida, es el hecho diferencial de una solución de Workplace dinámica e inteligente que permitirá resolver incidencias derivadas de un mal funcionamientos del equipo, sin desplazamientos y en un tiempo predecible, lo que contribuye a reducir el coste de gestión y la calidad del servicio percibida por el usuario.

Otra de las tecnologías que claramente deben formar parte de nuestra solución de Workplace: la Virtualización de Aplicaciones.

Las aplicaciones virtualizadas pueden reducir hasta el 60% del coste de prueba, paquetizado y soporte de una aplicación, y reducen el TCO total del entorno de escritorio entorno a un 7%, por lo tanto es una tecnología que debemos incluir en nuestro Workplace. Se trata de una tecnología que nos ofrece múltiples ventajas y muy pocos inconvenientes, por lo que la estrategia debe consistir en virtualizar todas aquellas aplicaciones que sean virtualizables. Existen varias tecnologías de virtualización de aplicaciones pero ninguna de ellas es perfecta, deberemos escoger la que mejor se adapte a nuestras necesidades. Dado que el Sistema de Gestión que proponemos nos abstrae de las tecnologías que subyacen, sería posible utilizar más de una tecnología si el beneficio obtenido así lo aconsejase.

Sin obsesionarnos, debemos analizar las soluciones de Plataforma Virtual y casi con seguridad que encontraremos escenarios en que dichas tecnologías darán respuesta a necesidades concretas y proporcionarán funcionalidades que harán necesaria su inclusión en la Plataforma de Puesto de Trabajo. Y en algunos casos puede ser esta tecnología la utilizada mayoritariamente.

Creemos que la concepción del puesto de trabajo de hoy en día y los próximos años, pasa por dar cabida a todas estas tecnologías en base a los requerimientos funcionales reales del empleado y el valor que nos aporta.

Tal como se desarrolla la exposición de nuestro discurso, alguien podría interpretar que cuantas más tecnologías incorporemos al Workplace, mejor. ¡NO! Todo lo contrario. Si podemos dar respuesta a las necesidades del negocio en este ámbito con una sola, considerémonos afortunados pero si, por el contrario, hay que integrar varias tecnologías para dar esa respuesta, no hay que afligirse porque existen soluciones para gestionar uniformemente la diversidad.

EL valor de la solución de Workplace que proponemos radica, no sólo en este nuevo concepto de puesto de trabajo heterogéneo, sino en el uso de herramientas que permitan una gestión homogénea y nos abstraigan de la complejidad tecnológica inherente.

INQUIETUDES

La problemática tiene unas características comunes:

- Las empresas gastan una parte importante del presupuesto IT en la Gestión, Aprovisionamiento y Soporte de la Plataforma Cliente.
- La heterogeneidad del hardware y aplicaciones y la diversidad de los perfiles de usuarios dificulta la gestión uniforme de la Plataforma Cliente
- Desde negocio, cada vez se demanda mayor capacidad de respuesta a las TIC.

RESPUESTAS

La solución del nuevo Workplace cumple con los objetivos:

- Reducir el coste de Mantenimiento
- Optimizar la Gestión mediante herramientas que faciliten una Gestión Homogénea de Plataformas heterogéneas.
- Mejorar el Servicio (aumentar la productividad del Usuario y la calidad de servicio percibida)
- Simplificar el Aprovisionamiento de aplicaciones
- Disminuir el «Time To Market» de aplicaciones y alinear el Negocio con IT.

Evolucionar a un Workplace eficiente, productivo y preparado para poder acceder a las aplicaciones y servicios en cualquier momento, desde cualquier lugar y dispositivo, donde los sistemas sean aprovisionados y gestionados dinámicamente, y donde la agilidad en los servicios permita el equilibrio entre un entorno seguro y flexible.

"El componente más importante en cualquier negocio, son las personas" y, sin embargo, no se tienen suficientemente en cuenta a la hora de diseñar el Workplace, nos preocupamos mucho de la seguridad, la robustez, la "mantenibilidad", etc. y nos olvidamos de lo fundamental, y es que la finalidad del Workplace es proporcionar al usuario herramientas que le faciliten su trabajo. Por eso hay que ser muy sensibles a la hora de tomar determinadas decisiones que van a afectar al usuario en su quehacer diario.

Para dar consistencia al mensaje y visión del nuevo Workplace deberemos disponer de una capa de gestión que nos abstraiga de las tecnologías que lo conforman.

Una capa de gestión que permita definir una arquitectura para el puesto de trabajo, flexible de forma que permita incorporar nuevos dispositivos hardware, así como nuevos servicios tecnológicos sin tener que modificar el modelo. Como decía al inicio, estamos integrando un escenario tecnológico que mañana ya no será igual que hoy, por lo tanto la estructura del edificio hay que pensarla para que cuando cambien algunos de los elementos del Workplace, no tengamos que construir el edificio de nuevo.

Para incorporar la iniciativa de la **"Consumerización"**, al sistema **Workplace** del que venimos hablando, habrán de incorporarse los mecanismos, procesos y procedimientos que gestionen los Smartphone y Tablets, pero eso debe ser trasparente para los agentes que lo gestionan, provisionan o dan soporte. Para entender lo dicho, pongamos un ejemplo: un Workplace que tiene un escenario con varios de los siguientes elementos: PC, VDI, RDS, APPs físicas, APPs virtualizadas, Markets, Stores, Smartphone (iPhone,W8 y Android) y Tablets (iPad, W8 y Android), y que tenemos que distribuir una aplicación a un usuario, el agente encargado de la distribución, solo tendrá que arrastrar el "objeto" aplicación al "objeto" usuario, el sistema ya se encargará de realizar las acciones que corresponda realizando procesos distintos si la aplicación es local o virtualizada, si es un PC, es un Escritorio Virtual, un iPad o un tablet Android.

Este nuevo escenario, el de la movilidad en los accesos a datos y aplicaciones corporativas, debe ser considerado por los departamentos de IT de las organizaciones y también por auditores en sistemas de información.

Social Media Marketing: ¿Truco o trato?

Esteban García Pérez
Miembro del Consejo Directivo de RASI-CGE
Director General de Hydra Social Media Marketing

Hace solo unas pocas semanas hemos celebrado la tradicional fiesta del día de Todos los Santos y, nos guste o no, lo cierto es que esta fiesta cada vez está siendo más sustituida por la tradición anglosajona del día de Halloween.

Según cuenta la leyenda popular, ese día, un terrible espíritu malévolo vaga por los pueblos y ciudades pasando de casa en casa poniendo a sus habitantes en la necesidad de tomar una terrible decisión, "truco" o "trato". La situación no es sencilla. La persona debe escoger sin saber qué va a suceder, es un misterio. No obstante, la leyenda aconseja escoger siempre "trato" ¡incluso sin saber las condiciones del mismo ni el coste que éste pueda llevar aparejado! De lo contrario, el terrible espíritu malévolo promete usar sus enormes poderes para hacer "truco" y proporcionar a la casa y sus desdichados habitantes todo tipo de infortunios.

Afortunadamente, como todos sabemos, la representación de esta leyenda es bastante más festiva que la historia anterior y consiste en que ese día los niños recorren las casas proponiendo "truco" o "trato" a sus habitantes como forma de recolectar dulces. Los habitantes de las casas se exponen, como mucho, a un poco de espuma de afeitar en la puerta o algún huevo estrellado en la ventana si no pagan el precio del trato en forma de unos cuantos caramelos.

Desde mi punto de vista la relación actual entre clientes y empresas tiene mucho de "truco" o "trato".

Las redes sociales han devuelto a los clientes la capacidad de demandar de las marcas una atención esmerada y hasta afectiva, diría yo. Esto es así porque la tecnología social (Web 2.0) se ha convertido en un enorme altavoz que los consumidores estamos aprendiendo a utilizar a marchas forzadas para exigir cada vez más un "trato" no solo correcto de nuestras marcas sino, como en el caso de la festividad de Halloween, un trato "dulce" y cercano.

Cada vez tenemos más y mejor constatación que nuestros clientes están cambiando, tratamos con clientes "conectados" permanentemente, más informados, que comparten sus opiniones y piden las de otros antes de tomar decisiones, que no dudan en recomendar algo o a alguien en sus redes sociales o, por el contrario, criticar abiertamente el trato recibido por alguna de las marcas con las que se relaciona. A este nuevo cliente lo llamamos "cliente digital" y es un tipo de cliente que busca acercarse a las marcas demandando de ellas, además de una relación transaccional justa (trato), un vínculo cada vez más personalizado y basado en las emociones (relación).

Pues bien, igual que en la historia anterior, nuestro nuevo cliente digital sale cada día de su casa y va llamando a la puerta de las empresas con las que quiere relacionarse. Y digo bien, es él ahora más que nunca el que lo decide y, para ello, se basa en un criterio irrenunciable, la reputación. La suma de las opiniones, recomendaciones, experiencias y sensaciones que otros clientes digitales como él y de los que se fía, le dan la pauta sobre a qué "puertas" llamar.

No obstante, y cuando se decide a hacerlo, comprueba que pueden presentársele muchas y variadas situaciones. Veamos alguna:

Primera Situación

No encuentra la puerta. Obviamente estamos hablando en un sentido figurado, pero imaginémonos la increíble situación de acercarnos a una casa y que no podamos encontrar la manera de llamar para que nos abran. Absurdo ¿no? Pues algo muy similar pasa con aquellas marcas que no han desarrollado un correcto posicionamiento en internet. Y claro, no hablamos solo de tener página web. Hoy casi todos tienen una, pero aún pocos han desarrollado una estrategia digital con sentido que permita el contacto directo y sencillo con nuestro nuevo tipo de cliente.

Consecuencia

El resultado es evidente. Como cada vez hay un mayor y mayor número de "clientes digitales", esta empresa tendrá una menor y menor de cuota de mercado. No es difícil adivinar cuál es el final de esta historia.

Consejo

La única ventaja de los problemas evidentes es que suelen tener soluciones fáciles de identificar. En este caso, la empresa debería desarrollar una correcta estrategia en internet que posicionase adecuadamente su marca en el ecosistema digital. Para ello recomendamos los siguientes pasos:

a. Intenta informarte y busca asesoramiento experto. No te lances a invertir recursos sin un plan preestablecido y una finalidad bien definida. En marketing digital no todos los caminos llevan a Roma y resulta bastante duro darse cuenta al final del recorrido que no hemos conseguido los resultados que esperábamos.

b. Teniendo en cuenta lo anterior, desarrolla una presencia digital que proporcione contenidos de valor a tus clientes. Como dice el refranero popular: "El que regala bien vende si el que recibe lo entiende". ¡Asegúrate de que los visitantes a tu página reciban algo de valor y ellos sabrán recompensártelo".

c. Idea, desarrolla y ejecuta una estrategia en redes sociales que potencie tu comunicación y atraiga tráfico hacia tu página web. Allí les esperará algo especial para ellos.

d. ¡Sé perseverante!

Segunda Situación

El "cliente digital" localiza fácilmente nuestra puerta. Es de las más llamativas, está bien construida y tiene un bonito timbre que invita a llamar. Sin embargo, una vez que lo hacemos, la manera en que somos recibidos y tratados no nos proporciona una experiencia positiva, más bien sentimos que somos tratados como mero objeto de oportunidad de negocio.

Volviendo a nuestro ejemplo de Halloween, es como llamar a una casa esperando recibir dulces y que el dueño nos dé un portazo en las narices.

Consecuencia

La reacción es de esperar, nuestro "cliente digital" saldrá de la casa lanzando un huevo a la puerta para manchar así la reputación de la familia delante de todo el vecindario y que los que vengan detrás de nosotros no se molesten en perder su tiempo con tales individuos.

Si retomamos el punto de vista empresarial, enseguida nos daremos cuenta que este tipo de empresas está desarrollando su base de clientes de manera errónea. Su manera de enfocar la relación con los clientes está ahuyentando a aquellos interesados en mantener un vínculo estrecho con su marca y que son capaces de aportar un mayor valor a medio y largo plazo. ¡Se están quedando con aquellos clientes oportunistas más sensibles al precio! Grave error.

Pero, no siendo suficiente malo esto, los clientes desengañados se encargarán de dejar constancia de su desencanto en las redes sociales como aviso a navegantes, perjudicando mucho la reputación de la empresa.

Consejo

En este caso, a diferencia del anterior, la solución es bastante más compleja y, llegado este momento, debemos tomar conciencia de que las redes sociales son un potente "aparato de Rayos X" que ponen de manifiesto a los ojos de todos tanto los aspectos positivos de las empresas como los negativos.

La cultura interna de una compañía no es fácil de cambiar. Es el caso de la manera en que consideramos y tratamos a nuestros clientes. ¿Son para nosotros una mera oportunidad de negocio?, ¿estamos realmente interesados en conocerles y

atenderles con la intención de crear un vínculo a nivel emocional con ellos?, ¿nos contentaremos con operaciones en el corto plazo tipo "si te he visto no me acuerdo" teniendo la oportunidad de crear auténticos fans de nuestras marcas?

Para ello, permíteme tres consejos:

a. Identifica a tus clientes y preocúpate de conocer sus necesidades.

b. Invierte tiempo en diseñar para ellos una experiencia de uso positiva y memorable. Esto les vinculará emocionalmente con la marca y te devolverán tu interés por ellos en forma de fidelidad.

c. Dales voz en las redes sociales. Recuerda que ellos son los que construyen la reputación de la que vives.

Tercera Situación

¡Por fin "trato"! Después de dos malas experiencias, nuestro perseverante "cliente digital" opta por llamar a una tercera puerta. La casa está adornada para la ocasión, todo en ella le llama la atención. Piensa… ¡ésta sí que me cuadra! Además, al fijarse un poco más, ve salir de la casa una pareja con una bolsa llena de caramelos y con una enorme cara de satisfacción. Ahora está seguro, ¡esta vez ha dado con el lugar correcto!

Volviendo al territorio real de nuestras empresas, la historia imaginaria descrita trata de describir aquella situación en la que las empresas han dado, por fin, con la estrategia adecuada de posicionamiento en el entorno digital, su estrategia de contenidos es coherente con su oferta de valor y ésta es correctamente comunicada a su público objetivo a través de los medios sociales (blog corporativo, redes sociales, etc.).

Además, éstos, cuando llegan a la página web de la compañía, no solo pueden encontrar los bienes o servicios que estaban buscando sino que sus expectativas se ven superadas porque encuentran ese "algo más" que necesitan y que alguien dentro de la empresa se ha tomado la molestia de ponerse en su lugar para identificarlo y ofrecérselo.

Resumiendo, la experiencia para él ha sido muy positiva, está agradecido y está dispuesto a compartirlo con otros. Eso es exactamente lo que buscamos.

Consecuencia

El resultado de todo lo anterior es que ahora, además de un cliente satisfecho y fidelizado, hemos creado un embajador de nuestra empresa, alguien que hablará positivamente de nosotros en las redes sociales desencadenando un poderoso mecanismo de "boca-oreja electrónico" que nos permitirá recuperar multiplicado cada recurso que invirtamos en una estrategia de este tipo. Además, poco a poco en nuestra base de clientes irá teniendo cada vez más peso un tipo de clientes más sensible al valor y no tanto al precio. Como la sabiduría popular bien dice: "recogemos lo que sembramos" y en el mundo digital más.

Consejo

Ahora hemos llegado al punto que queríamos alcanzar, ¡enhorabuena! Pero el viaje aún no ha terminado. De hecho esto es un viaje que nunca debe terminar, la mejora debe ser continua y para ello lo recomendable sería:

a. Invierte aún más en conocimiento y personalización de tus clientes.

b. Traza un programa de innovación que, trascendiendo el ámbito digital, termine trasformando la organización hasta que sea completamente "cliente céntrica". Para ello, considera la posibilidad de utilizar técnicas de co-creación para asegurarte que nunca se pierde la perspectiva del cliente.

c. Investiga nuevos recursos digitales y utilízalos solo si tienes claro que podrás ponerlos al servicio de tu estrategia digital.

d. ¡Nunca te des por satisfecho!

CONCLUSIÓN

La tradición de Halloween nos recomienda siempre pactar antes que exponernos al truco del malvado espíritu. Hoy nuestros clientes nos colocan ante una tesitura similar, llaman a nuestra puerta demandando conocernos mejor y relacionarse con nosotros, quieren saber más antes de tomar una decisión. Y todo ello en el medio digital. Ellos, al igual que los niños en Halloween, se acercan a nuestra puerta y nos preguntan: ¿truco o trato?

La pelota está en nuestro tejado. Caramelos o portazo. Abro mi casa a mis clientes y le proporciono una "dulce" experiencia o les doy "calabazas".

La decisión es de cada uno de nosotros. El resto de nuestra historia quedará escrita en las redes sociales.

Gestión de la información basada en una estrategia de riesgo para pymes

Yazomary García García
Asesora del Consejo Directivo de RASI-CGE

Actualmente las empresas en Europa están esforzándose más por la gestión de la información, tomando en consideración los niveles de riesgo a los cuales se encuentran expuestas. Si bien es cierto que la concienciación sobre la exposición al riesgo y la necesidad de gestionarlo en las Pymes ya no es el problema, sí lo es la carencia de estrategias y medidas que permitan gestionar la información adecuadamente y a unos niveles de riesgos bajos. En un momento donde las vulneraciones de la seguridad de los datos, el aumento de las redes sociales y los ciberataques están en su punto más alto y la filtración de datos crece exponencialmente, las Pymes continúan totalmente desprotegidas frente a daños irrevocables que pueden originar una filtración de los datos.

Se hace imperativa la necesidad de las empresas de gestionar el volumen de datos creciente al que se enfrentan. La cantidad de datos, tanto digitales como en papel, que crece cada año de forma exponencial, exige la definición de políticas, procesos y uso de herramientas y tecnologías que permita a las empresas la categorización de la información, para así poder determinar aquélla que se debe guardar o destruir; en función a las diferentes normativas que existen en referencia a la conservación de documentos empresariales.

En este sentido, la manera de proteger los datos es diseñando una estrategia general de seguridad de la información basada en un conocimiento de los riesgos y amenazas, entre los que podemos citar: robo de información, pérdida de datos, falta de confidencialidad, incumplimiento normativo, etc., así como de la aplicación de mecanismos de supervisión de la seguridad de los datos. En general se pueden citar algunas medidas, consideradas por los expertos como las más eficaces, y buenas prácticas para la gestión de la información:

- **Desarrollo de una estrategia de riesgo de la información,** considerando:
  - Medio de almacenamiento, cómo se transfieren y cómo se eliminan los datos, tanto internos como externos. Para ello se deben identificar los datos que se tienen, la cantidad de almacenamiento electrónico por tipos de ficheros y bases de datos, la cantidad de archivos físicos, etc.
  - El proceso, la tecnología y los controles de personal que se necesitan para gestionar la información durante su ciclo de vida.
  - La identificación, si los datos son gestionados en la empresa, por un tercero, en su país, fuera, etc.
  - El diseño y aplicación de controles de seguridad de la información.
  - La concienciación y aumento de la cultura de responsabilidad por la seguridad de los datos y de la información.
- **Compromiso de la alta dirección** por el desarrollo y cumplimiento de la seguridad de la información en toda la organización.
- **Estudio del valor de los datos,** del gasto en seguridad de la información y del costo de su reemplazo; todo esto como una medida de concienciación y de valoración de los datos.
- **El desarrollo y la comunicación a toda la empresa de un proceso de gestión de la información** que incluya la clasificación, almacenamiento, condiciones de tratamiento de datos, retención de datos, normas de supervisión de la seguridad de los datos, copias de seguridad y mecanismos de control de acceso a los datos.

La información mal gestionada puede hacer que las empresas queden expuestas a un mayor nivel de riesgo de pérdida y robo de datos, de incumplimiento de la normativa de conservación de documentos y de costes ocultos. Es por ello que en las Pymes se hace necesario una mayor involucración por parte de la alta gerencia, en la definición de la estrategia a seguir para gestionar la información en conjunto con el área de informática, para garantizar la aplicación de mecanismos de control suficientes que proporcionen una adecuada seguridad, confidencialidad e integridad de la información. Si bien es cierto que las Pymes deben funcionar efectivamente y con ventaja competitiva también lo es que la información es un recurso valioso, diferenciador y competitivo.

Cómo afecta la zona única de pagos en euros –SEPA– a la empresa

Joaquim Altafaja Diví, CISA, CISM, CGEIT
Asesor del Consejo Directivo de RASI-CGE

Con la publicación el pasado 30 de marzo de 2012 del Reglamento UE 260/2012, Reglamento directamente aplicable en todos los Estados de la Unión Europea, se dio luz verde a la creación de un mercado integrado de pagos electrónicos en euros, sin distinción entre pagos nacionales y transfronterizos. El proyecto de zona única de pagos en euros (Single Euro Payments Area, SEPA) persigue la implantación de servicios de pago comunes a toda la Unión Europea que sustituyan a los actuales servicios de pago nacionales. Inició su andadura con la Directiva Europea de Servicios de Pago en diciembre de 2007 y transpuesta a la legislación española mediante la Ley de Servicios de Pago en diciembre de 2009.

La introducción de normas, disposiciones y prácticas de pago estandarizadas y comunes, mediante el procesamiento integrado de los pagos, supone un nuevo paso en la integración europea y debe aportar a los ciudadanos y empresas de la UE servicios de pago en euros seguros, a precios competitivos, de fácil uso y fiables. En este sentido, el Reglamento UE 260/2012 introduce la igualdad de condiciones económicas (tarifas) en operaciones nacionales y transfronterizas sin límite de cuantía.

A estos efectos, a partir del **1 de febrero de 2014,** todas las transferencias y domiciliaciones bancarias se realizarán de acuerdo con las reglas SEPA y desde esa fecha, sólo podrán realizarse aquellas operaciones que respeten las características técnicas y de negocio de los instrumentos SEPA, siendo, por tanto, necesario la adaptación de todos los usuarios en el plazo previsto debiendo acomodar, entre otros aspectos, el manejo de sus órdenes de domiciliación, los datos a intercambiar en la cadena de pago o los formatos de inicio de sus órdenes de cobro y pago.

Sin embargo, la Comisión Europea el pasado 9 de enero de 2014, destacó que los avances que se han producido en la migración hacia la zona única de pagos en euros (SEPA) no están siendo los suficientes como para garantizar un cambio completo sin riesgos para el nuevo sistema el próximo 1 de febrero. Por lo tanto, la Comisión propone introducir un período transitorio adicional de seis meses, para garantizar una mínima perturbación a los consumidores y a las empresas.

En la práctica esto significa que la fecha límite para la migración sigue siendo el 1 de febrero 2014, pero los pagos que difieran de un formato SEPA podrán seguir siendo aceptados hasta el **1 de agosto 2014,** según la propuesta realizada por la Comisión Europea.

Una de las principales novedades que introduce SEPA es que los usuarios de servicios bancarios pasarán a utilizar el código IBAN (Código Internacional de Cuenta Bancaria), en lugar del actual Código CCC (Código Cuenta Cliente) para identificar su cuenta. Además con la nueva normativa, el usuario receptor de adeudos (deudor-ordenante) podrá exigir a su entidad bancaria un mayor control antes de que dichos cargos se anoten en su cuenta.

Instrumentos SEPA

Los instrumentos de pago afectados por la introducción de SEPA y las características de cada uno de los instrumentos existentes se detallan en los siguientes apartados. Resulta importante destacar la distinción que realiza SEPA entre los pagos entre Empresas y Consumidores *(B2C-Business to Customers)* y los que afectan exclusivamente a Empresas y Autónomos *(B2B- Business to Business).*

Instrumentos de pago afectados a fecha 1 de febrero de 2014

Recibos (Cuaderno 19)	Correspondientes a cuotas o pagos, generalmente de carácter periódico, por suministros o prestación de servicios.
Aportaciones de fondos	Adeudos domiciliados en los que el cliente ordenante y beneficiario coinciden y en los que existen, además, limitaciones en cuanto al importe y frecuencia de los mismos.
Anticipos de crédito (Cuaderno 58)[1]	Correspondientes a derechos de crédito legítimos ostentados por el cliente ordenante frente a sus deudores por operaciones específicas de su actividad comercial o empresarial.
Recibos (Cuaderno 32)[1]	Documento expedido en el tráfico mercantil, en cualquier soporte escrito incluido el informático que, por sí mismo, acredita, literalmente y con carácter autónomo, el derecho económico de su legítimo tenedor para cobrar de la persona que designe y en el lugar y fecha, que, con independencia de los de emisión, el propio documento señale, una cantidad determinada en dinero o signo que lo represente.
Transferencias (Cuaderno 34)	Ordenadas en España, tanto de residentes como de no residentes, en concepto de transferencia, nómina o pensión.
Órdenes de Traspaso de Efectivo	Traspaso de dinero entre cuentas de la misma titularidad situadas en entidades distintas, que se formaliza mediante la orden dada por un cliente a la entidad que ha de recibir el dinero, para que ésta la transmita a la entidad de la cuenta de cargo. El traspaso se materializa mediante transferencia desde la entidad de la cuenta de cargo a una cuenta de la misma titularidad en la entidad solicitante del traspaso.

1. Exención autorizada hasta 1 de febrero de 2016

Transferencias de Crédito (SEPA Credit Transfer)

Definición	Movimiento de fondos iniciado por el pagador (deudor-ordenante), en los que éste envía una orden de pago a su entidad bancaria (entidad remitente), que traspasa los fondos a la entidad bancaria del beneficiario (entidad receptora)
Producto asimilado	Sustituye a las actuales transferencias. (Cuaderno 34)
Ámbito	En euros, de cuenta del ordenante a cuenta del beneficiario, sin límite de importe
Contenido	El detalle del pago es de 140 caracteres que se envían en su totalidad
Gastos	Compartidos entre el ordenante y el beneficiario
Materialización	La operación se materializa a más tardar el día siguiente a la ejecución de la orden (D+1)
Identificación	El IBAN será el único dato identificativo válido del beneficiario
Formato	Entre Bancos es obligatorio XML ISO 20022, entre cliente y banco lo será a partir de febrero de 2016, pudiendo utilizarse hasta esa fecha el formato AEB 34.14
Tipología del pago	Indica el objeto de la transferencia de forma genérica (nómina, pensión, pago de impuestos, pago a proveedor, …)
On behalf of	Permite enviar pagos por cuenta de, último ordenante
Último beneficiario	Permite enviar pagos a favor del último beneficiario

Transacción de Adeudo Directo Básicos o Core *(SEPA Direct Debit – B2C)*

Definición	Es el medio de pago mediante el cual la cuenta del pagador (deudor – ordenante) se adeuda a iniciativa del beneficiario (acreedor) en virtud de un mandato previamente autorizado (mandato u orden de domiciliación). El acreedor y deudor pueden ser particulares y/o empresas
Producto asimilado	Sustituye a los actuales recibos domiciliados. (Cuaderno 19)
Intervinientes	La transacción depende de la conexión de cuatro intervinientes, el acreedor y su banco, el deudor y su banco
Contenido	El actual recibo domiciliado admite 640 caracteres, el nuevo formato admite un **máximo de 140 caracteres**
Presentación	*Ver Figura 1*
Reembolso	Para las operaciones autorizadas 8 semanas, las operaciones NO autorizadas 13 meses
Identificación	El IBAN será el único dato identificativo válido del beneficiario
Formato	XML ISO 20022 Core, hasta febrero de 2016 admitido AEB 19.14
Tipología del pago	Cuotas o pagos, generalmente de carácter periódico, por suministros o prestación de servicios
Excepciones	*Ver Figura 2*

Transacción de Adeudo Directo *(SEPA Direct Debit – B2B)*

Definición	Es el medio de pago mediante el cual la cuenta del pagador (deudor – ordenante) se adeuda a iniciativa del beneficiario (acreedor) en virtud de un mandato previamente autorizado (mandato u orden de domiciliación). El acreedor y deudor deben ser personas jurídicas o autónomos. **No permite obtener financiación**
Producto asimilado	Sustituye a los actuales anticipos de crédito. (Cuaderno 58)
Intervinientes	La transacción depende de la conexión de cuatro intervinientes, el acreedor y su banco, el deudor y su banco
Contenido	El actual recibo domiciliado admite 640 caracteres, el nuevo formato admite un **máximo de 140 caracteres**
Presentación	*Ver Figura 1*
Reembolso	Para las operaciones autorizadas el deudor renuncia al derecho de devolución, las operaciones NO autorizadas 13 meses
Identificación	El IBAN será el único dato identificativo válido del beneficiario
Formato	XML ISO 20022 B2B, hasta febrero de 2016 admitido AEB 19.14 – 19.44
Tipología del pago	Pagos por operaciones específicas de la actividad comercial o empresarial sin posibilidad de financiación
Excepciones	*Ver Figura 2*

Figura 1 · **SEPA Direct Debit - Cronograma**

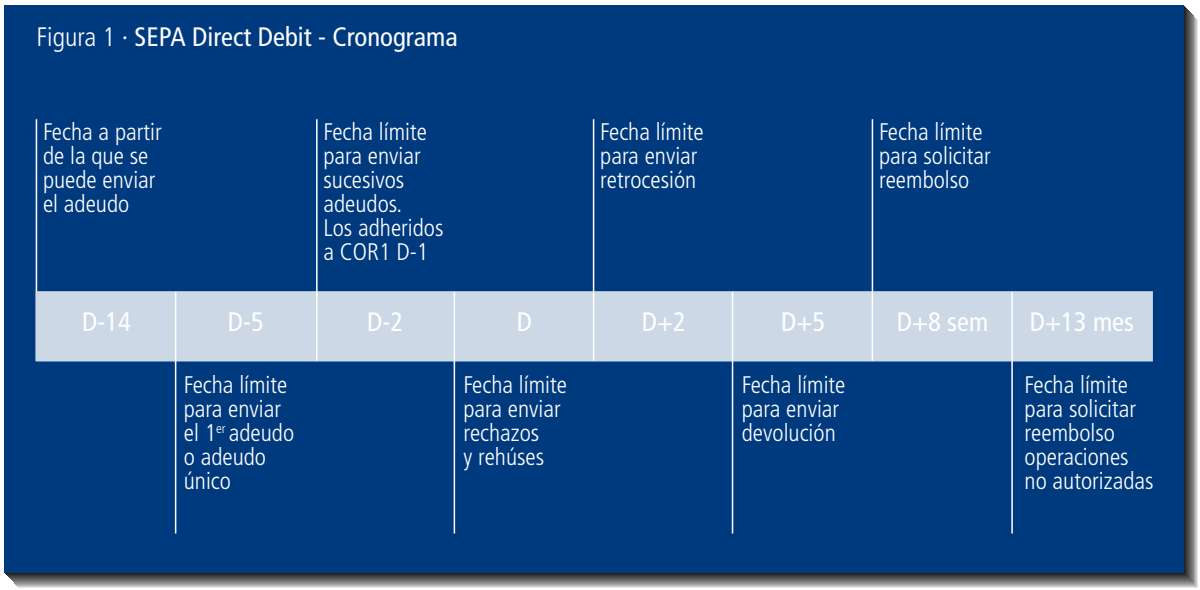


Figura 2 · **SEPA Direct Debit - Transacciones-R (Excepciones)**

Reembolso	Posibilidad del deudor de solicitar que se le reintegre un adeudo, una vez ha sido cargado en su cuenta. En esquema B2B no existe para operaciones autorizadas
Rechazo	Posibilidad del deudor de instruir a su banco sobre el No pago de un adeudo. El plazo es de 1 día para oficina
Devolución	No ejecucción de un adeudo motivada porque el banco deudor no puede hacerlo efectivo. Los posibles motivos de devolución son falta de saldo, deudor fallecido, etc. El plazo para llevar a cabo la devolución en B2B es de 1 día para oficina
Cancelación	Solucitud del banco acreedor por instrucción del acreedor de cancelación de un adeudo antes de la liquidación. El plazo para la retrocesión es de 2 días antes de la liquidación
Retrocesión	Solucitud del acreedor de anulación de un adeudo que ya ha sido ejecutado. El plazo para la retrocesión es de 1 día

El mandato en adeudos directos SEPA

Es el medio por el que el deudor autoriza y consiente al acreedor a: (a) iniciar los cobros mediante el cargo en cuenta indicada por el deudor (b) autoriza a la entidad del deudor a cargar en su cuenta los adeudos presentados al cobro por la entidad bancaria del acreedor.

El mandato debe estar suscrito por el deudor como titular de la cuenta de cargo o por persona que disponga de un poder otorgado por éste.

El mandato firmado debe quedar almacenado en poder del acreedor mientras esté en vigor, durante el período de reembolso, así como durante los plazos que establezca la Ley para la conservación de documentos, una vez cancelado.

La importancia del mandato (órdenes de domiciliación)

El mandato es el documento que como acreedor confiere el derecho o crédito comercial ante los clientes.

La correcta recogida, custodia, mantenimiento y gestión es crucial con la entrada en vigor del nuevo Reglamento.

La no existencia de un mandato, la incorrecta gestión del mismo o su mantenimiento descuidado, puede acarrear graves riesgos operacionales e incluso pérdidas económicas.

Flujo del mandato

El acreedor envía el mandato, ya sea en formato papel o electrónico, al deudor para cumplimentación (datos personales y bancarios) y firma.

El deudor devuelve el mandato cumplimentado y firmado al acreedor.

El acreedor una vez que dispone del mandato firmado puede iniciar los cobros de acuerdo con los requisitos establecidos.

Si el mandato está en papel el acreedor transforma los datos a un soporte electrónico (desmaterialización del mandato).

Los datos del mandato se envían de forma electrónica junto con cada adeudo a la entidad bancaria del acreedor.

La entidad bancaria del acreedor envía electrónicamente los datos del mandato a la entidad del deudor en un único flujo como parte de la transacción de cobro utilizando el mecanismo de compensación seleccionado.

Validez de los mandatos existentes

De acuerdo con el artículo 7.1 del Reglamento UE 260/2012: *"Las autorizaciones válidas de un beneficiario para el cobro de adeudos domiciliados periódicos en un sistema tradicional antes del 1 de febrero de 2014 seguirán siendo válidas con posterioridad a dicha fecha y se considerarán representativas de consentimiento para que el proveedor de servicios de pago del ordenante ejecute los adeudos domiciliados periódicos cobrados por dicho beneficiario con arreglo al presente Reglamento, de no existir una normativa nacional o acuerdos con los clientes que mantengan la validez de las órdenes de adeudos domiciliados".*

Lo que supone que para la migración de las operaciones de domiciliación al Adeudo Directo SEPA Básico o Core regulado por el citado reglamento no se tendrá que recabar un nuevo consentimiento y queda a la elección del acreedor que efectúe una comunicación a su cliente, que comenzará a recibir información con diferente codificación a la que está acostumbrado. Si bien, el mandato SEPA requiere alguna información obligatoria que no recogen las órdenes de domiciliación actuales.

El mandato en nuevos adeudos directos SEPA Básicos o Core

En cualquiera de los instrumentos de adeudo para emitir operaciones de adeudo, es necesario que previamente exista una orden firmada por el deudor para domiciliar los pagos. La gestión de dicha orden será entre acreedor y deudor y será custodiada por el acreedor.

Caso de no existir ese mandato se entenderá que la operación no está autorizada.

El cliente deudor da su consentimiento tanto al beneficiario, como a su entidad indirectamente a través del beneficiario, por lo que los mandatos, así como toda modificación o cancelación posterior, han de quedar en poder del beneficiario (o de un tercero por cuenta de éste) por el tiempo que le pueda ser requerido.

Cuando el acreedor no presente adeudos con arreglo a un mandato válido en un período de 36 meses (a contar desde la fecha del último adeudo, independientemente de que este fuera pagado, rechazado, devuelto o reembolsado), el mandato queda extinguido y, por tanto, no podrá iniciar más cobros acogidos a dicho mandato, debiendo crear uno nuevo para cobros futuros.

A partir de febrero de 2014 deberá recogerse el nuevo formato de mandato para nuevos contratos, cambios de banco, cambio de referencia del mandato, cambios de referencia del acreedor, etc. La gestión con el banco será la misma que con un primer adeudo, al igual que la pre-notificación.

El mandato en nuevos adeudos directos SEPA B2B

Es un nuevo producto con condiciones operativas diferentes, requiere al acreedor recopilar mandatos B2B de todos sus deudores.

Existe un formato normalizado, es recomendable utilizarlo para cumplimentar los datos obligatorios.

La gestión será entre el acreedor y el deudor y será custodiada por el acreedor.

El deudor debe autorizar a su banco el mandato antes del primer adeudo al renunciar al derecho de devolución.

Instrumentos y obligaciones exentas hasta 1 de febrero de 2016

El reconocimiento, a efectos de la Comisión Europea, de los anticipos de crédito (cuaderno 58) y de los recibos (cuaderno 32) como productos nicho, ampliándose hasta febrero de 2016 el plazo de migración de los mismos

En línea con lo anterior, y hasta la misma fecha del 1 de febrero de 2016, no será exigible el requisito de tener que emplear los formatos de mensaje XML ISO 20022 para el intercambio de operaciones entre los clientes y los proveedores de servicios de pago en el caso de aquellos usuarios que inicien o reciban transferencias o adeudos domiciliados individuales agrupados para su transmisión

La habilitación hasta el 1 de febrero de 2016, para que los proveedores de servicios de pago puedan, discrecionalmente, ofrecer servicios de conversión gratuitos de CCC a IBAN a los clientes que sean consumidores y para las operaciones de pago nacionales.

¿Cómo afecta a la empresa?

La introducción de la Zona Única de Pagos en Euros supone para la empresa un ajuste en sus sistemas organizativos e informáticos debiendo reemplazar el actual código CCC por el código IBAN, adaptar sus procesos internos para generar los nuevos formatos de adeudos domiciliados y por último recoger, gestionar y custodiar adecuadamente la orden de domiciliación o mandato, en resumen gestionar todo el ciclo de vida de los mandatos SEPA y en este sentido, cabe destacar los siguientes aspectos.

Formatos de intercambio

- Generación del nuevo formato SEPA
- Adecuación del campo de concepto
- Creación del identificador del acreedor
- Cambio del CCC por IBAN
- Gestión de Transacciones-R (Excepciones)

Pre-notificación

- Acuerdo con deudores
- Adecuación de procesos

Mandatos

- Migración de antiguos mandatos
- Firma de nuevos mandatos
- Generación de la referencia del mandato
- Gestión y custodia
- Adecuación del proceso operativo

Plazos

- Adaptación a los nuevos plazos de presentación
- Adecuación de los procesos operativos

Comunicación

- Garantizar que el banco deudor puede recibir adeudos SEPA B2B
- Sistema y/o ERP de transmisión
- Comunicación de retorno de la transmisión
- Información para la conciliación

Riesgos

- Mayor tiempo de devolución
- Líneas de crédito

SEPA ya está aquí y ha venido para quedarse, no espere al último día para aprender a convivir con él.

Antonio Ramos

Presidente de ISACA Madrid

Socio Director
de n+1 Intelligence & Research

El efecto contable que debería tener la inseguridad informática

Hoy en día nadie pone en duda que los sistemas de información son una pieza básica en la mayoría de las organizaciones y que la información es uno de sus activos más valiosos. Por ese motivo, dotarse de una protección adecuada es fundamental para garantizar que la organización alcanza sus objetivos corporativos.

No obstante, identificar el nivel óptimo de protección no es trivial y siempre se producen tensiones entre las áreas de seguridad (control) que persiguen mayores niveles de protección y las áreas de negocio que lo perciben como un coste y mayores dificultades operativas.

Encontrar un punto de equilibrio entre ambas posturas es difícil, no sólo por las propias particularidades de la seguridad (como, por ejemplo, su componente aleatorio –aunque no invirtamos en seguridad puede que nunca suframos un incidente– aunque es más probable) si no también porque, en muchas ocasiones, la seguridad es una externalidad[1].

Esta característica hace que, normalmente, las decisiones que tomemos en relación a la seguridad presenten un sesgo por no incluir en la "ecuación" los efectos que tienen sobre otros nuestras decisiones en materia de protección, sobre todo cuando son insuficientes. Esto puede parecernos extraño, pero no lo es en absoluto. Un primer ejemplo sería la protección de datos de carácter personal; si no fuera por la Ley que impone sanciones en caso de una vulneración de su confidencialidad, las empresas no tendrían motivaciones para invertir en evitarlas, puesto que sus efectos los sufrirían los titulares de los datos, pero no la propia empresa.

Pero podríamos pensar en otro supuesto muy interesante; imaginemos que somos una pequeña empresa que vende zapatos por Internet. Para poder llevar a cabo nuestra actividad tenemos un software de gestión empresarial, un servidor web con nuestra tienda online, un servidor para compartir los recursos de red (impresoras, ficheros…) y alrededor de 30 puestos de usuario. Quizás pudiéramos pensar que tenemos poca posibilidad de sufrir un ataque cuya finalidad sea robarnos (información, fondos…) pero es factible que si nuestra infraestructura no está bien protegida:

- Nuestro servidor web sea vulnerado para instalarle software malicioso que infecte (o, al menos, lo intente) a todos los que visiten nuestra página.
- Instalen troyanos[2] en los equipos de nuestros usuarios para controlarlos de manera remota (lo que recibe la denominación de *botnet)* y lanzar ataques contra otras organizaciones o "simplemente" para enviar correo basura *(spam).*

En este caso vemos que los efectos de una seguridad insuficiente los sufren terceros ajenos a mi organización (los visitante de nuestra página web que son infectados o las organizaciones que son objeto de ataques a través de *botnets).*

Por este motivo, es importante que la falta de seguridad tenga un efecto sobre las organizaciones; de esta forma, las decisiones que se adopten en este materia estarán más cerca de la decisión óptima para todo el sistema.

Una vez dicho esto, las consecuencias pueden ser a posteriori o a priori. Lógicamente, si queremos evitar incidentes, será mucho más adecuado que dichas consecuencias sean lo más a priori posible. En particular, ¿cómo podríamos hacer que la inseguridad fuera considerada en la toma de decisiones de los gestores corporativos? **La propuesta que exploraremos en este artículo es que la inseguridad tuviera reflejo contable como un menor valor de los activos**[3].

Si aceptáramos este principio, entre otras cosas:

- La organización debería evaluar periódicamente la presencia de vulnerabilidades o amenazas sobre los sistemas de información y reducir el valor de dichos

activos de manera proporcional (en mayor medida, cuanto más graves fueran éstas).

- Dicha reducción de valor debería afectar también a los procesos de negocio a los que dan soporte los sistemas de información, ya que podría cuestionarse que pudieran servir para generar ingresos (un sistema inseguro es rechazado por los usuarios que, por ejemplo, no comprarían en el portal de nuestra pequeña empresa del ejemplo).

- Dado que la reducción de valor tendría su reflejo en la cuenta de resultados de nuestra organización, los gestores no podrían ignorar el nivel de seguridad de los sistemas y, más aún, tendrían incentivos a protegerlos, puesto que un sistema vulnerable supondría un resultado inferior y los efectos consecuentes sobre las cotizaciones bursátiles y los variables de los directivos.

- Las revisiones de seguridad pasarían a tener una importancia mucho mayor a una simple buena práctica y la responsabilidad de los revisores (auditores) aumentaría de manera equivalente, implicando una mejora de la calidad de este tipo de actividades.

- Dado que los auditores de cuentas tienen que opinar sobre la valoración de los activos, tendrían que incorporar revisiones de seguridad informática en sus procesos (no solo para dar fiabilidad a la información financiera) y comprobar que los sistemas de información no presentan riesgos de seguridad graves (es decir, que la valoración contable de los activos es acorde a su nivel de seguridad).

En definitiva, un escenario mucho más adecuado para asegurar que las empresas protegen los activos de información y con ello, contribuyen a un mayor nivel de seguridad de todo el ecosistema social en el que vivimos ya que no debemos olvidar que los sistemas de información están interconectados y el nivel de seguridad es tan fuerte como el eslabón más débil.

1. Una externalidad es aquella situación en la que los costos o beneficios de producción y/o consumo de algún bien o servicio no son reflejados en el precio de mercado de los mismos. En otras palabras, son externalidades aquellas actividades que afectan a otros para mejorar o para empeorar, sin que éstos paguen por ellas o sean compensados. Existen externalidades cuando los costos o los beneficios privados no son iguales a los costes o los beneficios sociales.

2. Un troyano es un tipo de software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo le brinda a un atacante acceso remoto al equipo infectado. El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero.

3. La Resolución de 18 de septiembre de 2013, del Instituto de Contabilidad y Auditoría de Cuentas, por la que se dictan normas de registro y valoración e información a incluir en la memoria de las cuentas anuales sobre el deterioro del valor de los activos contiene todo el soporte necesario para articular esta propuesta.

Auditorías de Seguridad: Necesarias por defecto

Daniel Calvo Castro
Ingeniero de Clientes. Departamento de Seguridad y Desarrollo de Secure&IT

Compañías de todos los tamaños adoptan hoy en día nuevas tecnologías como el cloud computing, virtualización, o el conocido "BYOD" (tu dispositivo de casa al trabajo), que a la vez que facilitan movilidad y eficiencia, añaden una nueva ventana ante un eventual ataque informático.

A pesar de la relevancia de firewalls, detectores de intrusiones, anti-virus de última generación y otras tecnologías de seguridad subyacentes, la mayoría de compañías son víctimas de ataques informáticos, ya sean dirigidos específicamente o aleatorios, debido a errores malintencionados de configuración y puesta en marcha de cualquier servicio en la red, bien a través de la propia red interna de la compañía, o en servicios de cara al público.

Las compañías están empezando a reconocer la importancia de la experiencia humana en el análisis de una arquitectura de red que se plantee mantener segura.

Los servicios de hacking ético ofrecen a sus clientes evaluaciones objetivas y del mundo real sobre debilidades de seguridad, vulnerabilidades, riesgos asumidos y contramedidas oportunas. Como resultado de ello, el hacking ético o test de intrusión (pen-testing) se está convirtiendo en una práctica esencial de seguridad que se debe realizar regularmente.

En ellas se abordan diferentes y elaborados análisis, dependiendo del tipo de Hacking-Ético que se ejecute, tales como la recogida de toda información que existe sobre una compañía en Internet y sus trabajadores, servicios en la nube, subdominios de la organización, visibles o no, análisis de vulnerabilidades de dichos servicios, explotación e informe en servidores de correo, páginas web, bases de datos, sistemas de telefonía para evitar fraudes, Wireless, etc.

Se suele organizar de diferentes maneras, dependiendo y asesorando a los clientes en qué consisten estos servicios: Caja Negra o Caja Blanca, y siempre bajo unos estrictos acuerdos de confidencialidad.

La diferencia entre Caja Negra y Caja Blanca radica en que en Caja Negra se realiza la auditoría desde el exterior o interior, sin conocimiento ninguno sobre la estructura de la organización, es decir, sin información alguna, escenario habitual de un atacante; en Caja Blanca, por el contrario, se acuerdan diferentes aspectos a auditar, tales como diferentes rangos IP de la organización, o algunas contraseñas de dispositivos, como pueden ser switches, facilitados por la propia compañía.

Desafortunadamente para los intereses de muchas de estas compañías, asumen incorrectamente que nunca serán objetivo de un ataque dirigido o que pueden seguir operando bajo prácticas obsoletas en cuanto a materia de seguridad.

Información: El activo más valioso

La información es considerada uno de los mayores activos de las empresas de hoy en día, y la fuga de la misma es más común de lo que pensamos.

Si atendemos a estudios recientes de Gartner en 2010 sobre fuga de información, podemos observar como entre un 80% y un 90% de dichas fugas son no-intencionales, accidentales o resultantes de procesos empresariales mal realizados.

La concienciación por parte de ejecutivos, empresarios y trabajadores que desconocen este riesgo es notable, ya que centran sus esfuerzos en el normal funcionamiento y productividad de la compañía.

Así mismo, un reciente estudio de la UE afirma que el 49% de los empleados se lleva información cuando cambia de trabajo, afirmando además que el empleado es el elemento menos predecible y controlado en cuanto a amenaza de seguridad se refiere.

Otro dato interesante radica en que el 63% de las empresas públicas y privadas pierden anualmente archivos de información valiosa, pero sólo el 23% procede de robos. De la pérdida de información, el 57% se debe al extravío de equipos como portátiles, móviles,

agendas electrónica, tablets, discos compactos o memorias USB tan extendidos hoy en día.

Como ejemplo, en 2007, un empleado de Boeing fue acusado de robar 320.000 ficheros sensibles que sacaba de la compañía en una memoria USB. Boeing estimó en el informe de la detención que si solamente una porción de los documentos robados fuera dada a los competidores podría costar a la compañía entre 5 y 15 mil millones de dólares.

Es por esto que existen unos determinados riesgos y amenazas para las compañías, las cuales pueden verse afectadas por cualquier vulnerabilidad o amenaza:

- Erosión de la confianza de la firma en el sector.
- Pérdida de volumen de negocio respecto a su competencia.
- Sanciones civiles.
- Sanciones criminales en el peor de los casos.

Riesgos por los que las empresas necesitan tomar medidas preventivas de seguridad para evitar que se produzcan estas fugas, informando y concienciando a sus empleados en materia de seguridad.

Por tanto, el principal objetivo que nos marcamos los auditores de seguridad cuando realizamos nuestro trabajo es el equilibrio de una balanza en un proceso continuo que incluya:

- Valoración minuciosa y continua de dónde residen los riesgos.
- Establecimiento de barreras para mitigar los riesgos.
- Aproximación proactiva a la seguridad en general.

Implantación de sistemas: Vorágine IT

El áuge de las telecomunicaciones y las tecnologías informáticas, han hecho que la implantación de los sistemas se vea envuelta en una vorágine de tiempos de entrega de servicio y puesta en marcha que impiden a los propios integradores el realizar auditorías de seguridad regulares en sus implantaciones o simplemente hacer una revisión de vulnerabilidades en los diferentes sistemas utilizados.

Resulta curioso cómo de fácil se puede comprometer la seguridad de una compañía y acceder a su información desde el exterior solamente porque los empleados no han actualizado su lector de PDF. Y lo mismo sería aplicable tanto a aplicaciones Java, como a sistemas de telefonía IP.

"¿Cómo es posible? Yo tengo un firewall"

Estamos acostumbrados a pensar que un firewall de por sí bloqueará todos los ataques entrantes a nuestro equipo, con lo que una conexión atacante hacia un equipo interno puede ser bloqueada por el propio diseño y tecnologías de los firewalls, pero un estudio a través de las redes sociales sobre un perfil tecnológico bajo de un empleado de la compañía hará posible un ataque dirigido mediante correo electrónico o algún enlace malicioso a través de Facebook o Twitter, convirtiéndose así en una ventana de entrada hacia el equipo, y por ende, a los recursos que él posee y sus compañeros de trabajo.

Esto también ocurre mientras navegamos, puede que sin darnos cuenta accedemos a un sitio web legítimo que puede haber sido comprometido para alojar Malware ofuscado entre códigos html, y que se ejecutan en el contexto del navegador infectando nuestro sistema, pudiendo pasar a ser parte de una Botnet para la realización de ataques de Denegación de Servicio, en el mejor de los casos. Ejemplos de esto pueden ser las web de PHP.net recientemente, anunciado en la lista de Hispasec Sistemas una-al-día, o la web oficial de la NFL con motivo de la Super Bowl estadounidense, comprometida el mismo día de la celebración de la final y que recibe millones de visitas diarias en los días previos a la cita.

Es por todo esto que **la seguridad de la información a través de Auditorías de Seguridad de Hacking-Ético o Pen-Testing se hace indispensable,** elaborando valiosos informes de mitigación de riesgos que permitirán, con la educación y formación de los empleados, mantener una óptima seguridad que permita a los diferentes departamentos, desarrollar su trabajo en un entorno mucho más seguro.

OBLIGACIONES RELATIVAS A LAS COOKIES

Estoy creando la página web de mi despacho ¿qué soluciones técnicas puedo implantar para cumplir con las obligaciones relativas a las cookies? ?qué información debe facilitarse a los usuarios? ¿existe algún tipo de cookie para la cual no es preceptivo recabar el consentimiento expreso del usuario?

En el momento de crear la web, o si ya se dispone de una página, lo que hay que plantearse en primer lugar es la necesidad real de incorporar cookies en la misma. En la mayor parte de los casos no son necesarias y pueden evitarse, ya que muchos desarrolladores o entornos las introducen por defecto sin nuestro conocimiento. Es una buena idea utilizar las herramientas del propio navegador para saber qué cookies se han insertado y eliminar aquellas que realmente no tienen utilidad.

Si, de todas formas, se considera necesario o conveniente utilizar cookies, es obligatorio informar de su existencia al iniciar la navegación, el propósito las mismas y la forma de evitar su instalación, solicitando el consentimiento del usuario antes de instalarlas. Asimismo, ha de informarse de las consecuencias de no permitir el uso de cookies en el servicio que la página web proporciona al usuario. Por lo tanto, toda esa información ha de estar visible en la página principal o la primera página del sitio en la que acceda el usuario.

En la ley se contempla una excepción al deber de obtener el consentimiento informado, que es cuando las cookies son esenciales para prestar el servicio que está reclamando de la página web o para la implementar la comunicación a través de la red. Las cookies se consideran exentas siempre que cumplan algunas de las dos condiciones.

Es adecuado tener dos niveles de información, de forma que en el primer nivel se proporcione la anteriormente señalada de forma general, y además un enlace a una segunda página con una explicación más detallada de los tipos de cookies, propósitos del tratamiento, medios de oposición, etc. La información sobre cookies ha de aparecer diferenciada de la política de privacidad y ha de indicar explícitamente si están utilizándose cookies de primera parte, o gestionadas por el propio dueño de la página, o de tercera parte, gestionadas por una entidad distinta del dueño de la página, como son generalmente las cookies de analítica web.

En este último caso, ha de existir un contrato entre el dueño de la página y la entidad que gestiona las cookies, sobre todo si estas manejan datos de carácter personal, en el que se limite el propósito del tratamiento a lo necesario para el funcionamiento de la página o lo declarado en la información proporcionada al usuario.

Hay que permanecer atentos a los futuros cambios que se prevén en la normativa sobre cookies y que aparecen en el proyecto de la nueva Ley General de Telecomunicaciones, que modifica los apartados relativos a este tema de la Ley de Servicios de la Sociedad de la Información.

LEY ORGÁNICA DE PROTECCIÓN DE DATOS

En nuestra empresa, un despacho de 22 trabajadores, dedicado a auditoría y asesoría fiscal y contable, estamos poniendo al día nuestro sistema para dar cumplimiento a las obligaciones derivadas de la Ley de Protección de Datos personales. En cuanto al documento de seguridad que tenemos que realizar, quería saber qué contenidos han de incluirse, quién ha de tener acceso a dicho documento y si tenemos que enviarlo a la Agencia Española de Protección de Datos para su revisión.

El documento de seguridad tiene carácter interno dentro la empresa, debe mantenerse siempre actualizado y ha de recoger toda la información señalada en la normativa de seguridad establecida al respecto. Deberá plasmar la integridad de las medidas, normas, reglas, obligaciones… que rigen el trabajo en esta materia, asegurándose además que, las mismas, se adaptan a las exigencias legales. Además, recogerá las funciones y obligaciones del personal que vaya a tratar los datos. En este sentido, deberemos asegurarnos de que dicho personal sea conocedor de sus funciones y obligaciones en dicha materia. Asimismo se recogerán las posibles incidencias surgidas de manera que las mismas puedan ser solucionadas y evitadas en el futuro. No es necesario enviar dicho documento a la AEPD para su revisión, no obstante, deberá estar disponible ante un posible requerimiento por la autoridad competente, dentro del marco de una posible inspección.

Disponer del documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar.

Como mínimo el contenido del documento de seguridad ha de ser el siguiente:

- Ámbito de aplicación.
- Especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares de seguridad.
- Funciones y obligaciones del personal.
- Estructura y descripción de los ficheros y sistemas de información.
- Procedimiento de notificación, gestión y respuesta ante incidencias
- Procedimiento de copias de respaldo y recuperación de datos
- Medidas adoptadas en el transporte, destrucción y/o reutilización de soportes y documentos.

Si además existen datos de nivel de seguridad medio y/o alto, de forma adicional a lo anteriormente manifestado habrá de incluirse:

- Identificación del responsable de seguridad.
- Control periódico del cumplimiento del documento.

En definitiva, se podrá incorporar al documento cualquier otra medida que se considere oportuna para incrementar la seguridad de los tratamientos, o incluso, adoptar las medidas exigidas para un nivel de seguridad superior al que por el tipo de información les correspondería, teniendo en cuenta la infraestructura y las circunstancias particulares del despacho.

En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, dicha circunstancia debe hacerse constar en el documento de seguridad, haciendo referencia al contrato suscrito y su vigencia, y mención expresa a los ficheros afectados por esta circunstancia.

El RLOPD especifica que se puede disponer de un solo documento que incluya todos los ficheros y tratamientos con datos personales de los que una persona física o jurídica sea responsable, un documento por cada fichero o tratamiento, o los que determine el responsable atendiendo a los criterios organizativos que haya establecido.

En el nuevo Reglamento General de Protección de Datos que está por aprobar a nivel europeo se instaura la figura del Delegado de Protección de Datos o DPO. ¿Qué implica para un despacho de asesores fiscales de 20 empleados la figura del DPO?

La figura del Delegado de Protección de Datos, Data Protection Officer o DPO, se introduce en el nuevo Reglamento General de Protección de Datos como obligatoria con ciertas condiciones, y su existencia es la justifica a la posible desaparición de la obligación de registrar los ficheros en el Registro de Protección de Datos.

Esta figura no es nueva en Europa, aunque no existía en el ordenamiento español sí que se encontraba en la regulación de protección de datos de varios países europeos. En el nuevo Reglamento se especifican de forma concreta sus funciones y se subraya su independencia y dedicación exclusiva al puesto. Esto último es muy importante, ya que la tarea del DPO no es una más que tendrá que asumir un miembro de la empresa, como ocurre en algunos casos con el responsable de seguridad.

No todas las empresas, por el hecho de tratar datos de carácter personal, habrán de tener designado un DPO. La regulación propuesta señala que sólo será obligatoria en los organismos públicos, las empresas de más de 250 empleados y aquellas empresas de menor tamaño en que las que el tratamiento de datos personales que realizan, por su naturaleza, alcance y/o fines, requieran un seguimiento periódico y sistemático de los interesados.

Esta última condición, que aparece en el artículo 35.1.c, puede ser la que más preocupe a un despacho como el que se refleja en la pregunta. Es un aspecto que ha estado en debate por su oportunidad y su falta de precisión. Muchos interpretan este apartado como la forma de introducir la obligación del DPO en aquellas empresas que, aunque sean de pequeño tamaño, tengan un elevado volumen de tratamiento de datos personales, y que habrá que ponderar teniendo en cuenta grado de sensibilidad de la información que manejan (por ejemplo datos de salud). Habrá que esperar a la entrada en vigor del nuevo Reglamento para ver los criterios que se establecen para la interpretación del mismo.

¿Puede un empresario abrir el correo electrónico de sus empleados?

La actuación descontrolada de los medios tecnológicos que el empresario pone a disposición de sus empleados, supone unos riesgos de salida de información sensible de la entidad, de daños en su reputación e imagen pública e incluso responsabilidades penales para la empresa. Bajo éste escenario no resulta extraño que el empresario quiera vigilar qué uso se realizan de los medios tecnológicos y en ese contexto, la doctrina jurisprudencial delimita los requisitos concretos para no incurrir en mobbing, persecución injustificada o trato discriminatorio.

Dentro del ámbito del derecho laboral, de un lado está cómo se documenta y se hace pública la política de la empresa en relación al uso no consentido de los medios tecnológicos puestos a disposición del trabajador en el entorno laboral, y de otro cómo se lleva a cabo la intervención a un trabajador en concreto.

La primera cuestión quedo diáfanamente definida en la Sentencia del Tribunal Supremo de 26 de septiembre de 2007 y que se pronuncio sobre la necesidad de la existencia de una política comunicada para poder intervenir la navegación y abrir los medios tecnológicos entregados al trabajador para el cumplimiento de la prestación laboral. Sin embargo, la referida sentencia no se refería a la apertura de los correos electrónicos.

La reciente Sentencia del Tribunal Constitucional de 7 de octubre de 2013 en recurso de amparo 2907/2011 ha venido a integrar el correo electrónico como parte de los que puede incluirse entre las materias objeto de instrucción empresarial, dando un paso más allá, y no ser necesaria la existencia de una política comunicada individual para cada organización sino que es suficiente que la misma, de manera incluso genérica, se contenga en un convenio colectivo sectorial. Basta, según el caso analizado, con que el mismo prohíba la utilización de los medios informáticos propiedad de la empresa para fines distintos de los relacionados con el contenido de la prestación laboral.

Cabe destacar que el fallo del Constitucional no entra a valorar el contenido de los correos electrónicos sino cómo se accedió a los mismos y si ese acceso suponía una vulneración de los derechos fundamentales del trabajador.

El Tribunal Constitucional entiende que la mención en el convenio a la limitación de uso con fines privados de los medios tecnológicos de la empresa era una advertencia suficiente para que no tuviese "una expectativa fundada y razonable de confidencialidad respecto al conocimiento de las comunicaciones mantenidas por el trabajador a través de la cuenta de correo proporcionada por la empresa". Así, considera que no se ha vulnerado ni su derecho al secreto de las comunicaciones ni su derecho a la intimidad.

Establecido cómo el aviso ha de producirse, queda ahora establecer cómo y en qué condiciones se puede escanear la actividad de un trabajador en concreto.

El razonamiento del Tribunal Constitucional hace uso de su doctrina sobre el carácter no ilimitado del derecho a la intimidad en el supuesto de colisión con otros intereses constitucionalmente relevantes. Así, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos:

- Si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad)
- Si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad)
- Y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)

En este sentido, se trataba en primer lugar de una medida justificada, puesto que, conforme consta en la sentencia de instancia, su práctica se fundó en la existencia de sospechas de un comportamiento irregular del trabajador.

En segundo término, la medida era idónea para la finalidad pretendida por la empresa, consistente en verificar si el trabajador cometía efectivamente la irregularidad sospechada al objeto de adoptar las medidas disciplinarias correspondientes.

En tercer lugar, la medida podía considerarse necesaria, dado que, como instrumento de transmisión de dicha información confidencial, el contenido o texto de los correos electrónicos serviría de prueba de la citada irregularidad ante la eventual impugnación judicial de la sanción empresarial; no era pues suficiente a tal fin el mero acceso a otros elementos de la comunicación como la identificación del remitente o destinatario, que por sí solos no permitían acreditar el ilícito indicado.

Finalmente, la medida podía entenderse como ponderada y equilibrada.

Resulta importante destacar de esta Sentencia, que la empresa que realice una intervención a un trabajador deberá pasar el juicio de idoneidad, necesidad y proporcionalidad para valorar si la infracción de la intimidad, que se produce en todo caso, está justificada. Y, además, no podemos olvidar que el artículo 197 del Código Penal sigue considerando delito punible con penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses al que "para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación".

formación

Se está cerrando la programación de otros cursos, tanto presenciales como online, de los que os mantendremos oportunamente informados.

Formación On Line

- Curso on line de Prevención de Blanqueo de Capitales y Financiación del Terrorismo. Expertos.
- Curso on line de Prevención de Blanqueo de Capitales y Financiación del Terrorismo. Socios y directivos.
- Curso on line de Protección de Datos Personales.

Formación Presencial

- Ayuda y Referencias a las Nuevas Técnicas en la Auditoría de Cuentas en entornos informatizados.. 3 horas
- Enfoque práctico a la Auditoría de Cuentas en entornos informatizados. 6 horas
- Enfoque al riesgo en la Auditoría de Cuentas, NIAs, PBC, LOPD, etc. 4 horas
- Entorno de control interno:
  Controles generales. 4 horas
  Controles de aplicación. 4 horas
- Responsabilidad penal: delitos económicos. 3 horas
- Novedades legislativas en materia de PBC. 4 horas
- Novedades legislativas en materia de LOPD. 4 horas
- Curso de Auditor Jefe en ISO 9001: 2008. 4,5 días
- Curso de Auditor Jefe en ISO 14001: 2004. 4,5 días
- Curso Auditor Jefe / OHSAS 18001: 2007. 4,5 días
- Curso de Auditor Jefe en ISO 27001: 2005. 4,5 días

Los Colegios interesados en realizar estos u otros cursos a nivel territorial, por favor, contactad con RASI a través del siguiente correo electrónico: rasi@economistas.es

Presentación de RASI en el Colegio de Titulares Mercantiles de Madrid

Dado el éxito de la sesión de presentación de RASI Auditores de Gobierno y Sistemas de la Información del Consejo General de Economistas realizada Vigo en Octubre, se repite esta vez en el Colegio de Titulares Mercantiles de Madrid, a cargo de **Sara Argüello.**

Curso para despachos profesionales

El pasado 26 de Noviembre, **Esteban Romero Frías** impartió el curso *"Cómo aprovechar los servicios de Internet en los despachos profesionales".*

Además de introducir conceptos básicos: web 2.0, medios sociales, trabajo en la nube y cultura digital; se explicaron los medios sociales de internet en la comunicación y en la gestión interna de conocimiento de los despachos.

Colaboración de RASI en el informe E-Pyme

Desde Fundetec han contactado con el Consejo General de Economistas para solicitar un año más su colaboración, a través de RASI-CGE, en la elaboración de la nueva edición del informe E-Pyme.

Fundetec

Presentación de RASI en Vigo

El pasado 29 de Octubre tuvo lugar la Presentación de RASI-CGE en Vigo a cargo de **Joaquim Altafaja** y **Sara Argüello.**

Además, se hizo una breve presentación de la guía para el auditor a la hora de evaluar controles generales, a disposición de los miembros de RASI.

De izda. a dcha.: Raquel Borrajo, Joaquim Altafaja, Sara Argüello y Francisco Vázquez

The Institute of Chartered Accountants in England and Wales

El pasado 17 de Octubre, el Vicepresidente de The Institute of Chartered Accountants in England and Wales - ICAEW **–Arthur Bailey–** hizo una visita al Presidente del RASI y del REA+REGA Auditores del CGE, **Carlos Puig De Travy,** con motivo de su presencia en el Congreso anual de Chartered Accountants en España, celebrado en la ciudad de Barcelona.

Entre los temas centrales discutidos durante la visita, podemos destacar:

- Los retos de la profesión en el entorno económico actual.
- La situación actual del mercado de Auditoría en España y Europa.
- Principales iniciativas de ambas organizaciones.
- Posibles temas de colaboración y sinergias entre ambos.

En la mayoría de los temas compartieron opiniones y posturas, especialmente coincidieron en que unos de los principales retos de la profesión es cambiar el enfoque de cómo se concibe la Auditoría, la cual debería ser considerada también como un servicio que aporta valor añadido a las organizaciones. Para ello, el auditor debe tener un mayor conocimiento y especialización en la industria en cuestión, así como del entorno informatizado. Sobre este tema, se comentó que ambas instituciones compartirán sus experiencias, conocimientos y buenas prácticas.

De izda. a dcha.: Yazomary García, Arthur Bailey, Agustí Saubí, Ángel Hermosilla y Luis Santaló.

En la reunión estuvo presente **Yazomary García,** miembro del Consejo Directivo de RASI-CGE, quien compartió los avances alcanzados hasta la fecha por RASI en cuanto a la formación del auditor en temas relacionados con el entorno informatizado, donde se gestionan los principales procesos de las compañías.

Una vez finalizado el encuentro, **Arthur Bailey** realizó una visita guiada a las instalaciones del Colegio de Economistas de Catalunya, en compañía de **Ángel Hermosilla,** Director del Aula de Economía, y **Luis Santaló,** Secretario Técnico, donde se explicaron las diferentes actividades que realiza el Colegio relacionadas con la Auditoría de Cuentas.

Presencia de RASI en el 4º AuditMeeting

En el marco del 4º AuditMeeting, organizado por REA+REGA Auditores del CGE, se presentó la ponencia *"Presencia del auditor en la red"*, a cargo de **Francisco Sierra,** vocal del Consejo Directivo de REA+REGA del CGE, y **Esteban Romero,** profesor de la Universidad de Granada y próximo miembro del Consejo Directivo de RASI-CGE. Fue moderada por **Joaquim Altafaja,** asesor del Consejo Directivo de RASI-CGE.

De izda. a dcha.: Joaquim Altafaja, Esteban Romero y Francisco Sierra

4º AuditMeeting

Se repasó la incidencia de las nuevas tecnologías en los despachos profesionales, destacando el necesario cambio cultural de éstos para sacarlas provecho, sin olvidar el peso de la tecnología sobre los modelos de negocio que fuerzan la desaparición de unos y la aparición de otros.

Asimismo, en el AuditMeeting se expuso una ponencia sobre *"Prevención de Blanqueo de Capitales"*, a cargo de **Pilar Cruz-Guzmán,** del SEPBLAC.

ÚLTIMAS INCORPORACIONES

Colegio de Economistas de Albacete:

Castillo Rodriguez, Francisco Javier	Nº 362

Colegio de Economistas de Alicante:

Sogorb Pomares, Teofilo	Nº 343

Colegio de Titulares Mercantiles de Alicante:

Palomares Miralles, Pascual	Nº 354

Colegio de Economistas de Baleares:

Ramírez Aguilar, Julio	Nº 340

Colegio de Economistas de Cádiz:

Gómez Garcia, Francisco Javier	Nº 332

Colegio de Economistas de Castellón:

Planelles Segarra, Salvador	Nº 346
Felip Bardoll, Francisco Javier	Nº 348

Colegio de Economistas de Córdoba:

Lomas Molina, Miguel	Nº 331

Colegio de Titulares Mercantiles de Córdoba:

Velasco Maturana, Carlos	Nº 344

Colegio de Economistas de Extremadura:

Sánchez Pulido, Agustin Javier	Nº 335

Colegio de Economistas de Granada:

Castellano Arjona, Francisco	Nº 339

Colegio de Titulares Mercantiles de Granada:

Romero Frias, Esteban	Nº 361

Colegio de Economistas de La Coruña:

Pita Wonenburger, Xabier	Nº 341
Reigosa Cubero ,Javier	Nº 360
Ordoñez Castro, María Begoña	Nº 366
Juega Cuesta, Juan José	Nº 370

Colegio de Titulares Mercantiles de La Coruña:

Palleiro Barbeito, Ricardo	Nº 355

Colegio de Economistas de Las Palmas:

Cabezas de Herrera Santamaria, Pedro	Nº 352
Alonso Sosa, Pedro	Nº 369

Colegio de Economistas de Madrid:

Pérez Iglesias, Alberto Manuel	Nº 330
Villar Fernández, Carlos	Nº 337
Moreno Gallego, Luis Santiago	Nº 353
Calero Pérez, Mª Loreto	Nº 358
Rodríguez Fernández, Pedro	Nº 363
Gredilla Bastos, José Manuel	Nº 364
Moracho García, José María	Nº 365

Colegio de Titulares Mercantiles de Madrid:

Rivera Dianez, Eduardo	Nº 368

Colegio de Economistas de Málaga:

Hernández Calviche Emilio	Nº 334
Sánchez Varela Enrique	Nº 338

Colegio de Titulares Mercantiles de Málaga:

Martín Gutiérrez, Pedro Juan	Nº 357

Colegio de Titulares Mercantiles de León:

Vallinas Antolín, Miguel Pedro	Nº 303
Llamazares Martínez, Ismael	Nº 324
Rodríguez Llanos, Manuel	Nº 326

Colegio de Economistas de Murcia:

Nicolás Chaparro, Guillermo	Nº 350
Cotera Manzanera, Diego de la	Nº 367

Colegio de Economistas de Pontevedra:

Monforte Perez, Carlos S.	Nº 336

ÚLTIMAS INCORPORACIONES

Colegio de Economistas de Sevilla:

Trujillo Fuentes, Rafael	Nº 347

Colegio de Economistas de Tenerife:

Hernández González, Juan Ramón	Nº 345
Ramos Alonso, Alberto	Nº 351

Colegio de Economistas de Valencia:

Escarti Carbonell, Juan Carlos	Nº 342
Raimundo Terrada, Jesús	Nº 349

Colegio de Economistas de Valladolid:

González Moreno, Ana Mª Begoña	Nº 333

Colegio de Titulares Mercantiles de Zamora:

Salvador Montero, Luis	Nº 356

Asociados:

Llado Palau, Albert	Nº 359
Nandwani Villalba, Ricardo Moises	Nº 371

REGISTRO DE EXPERTOS EN PBC Y FT

Calle Arenas, Mª Isabel
Raduan Domenech, Mauro
Marin Ospino, Alfonso
Calders Pidemunt, Josep Maria
Soltero Ramírez, Javier
Carbo Royo, Begoña
Martínez Ortega, Antonio
Prado Villarreal, Alberto
Vilalta Miquel, Jordi
Barrasate Barrenechea, Juan Ángel
Díaz José, Joan
Tur Riera, María
Fernández Palazuelos, Eva
Jerez Iglesias, José
Torices García, Alex
Fernández Carrasco, María José
Martin Moya, Cristina
Navarro Siles, Xavier
Polo Riego, Myriam
Pons Rocañin, Sergi
Robles Sánchez, Thais
Canudas Obradors, María
Moises Falco, Xavier
Mestre Llop, Miquel
Massana Llorens, David
Pascual Hervas, Ricardo
Ibarrola Navaz, José Luis
Ceresuela Fernández, Alejandro
Donadeu Prieto, José María
Heredia Heredia, Carmelo
Carreras Fornells, Josep
Quadras Puig, Luis de
Oro Sole, Mónica
Serra Subirana, Ana
Álvarez Melcon, Sixto
Mato Fernández Demetrio

RASI

cumplimiento normativo (PBCyFT, protección de datos ...)

cloud computing

e-commerce

estrategia digital

social media

influyendo en la Sociedad de la Información

RASI

- Auditoría
- Asesoría Fiscal
- Economía Forense
- Expertos Contables
- Asesoría Financiera
- Docencia e Investigación
- Asesoramiento Laboral

→ Formación
→ Información
→ Investigación
→ Colaboración
→ Apoyo

→ sobre TIC → a todo el Colectivo Profesional

economistas
Consejo General
RASI
Asesores de Gobierno y Sistemas de la Información
Σ economistas y titulados mercantiles

solicitud de inscripción
www.rasi.economistas.es