Título: *La prevención del uso incorrecto de las nuevas tecnologías en la empresa: aspectos prácticos*

Ponente: Juan Alfonso Álvarez García. Director de Relaciones Laborales de La Caixa.

Primero, como os ha comentado mi compañero, cuando las ponencias van las últimas es una faena porque va todo muy condensado y siempre te dejan menos tiempo, como es obvio. Por eso voy a intentar condensarlo lo máximo posible sin llenarles a ustedes la cabeza de cosas. Lo segundo, ustedes también están cansados, ha sido un día muy condensado. Lo tercero, hay riesgo grave de que, a partir de cierta hora, a ustedes les entren ganas de comer, lo cual también hay que tenerlo presente. Y, por último, el riesgo más gordo es que, con la calidad de los ponentes de hoy, el riesgo de que hayan dicho todo lo que se puede decir sobre evidencias electrónicas es muy alto.

Ahora les voy a contar un pequeño secreto, que es por qué acepté ser el último ponente. Fue porque cuando los señores de Cybex se pusieron en contacto conmigo, me llevaron a una conclusión en la que tenían razón. Lógicamente, cuando alguien tiene razón es más difícil defenderse. Me dijeron: "mira, lo que sí que interesa es que vosotros sois una empresa, la Caixa, que habéis trabajado este tema, que habéis implantado cosas y estaría muy bien que, para cerrar la jornada, bajemos al terreno de la realidad". Yo no quiero meterme con el resto de los ponentes, por supuesto, pero los juristas dan su visión, que es muy interesante, los técnicos dan la suya, los poderes públicos más que darla la suelen aplicar… con lo cual, yo creo que es evidente que el tema de evidencias electrónicas afecta más, hoy por hoy, al tema de empresas que a particulares, aunque creo que también llegará a particulares. Entonces, claro, nosotros somos una empresa, nosotros hemos tomado una serie de medidas para evitar el fraude o el mal uso de las herramientas electrónicas y por eso estoy yo aquí.

La segunda pregunta era, señores de Cybex, en la Caixa hay unos departamentos muy potentes de auditores, de informáticos, de técnicos que saben muchísimo más de evidencias electrónicas. Hablando con ellos, llegamos a una conclusión, es que nos interesa mucho la visión desde el punto de vista de las personas porque, al final, detrás de cualquier tema de evidencias electrónicas o cualquier prueba que hemos

estado hablando hace un minuto, hay un comportamiento humano. Un comportamiento humano que, hoy por hoy, se centra sobre todo en la vida de las empresas, no de los particulares. En el momento en que tienes un comportamiento humano en el ámbito de las empresas, ahí entramos nosotros. Normalmente los auditores y los técnicos dicen que deberíamos hacer esto, y luego la empresa consulta a los jurídicos "¿y esto cómo se hace?", pero luego hay que tomar la decisión. Naturalmente, se cabrean contigo los técnicos porque no has hecho todo lo que sería deseable hacer, se cabrean contigo los juristas porque a lo mejor te has quedado un poco corto o has sido demasiado largo; y luego hay que ir con mucho cuidado también porque las cosas que hagamos tienen después muchas repercusiones. Es muy bonito decirlas desde un punto de vista teórico, pero luego corres el riesgo, si te has equivocado, de palmarla. Yo me voy a limitar hoy a explicarles la experiencia que hemos tenido nosotros, que no ha acabado aquí. Nosotros seguimos haciendo cosas y me imagino que, tal y como va este mundo, vamos a tener que hacer muchas más. Por eso también les ruego que, cuando ustedes quieran, por favor interrumpan y que, sobre todo, si se les ocurre alguna idea en este mundo que no se nos ha ocurrido -o que la hemos hecho mal- y nos pueden echar una mano, tanto hoy como cualquier día, por favor les rogaría nos llamaran.

Después de esta pequeña introducción, les quería decir una cosa que a los señores de Cybex seguramente les iba a enfadar. Para nosotros el problema de las evidencias electrónicas lo mejor que se nos ha ocurrido es intentar que no se produzcan, es decir, a nosotros nos está muy bien y nos parece genial que se llegue a juicio, que logremos defender que un email lo ha hecho menganito o que había provocado este imperfecto o este otro imperfecto. Pero está claro que el mal ya está hecho, por eso yo me centraría más en la última frase que ponía aquí "aunque resulte un poco paradójico para la empresa, resulta tan importante acceder a las evidencias electrónicas y poder hacer uso de las mismas como conseguir que éstas sean innecesarias".

Nuestra política en la Caixa ha sido básicamente preventiva y esto también es un tema que insistí cuando hablé con Cybex. Cuidado. También la experiencia de un banco a lo mejor no es muy aplicable a otras empresas. Nosotros nos manejamos con un material que es conocido de todos ustedes, que es el dinero y que seguramente obliga a unos controles y a unos sistemas de seguridad que a lo mejor no son extensibles a otro tipo

de empresas. Pero yo he intentado dirigir la ponencia escogiendo aquellos elementos de la política que hemos llevado nosotros que pudieran ser aplicables al máximo de sectores posibles.

Lo primero que nosotros tenemos muy claro es que, cada vez más, el impacto de las nuevas tecnologías en las organizaciones es evidente, no sólo en los bancos, que empezaron hace muchos años con sistemas electrónicos de control de datos, etc, sino que hoy hemos pasado, al menos desde nuestro punto de vista, de entender los soportes electrónicos como una herramienta de trabajo a formar parte de las estrategias de las empresas. ¿Por qué? Pues porque hoy se gestionan y se cuestionan miles de datos de clientes, de proveedores, de empleados, etc. Ya no es sólo el tema de que antes el ordenador ayudaba, en vez de tener fichas en papel; ahora el tema es más complejo. El propio negocio se canaliza a través de las nuevas tecnologías. Hoy no hay ninguna empresa con cierto volumen que no tenga una página web y que no esté interactuando con los clientes a través de su página, por tanto ya no es un mero soporte de datos; el tema es que el negocio se está vehiculando a través de las nuevas tecnologías. Hay un alto nivel de comunicaciones, nos estamos cruzando emails con todo el mundo y dejando rastro de ello y tenemos un volumen creciente de soporte informático aunque luego ya veremos que estoy hay que matizarlo.

También en el mundo laboral hay nuevas formas de trabajar: se trabaja con email, Internet, telefonía móvil, etc. y el acceso de empleados, clientes y proveedores a estos sitios donde tenemos depositados los datos es cada vez es mayor. Luego -permítanme que haga un salto en el tiempo- desarrollaré un punto que es muy importante que son las subcontratas, es decir, cuando estamos hablando de una empresa, no podemos perder de vista que ya no sólo son los empleados de una empresa los que están entrando, accediendo, interactuando. Entonces es una tontería dotarnos de una serie de medidas preventivas para evitar que ocurran una serie de cosas si no somos conscientes de que otras personas que no son de nuestra organización también van a tener que aplicarlas en cierta manera. Por otro lado, también es evidente que hay un entorno sociolaboral, hay una sensibilidad social y sindical más alta hacia este tema. Quizá nosotros hemos sido muy sensibles hacia esta cuestión cuando algún cliente se queja y dice “mire, yo creo que alguien ha

mirado unos datos que no tenía que mirar", pues esto es una sensibilidad que hace unos años no existía. Y yo creo que todos ustedes en sus ámbitos respectivos también se están encontrando con este tipo de problemas.

Esta responsabilidad conduce a que el problema de la utilización de las herramientas informáticas no sólo sea un problema ni de Recursos Humanos, ni de personal, ni de auditoría ni de los informáticos. Al final, estamos hablando de un problema de responsabilidad corporativa y (esto huelga decirlo) ante nuestros clientes, ante los proveedores, tenemos un problema de imagen si tenemos cualquier pleito de estas características. Trata directamente todo el tema de buenas prácticas que ustedes saben que está muy de moda, pero también quiero llamar la atención de que es un tema también que inquieta a las propias plantillas de las organizaciones. Los empleados también cada vez son más sensibles al derecho a la intimidad y no quieren que en sus datos se sepa que menganito tiene una categoría profesional o cobra tanto o cobra lo otro, que se sepa en el seno de la organización. Por lo mismo, ya no les cuento (lo he puesto aquí muy *light*) situaciones de riesgo, pero de palabra sí que se lo puedo decir. No les explico lo que puede haber detrás de una mala utilización de herramientas electrónicas, por ejemplo, en casos de acoso sexual o de *mobbing*, Entonces también tenemos un cliente interno que es sensible al uso de las nuevas tecnologías, y luego, por supuesto, a las autoridades, que creo que hay alguna presente por aquí. Este paso lo voy a saltar.

Yo les voy a explicar con qué filosofía afrontamos las medidas preventivas en nuestra casa y después voy a intentar detallarles en la medida que sea posible y que sea claro en qué han consistido estas medidas que hemos tomado nosotros en La Caixa. Lo primero, nosotros quisimos diferenciar entre el mal uso, el abuso y el uso fraudulento. Los tres constituyen, desde nuestro punto de vista, un uso incorrecto pero creemos que, de cara a tomar una serie de medidas preventivas primero, operativas después y disciplinarias en último término, no podemos juzgarlas de la misma manera. Es decir, el mal uso en el sentido de que, entendido como un error (se ha entrado en una página web por error o se ha enviado un email que tenía virus por error o por una instrucción mal dada o mal entendida), imagínense que damos una instrucción para manipular el nuevo PC que estamos instalando en la oficina, y como las instrucciones están mal, alguien rompe el disco duro. Esto es una instrucción mal dada, es un mal uso de la

herramienta, pero no puede tener ni el mismo trato ni la misma prevención que los otros dos tipos de uso incorrecto. No obstante, hay que llamar la atención de que el mal uso, aunque sea con toda la buena intención y con cariño, o por puro error, puede llegar a producir los mismos efectos que el uso fraudulento; es decir, una cesión de datos hecha sin querer, provoca a las organizaciones el mismo daño que si hubiera sido queriendo. Esto ustedes al cliente no se lo pueden explicar: “mira, te hemos dado un fichero pero es que se me ha caído del bolso, lo siento, esto ha salido y ha provocado… etc etc.”

El abuso, por su parte, tiene un componente que, yo diría, no es tanto de herramienta electrónica, sino que indica una forma de trabajar o una forma de actuar, que se da en la evidencia electrónica, pero que se puede dar en todo. Es decir, un empleado puede hacer un abuso en facturar facturas que no corresponden o puede hacer un uso abusivo de las páginas web, se puede pasar tres horas mirando páginas Web que no son profesionales. Y aquí el problema no es tanto de evidencia electrónica, sino que es el tiempo que ha estado perdiendo viendo la página web. Evidentemente, lo que va a requerir más nuestra atención de cara a políticas preventivas es el uso fraudulento. Aquí ya estamos hablando de comportamientos dudosos, con trasgresión de los fines de la relación laboral o profesional. Entonces, nosotros hemos basado toda nuestra política preventiva en lo que hemos llamado principios preventivos, que a algunos de ustedes les van a parecer evidentes. Seguro que muchos han salido durante el día de hoy, pero nosotros, de todo lo que nos han aconsejado los abogados, escogimos éstos. Nos hemos dejado adrede algunos que no nos hemos atrevido a adoptar en nuestra organización y hemos puesto otros de nuestra propia cosecha.

El primer principio preventivo es que los medios y herramientas son propiedad de la empresa y están para usos profesionales, que creo que ya se ha debatido. El segundo, que tiene más puntualización, es que son para utilizarse para la consecución de objetivos empresariales, es decir, no sólo que son propiedad de la empresa y están para trabajar, sino para trabajar con los objetivos que te marca la empresa. Un señor se puede dedicar a utilizar un email para enviar un montón de emails de contenido profesional a un montón de trabajadores de la empresa, pero que no vienen a cuento con lo que la empresa espera de él. No se pueden conectar ni periféricos ni software

sin permiso porque puedes hacer un gran daño a la organización, y esto incluye portátiles y agendas personales.

El segundo principio preventivo, y esto es todavía una parte muy introductoria, es la responsabilidad y el respeto a la legalidad. Es decir, "una cosa es que usted haga un mal uso o un uso incorrecto, pero si además ese uso incorrecto, usted lo hace con un contenido ofensivo que atenta contra la dignidad humana o los derechos fundamentales (especialmente el de la intimidad), estamos ante un problema todavía más agravado. Antes he comentado una posible utilización del email como herramienta de acoso sexual: un señor o una señora se dedica a hacer un acoso a un compañero, una compañera, un cliente o un proveedor. Aquí no estamos hablando sólo de empleados; está claro que hay un mal uso por los dos primeros puntos, se ha utilizado un medio para una cosa que no es profesional y no tiene nada que ver con los fines de la empresa. Pero es que, además, se ha incurrido en un atentado contra los derechos fundamentales. Esto añade un plus de gravedad que tiene que hacer que las herramientas que pongamos para arreglarlo sean más potentes, por el mismo respeto a la Ley de Protección de Datos, por respeto a la Ley de Propiedad Intelectual e Industrial, accesos y contraseñas, etc.

Este tercer punto, yo diría que es el más importante para nosotros y el que nos dio más qué pensar sobre el valor estratégico y no disciplinario. Todas las medidas estratégicas que hemos implantado en la casa para evitar el mal uso de las herramientas informáticas, como les he dicho, hemos tenido la intención de poner mucho énfasis en que no sea un problema estrictamente de Recursos Humanos, o estrictamente de seguridad informática. Esto es un problema corporativo, por lo tanto forma parte de la estrategia de la empresa el ir implementando esta cultura, a todos los niveles y con varias finalidades, no sólo para prevenir los malos comportamientos y el mal uso de las herramientas informáticas. También aporta como ventaja que ayuda a mejorar el buen uso de los medios, mejora nuestra calidad de servicio hacia los clientes y optimiza también la eficiencia de recursos, lo cual forma parte de las estrategias de una empresa. Respecto al uso no profesional, cuando ustedes consultan con los abogados, los abogados suelen ser muy rígidos en el sentido de decir "oiga, mire, el punto primero, éste si que lo adoptamos de los abogados". Las herramientas están para trabajar y para el tema profesional nosotros dijimos que sí,

que todo eso está muy bien pero lo que no puedo hacer es dedicarme a perseguir policialmente a todo el mundo que haga una llamada a un teléfono que no sea profesional o perseguir a todo el mundo que de repente entre en una página web de google o a todo el mundo que entre mañana para hacerse un viaje por Internet. Primero llegaríamos a un estado policía; segundo llegaríamos a un estado demencial; y tercero, no tenemos tiempo ni recursos para hacer todo esto.

¿Qué se nos ocurrió? Que todas nuestras medidas preventivas, que ahora más adelante pasaré a detallarles, fueran no rígidas. Es decir, primero limitar el uso no profesional (el uso personal de las herramientas informáticas o electrónicas) pero no prohibirlo, sino dotarnos de unas herramientas para evitar el uso y el abuso de los accesos individuales o privados. No limitarlos de forma taxativa. ¿Por qué? Pues porque en el fondo es irreal. Para nosotros hubo un ejemplo que fue el del uso del teléfono: el uso del teléfono de las empresas está claro que es una herramienta, está claro que se tiene que usar para trabajar, pero a nadie le cabe en su sentido común que un señor o una señora no llamen a medio día diciendo “oye, no voy a llegar a comer a casa”.

También tuvimos muy claro regular separadamente el uso sindical. Aquí supongo que ya se ha hablado esta mañana, pero el uso sindical de las herramientas está un poco entre dos aguas, entre profesional y privado. Es decir, un señor que está afiliado a un sindicato tiene derecho a usar las herramientas para dirigirse o no a sus sindicatos. Éstos están en el seno de la empresa, pero no deja de ser un tema particular y estaría un poco entre dos aguas. Entonces nosotros lo que hicimos fue tratarlo separadamente.

En cualquier caso lo que sí quisimos dejar muy claro es que el uso particular de las herramientas no debe afectar en ningún caso al desarrollo de su trabajo. Es el caso que os contaba antes sobre el señor que se tira tres horas cada día mirando Internet- salvo que lo necesite por su trabajo - a nosotros nos da igual que usted entre diez minutos a edreams a buscarse un viaje fantástico a las Malucas, pero lo que no vamos a tolerar de ninguna manera es que desde nuestra organización, desde nuestros medios, usted acceda por ejemplo a una página que distribuye pornografía infantil, es

decir, que nosotros hayamos abierto un poquito la puerta al uso personal, no significa que usted esté autorizado a hacer todo esto.

Y, por último, hemos intentado avanzar como principio preventivo el de la duplicidad de medios. Hoy se ha hablado en este foro del email personal, del teléfono personal y profesional. Nosotros seguimos avanzando en esta línea. Por ejemplo, este año hemos dotado a todos nuestros empleados, con ocasión de nuestro centenario, de un año de línea ADSL gratuita. Va un poco ahondando en esta línea: "usted podía entrar tres minutos en una web que no sea profesional, pero es que, además, le facilito un ADSL en su casa, con lo cual, por favor, si tiene que estar tres horas, va a su casa y la mira."

Otro principio preventivo para nosotros es el deber de aviso, es decir, entendemos que tanto proveedores, -vuelvo a decir que es importante- clientes, como proveedores y todas las personas que interactúan con nuestra organización tienen que ayudarnos a prevenir. De nada sirve que ustedes hagan unas medidas preventivas fantásticas si los destinatarios de estas medidas no les ayudan a detectar cuándo fallan o cuándo realmente se ha producido una vulneración de las mismas. En este sentido, si hay virus, perdidas de equipos, etcétera, etcétera, tienen el deber de avisar nuestros colaboradores.

Otro principio importante que deriva del primero es el de la auditabilidad. Nosotros entendemos que si los medios son de la empresa, son auditables; eso sí, es muy importante que no se queden ustedes en decir que hay un principio de ser auditables; tienen que decir cómo se hace y que hay garantías, ya que el respeto a las personas, lógicamente, exige hacerlo con una serie de protocolos. Para nosotros, el símil más importante fue el de la taquilla que está previsto en el estatuto de los trabajadores: históricamente, como no había ni ordenadores ni teléfonos móviles ni nada, todos los trabajadores tenían una taquilla, un armario donde podían guardar sus cosas. Para nosotros las herramientas electrónicas vendrían a ser como el cajón que cada uno tenemos en nuestras mesas.

Por último, como principio preventivo también les aconsejamos que su política preventiva no se centre sólo en la política de la empresa, sino que tenga lugar también

cuando un proveedor o un empleado, o un cliente, deja de tener relación con nosotros porque seguimos estando en riesgo. Es muy importante dejar cerrado qué ocurre en ese momento -la propiedad de los medios es nuestra- y qué procede al acceso y destrucción de archivos privados, y limitar el acceso a los medios profesionales.

Y los dos últimos principios preventivos. La adecuación permanente: evidentemente ustedes no se pueden relajar, no se pueden dormir diciendo "ya hemos hecho una política preventiva fantástica y ya tenemos todo hecho porque la tecnología evoluciona". La Ley Orgánica de Protección de Datos evoluciona apretando un poquito más, los tribunales también evolucionan también apretando, y es muy importante que todos nuestros colaboradores, clientes, empleados sean conscientes de los cambios que estamos haciendo. Porque si ustedes no lo comunican, no sirve de nada tenerlos implementados. Y, por último, es importante tener un canal permanente para dudas y consultas en abierto para todos los que colaboran con nosotros por todo lo que les he dicho antes: porque es muy importante crear un canal de ida y vuelta.

Ahora ya vamos a entrar completamente en las medidas preventivas que nosotros hemos implementado en La Caixa. Esta mañana les han hablado los señores de Cuatrecases de la importancia de tener un código telemático. Supongo que les han dicho que la ventaja que te aporta es el "ya te lo avisé" o cuando tú vas a un juicio el decir "como yo ya te lo he avisado". Nosotros, aparte de este efecto -que no voy a ocultar que lógicamente fue uno de los primeros que quisimos que tuviera- que plasmara un poco los principios que les voy a decir, que no se quedara sólo en una prueba para conseguir la culpabilidad o determinar un determinado comportamiento de dos personas. Nuestro código intentamos que fuera sencillo, claro y con vocación de permanencia; segundo, que fuera universal, para todos los empleados, que fuera temporal, que sirviese para todas las tecnologías. Si nosotros hubiéramos hecho un código que detalla mucho cómo se utiliza Internet o cómo se utiliza el teléfono móvil, te encuentras con que a los dos días ya no existe Internet y que los teléfonos móviles ahora son PDA y hacen hasta la comida.

Es muy importante para nosotros que tuviera una vigencia permanente, es decir, nosotros no podemos marear a nuestros colaboradores ni a nuestros clientes ni a nuestros proveedores con un código que cambia cada diez días y tenemos que

conseguir que lo vean fácil y que llegue de una forma accesible a todos ellos. Por eso, lo tenemos puesto en la primera página de Intranet, aunque creo que deberíamos ponerlo un poco más evidente. Y lo que sí hacemos es entregarlo a todos los empleados que trabajan con nosotros y avisamos siempre de futuras versiones y actualizaciones. Lo que intentamos, además, (porque si no podemos crear una empanada importante) es que sea coherente con otros códigos que existen en la empresa: el código de ética o el de buenas prácticas. No pueden decir ustedes dos cosas distintas en códigos que se peguen de bofetadas porque entonces, pese a que un jurista les haya ayudado a hacer un código precioso, lo que van a tener es una plantilla o unos colaboradores totalmente confundidos. Nosotros lo que hicimos, (lógicamente, no somos especialistas en códigos) fue pedir la ayuda de abogados externos. Sí les recomiendo que tengan implicados a todos los niveles de la organización, que se lo apruebe su comité de dirección, que lleven muy bien la política de comunicación a la plantilla y a los proveedores. En nuestra experiencia no fue excesivamente polémico. En cuanto lo implementamos, la gente lo entendió de forma bastante natural, bien es cierto que ya teníamos implementado un código de ética anterior. Quizá tuvo más impacto en los servicios centrales, que en las empresas son, normalmente, los más tecnificados, con utilización más masiva de nuevas tecnologías y es lógico que rascara más. También al no tener la presión del público, hay una tentación más fuerte de hacer un uso fraudulento de las mismas y tienes más tiempo para mirar webs. Yo estoy en servicios centrales y lo digo por mí mismo.

La reacción de la representación laboral no fue muy buena, pero no tanto por el contenido, -esto sí que me gustaría remarcarlo- sino porque no se había hecho con ellos. No fue posible llegar a un acuerdo con ellos, pese a que lo intentamos… pero el tema sindical lo dejaré muy para el final.

Nuestro código lo denunció la representación laboral frente a la inspección de trabajo, pero no ante los tribunales. Hizo una campaña de prensa, pero hasta ahora no hemos tenido ninguna sanción ni ninguna reconversión por el código que nosotros hemos implementado y que llevamos dos años con él en marcha. Hemos dejado la puerta abierta a negociar el uso sindical y, de momento, el único código que hemos encontrado en la Administración Pública es uno que publicó el año pasado la

administración de justicia y que iba bastante de acuerdo con los principios que les he explicado antes. Si alguien tiene interés, se lo podemos facilitar.

Muy rápido también porque el tiempo se acaba. Junto con el código, nosotros hemos publicado también un anexo de seguridad, que éste sí es variable. Son instrucciones operativas y cambia cada vez que nosotros cambiamos un circuito, cada vez que cambiamos el sistema de password, cada vez que cambiamos las máquinas. Esto tiene la gran ventaja de que el empleado colaborador, los principios los tiene siempre en un sitio y no le cambian; pero, en cambio, lo que tiene que aplicar cada día sí que lo tiene en otro documento que, a su vez, tiene que ser accesible, etc. Volvemos otra vez a la misma cadena: el anexo de seguridad no puede ser contrario a las políticas que contiene el código.

Aquí no hay problema en que ustedes establezcan -es nuestro consejo- distintos anexos para distintos departamentos o divisiones de la organización porque podemos entender que hay empresas que tienen muchas líneas de negocio y, a lo mejor, cada una necesita de una herramienta específica. Pueden hacer tantos como quieran.

Respecto a los equipos informáticos, en ese anexo de seguridad hemos instaurado las siguientes medidas que, seguramente, la mayoría ya las tienen ustedes. Pero bueno, si algunas son aprovechables, tome nota, y si se les ocurren otras, me las dicen, por favor. La primera: nosotros tenemos el bloqueo automático del teclado y de la pantalla en el caso de ausencia, ¿Qué nos ocurrió? Teníamos un sistema de passwords muy rígidos y lo seguimos teniendo, por supuesto. Pero ustedes piensen en una oficina bancaria. Sería una barbaridad que un terminal, una ventanilla, una mesa de atención al público sólo pueda hacerla funcionar un empleado. Entonces, ¿qué tenemos?. Primero un sistema de passwords que ahora les explicaré cómo funciona; y segundo, el hecho de que nadie pueda acceder a tu ordenador mientras que tú no estás porque entonces podríamos tener un conflicto sobre quién ha utilizado la máquina.

La segunda: hay obligación de cerrar el PC y, como no puede ser de otra manera y nosotros tenemos el principio de no cesión de las contraseñas, a nosotros todos los juristas nos recomiendan que la contraseña tiene que ser privada; en el momento en

que usted dé la contraseña, estamos perdiendo herramientas para poder evidenciar que alguien ha hecho un mal uso. Pero eso, en la realidad, es muy difícil. Yo puedo entender que si yo me voy un momento, mi PC se tiene que autobloquear para que nadie me lo utilice mal, pero si yo me pongo enfermo mañana y alguien tiene que acceder a mis emails para poder contestar, a lo mejor yo tengo que ceder el password. Lo que nosotros hemos obligado en el código es a que esto sea con autorización expresa del titular, con lo cual ante un problema de evidencias electrónicas puedes ir tirando del hilo, lo que no sirve es pasarse el password de palabra; se hace con un papel o un email: "Menganito o menganita te autoriza para que entres en mi herramienta". Y esto sirve para teléfonos, para PCs, para PDAs, para todo lo que ustedes quieran. Por último, tener niveles de autorización diferentes en la empresa, pero esto supongo que ya se da por hecho.

Con respecto a Internet, nosotros no tenemos la Internet abierta a todos los empleados, sino que hemos hecho un filtrado de páginas, es decir, a determinadas páginas con determinados contenidos no se puede acceder. Hemos hecho un sistema que cuando estás navegando, si necesitas por tu trabajo acceder a una página web que no es de uso frecuente o a lo mejor es de un contenido que a lo mejor no tenga mucha vinculación con la empresa pero que por tu trabajo específico sí te puede ocurrir, lo que tienes que hacer es lo que la máquina te dice: "Está intentando entrar usted en una página web que no está autorizada. Si usted lo necesita, dígamelo, que le autorizo".

Fíjense que todo el rato estamos hablando de medidas preventivas porque son medidas preventivas para evitar que se hagan cosas. Pero no queremos caer tampoco en la rigidez. Se puede dar el absurdo de que, a lo mejor, alguien -por su trabajo- tiene que entrar en una página de contenido pornográfico. Si hay una denuncia de que alguien esta enviando fotos pornográficas desde una página web, pues el investigador quizá tiene que entrar para comprobarlo.

Y, por último, también hemos tenido una política muy importante con la salvaguarda de dominios. Vigilamos mucho que no se utilice el nombre de Caixa fuera de Caixa. En la misma línea, recomendamos tener sistemas de vigilancia corporativa, rastreos de la web para saber dónde aparece el nombre de Caixa, La Caixa o Grupo La Caixa.

También hemos puesto como herramienta preventiva el uso del correo electrónico estrictamente profesional y propiedad de la empresa, por lo tanto es auditable y sujeto al código. Y ahora estamos trabajando en la firma electrónica. Nosotros también hicimos caso a los abogados (ha salido ahora el tener un doble email), hemos implementado un doble email personal a nuestra plantilla y a cada trabajador que se incorpora nuevo en La Caixa se le da automáticamente la posibilidad de tener un correo personal. Lo único, y esto si que se lo cuento de forma muy breve, porque fue interesante en nuestra experiencia, lo que quisimos fue ser coherentes con lo que estábamos diciendo: "oiga si nosotros dotamos de un email personal a nuestros empleados, no queremos saber nada de este email, nosotros lo contratamos con un servidor externo, nosotros no tenemos posibilidad de saber quién está detrás de cada dirección; si se hace un mal uso de ese correo, lo que queremos es que las autoridades, igual que si se hace un mal uso de cualquier otra cosa, nos exijan saber quién es ese señor que está detrás del email. Hay una forma de saberlo. Lo que hicimos es un sistema de doble llave. Hicimos un código personal, que sí lo conoce la empresa, pero el usuario y el password sólo lo conoce el proveedor del email. Lo que hacemos es que el empleado recibe una clave secreta (que solo él conoce) y con eso él activa su email personal, pero eso no pasa por los ordenadores de Caixa. Lo que sí le decimos al trabajador es que el uso del email personal esta sujeto, lógicamente, a las leyes y al buen uso. Esto, evidentemente, tiene la gran ventaja de que nadie puede alegar la excusa para usar el email profesional. Hay una pequeña duda -también lo digo- y es que no todo es de color de rosa. Una pequeña duda que ha flotado en todo el tema del email personal, que es qué ocurre con el correo entrante. Yo utilizo el correo profesional para mi trabajo pero resulta que me envían (pues ahí lo exigimos) un email; lo que tienes que decir a la persona que te lo envía es que, por favor, te lo envíe al email personal.

Por último, estamos trabajando en medidas sobre temas de acceso a redes, a redes de tipo wifi, inalámbricas, etc, Estamos trabajando en el tema de la extranet y aquí les aconsejamos trabajar en temas de barridos y control de acceso: saber si alguien está intentando acceder a nuestras redes inalámbricas y ver si alrededor nuestro también hay redes inalámbricas que podrían interactuar con nuestros sistemas.

En el tema de portátiles y agendas estamos trabajando en materia de configuraciones específicas para estos medios, passwords, sistemas de passwords excepcionales (más potentes que los de las máquinas fijas), y, sobre todo –esto sí que lo recomiendo- el b*ackup* de seguridad debe estar en la empresa, porque, si no, ustedes se pueden encontrar con un profesional que se vaya con su agenda o que la pierda y que no haya soporte en la empresa, al menos, para saber qué es lo que se ha perdido.

En relación a la parte de la representación sindical, aquí simplemente dos apuntes muy rápidos. Nuestro consejo es que, en la medida que puedan lograr que ellos se impliquen y que participen tanto del código como de las medidas preventivas, no tiene ningún desperdicio y les recomiendo intentar; otra cosa es que luego se llegue a un acuerdo o no. Nosotros partimos de la filosofía de que cuatro ojos ven más que dos; creemos que es mejor unas políticas preventivas con participación sindical que sin ella. Hace poco hemos publicado una normativa interna sobre confidencialidad en la que ellos han participado. Su implicación, creo, que es importante de cara a crear cultura. Como les he dicho, nuestras políticas o nuestras herramientas preventivas no son tanto para perseguir comportamientos, sino para crear cultura (para lo otro también, no quiero que se equivoquen).

Por último, hemos dejado la negociación de uso sindical: lo que es el email entre sindicatos, relaciones sindicales, etc. Aquí solo un tema que es importante que también les sugiero, nosotros les hemos propuesto la creación de un tablón de anuncios virtual para evitar que ellos utilicen el papel. La propuesta la estamos haciendo a través de nuestro comité medioambiental por un tema ecológico: “señores sindicatos, ustedes distribuyen miles de hojas de papel cada semana poniéndonos a caldo, pero aparte de que nos pongan a caldo, sería interesante trabajar juntos a ver si podemos hacer un tablón virtual, con lo cual ustedes quedan mucho mejor ante el tema ecológico y nosotros nos ahorramos también un montón de papel además colaboramos todos con el medio ambiente”. Para los sindicatos esto aporta, además, una gran ventaja, que es la inmediatez de las noticias.

El uso de Internet, el tener un correo, el tener un correo personal, etc… todas estas medidas no tienen mucho sentido si no tienen en cuenta que hoy las empresas cada vez interactúan más con el mundo exterior. ¿Aquí qué ocurre? Nos encontramos con

proveedores que acceden a nuestros sistemas, nos encontramos con trabajadores como los autónomos que están trabajando con *teleworking*, nos encontramos con que las empresas cada vez van más allá y están creando lo que se llama los portales del empleado (portales donde la familia del empleado, los amigos del empleado pueden acceder libremente) y todo esto lleva a que las medidas que ustedes diseñen sería muy conveniente que tuvieran en cuenta esta extensión fuera de la empresa. Concretamente, lo que nosotros aconsejamos a los proveedores es que en el momento de que se contacta con ellos, nosotros les hacemos llegar una copia de nuestro código de buen uso y de buenas prácticas. Especialmente, en el tema de contratas el tema se vuelve un poco más complicado. Como ustedes saben, ha salido una nueva legislación el año pasado sobre subcontratistas que -por decirlo llanamente- carga toda la responsabilidad en determinadas materias como protección de datos, prevención de riesgos laborales, de nuestros subcontratistas a la empresa principal. Aquí nosotros lo que estamos adoptando son medidas de autoprotección para la empresa y en la línea de que, siempre que haya trabajadores en la empresa subcontratada que acceden a nuestros sistemas informáticos o a nuestras herramientas informáticas, lo que queremos es que nos detallen qué personas son y qué *password* tienen asignados en todo momento. Porque, además, aquí hay un riesgo añadido, que es el riesgo de cesión ilegal de trabajadores: si ustedes están trabajando con un contratista y ese contratista acabó su contrata pero resulta que sus trabajadores siguen teniendo los password y siguen entrando en su sistema o en sus teléfonos móviles, nadie les exonerará a ustedes de la responsabilidad de lo que esté ocurriendo con esos equipos; y esos trabajadores, a su vez, podrán demandarles a ustedes porque podrán demostrar una cierta continuidad con la labor que están haciendo con ustedes, es decir, pueden demandar ser trabajadores de su empresa, vía evidencia electrónica.