

La Seguridad de la Información en los Recursos Humanos

Daniel Barriuso, Information Security Manager

http://www.rrhmagazine.com/articulos.asp?num_art=251

http://www.rrhmagazine.com/articulos.asp?num_art=254

¿Se dedica a la gestión de Recursos Humanos? ¿Ha pensado alguna vez en la seguridad de la información de su empresa? Si la respuesta es afirmativa a ambas preguntas, seguramente el presente artículo le va a resultar de interés. En cambio, si sólo es afirmativa la primera respuesta, probablemente el presente artículo no sólo le interesa, sino que le sorprenderá saber que usted juega un papel fundamental en la seguridad de la información corporativa.

¿Qué es seguridad de la información?

La seguridad de la información consiste en proteger uno de los principales activos de cualquier empresa: la información.

La seguridad de la información es requisito previo para la existencia a largo plazo de cualquier negocio o entidad. La información es usada en cada uno de los ámbitos empresariales, los cuales dependen de su almacenamiento, procesado y presentación.

Los tres fundamentos básicos de la seguridad en la información son:

- Confidencialidad. La información debe ser accedida sólo por las personas autorizadas a recibirla.
- Integridad. La información debe ser correcta y completa.
- Disponibilidad. La información debe estar disponible siempre que sea necesario.

¿Qué tiene que ver la seguridad con los Recursos Humanos?

La gestión de la seguridad de la información, al igual que la mayoría de los ámbitos de la gestión empresarial, depende principalmente de las personas que componen la Organización. La información sólo tiene sentido cuando es utilizada por las personas y son estas, quienes en último término, deben gestionar adecuadamente este importante recurso de la empresa. Por tanto, no se puede proteger adecuadamente la información sin una correcta gestión de los Recursos Humanos.

¿No debe ser el departamento de Seguridad quien se encargue de estos temas?

Proteger los activos de información con los que cuenta una empresa es una tarea que no sólo debe implicar al Director de Seguridad, sino que debe ser compartida por toda la Organización. Cada área de Negocio juega su papel: el área de Marketing se centra en la protección de la imagen corporativa, el área Comercial está más relacionado con la protección de los datos de los clientes, IT se ocupa de la correcta protección de sus Sistemas de Información, etc. Pero sin duda, una de las áreas que más importancia tiene en la seguridad de la información es el departamento encargado de gestionar los Recursos Humanos.

Aspectos como la formación de los empleados, la captación y selección de nuevos miembros de la plantilla, la gestión de empleados que abandonan la Organización o la implementación de la normativa interna, son fundamentales en el tema que nos ocupa.

Todas las claves que se van a desarrollar en el presente artículo, se podrían resumir en una sola frase: conseguir que los criterios de seguridad estén presentes en la gestión de los Recursos Humanos. Un magnífico punto de partida podría ser que los responsables de Seguridad y Recursos Humanos se sienten juntos y compartan impresiones. Seguro que inmediatamente encontrarían preocupaciones comunes y puntos de colaboración. Entre tanto, podemos anticipar algunos aspectos fundamentales a tener en cuenta.

Reclutamiento y salida de empleados

Existen dos puntos fundamentales en el ciclo de vida de todo empleado en una Organización: El inicio de su actividad profesional y la finalización de la misma.

Reclutamiento

Cada nuevo empleado de la Organización es una apuesta de futuro. La empresa asigna una serie de tareas y responsabilidades al nuevo empleado, y le proporciona los medios materiales y la información necesaria para que pueda llevarlas a cabo. Debe existir un procedimiento de reclutamiento que tenga en cuenta los siguientes aspectos relativos a la seguridad:

Definición del puesto: Para cada nueva vacante se debe definir la criticidad del puesto a cubrir según su responsabilidad y la información que maneja. Cada empresa debe definir su criterio propio. Algunos puestos críticos pueden ser directivos, personal de seguridad, personal de contabilidad, etc.

Selección: En la selección de candidatos a puestos críticos se deben comprobar los antecedentes penales y las referencias profesionales.

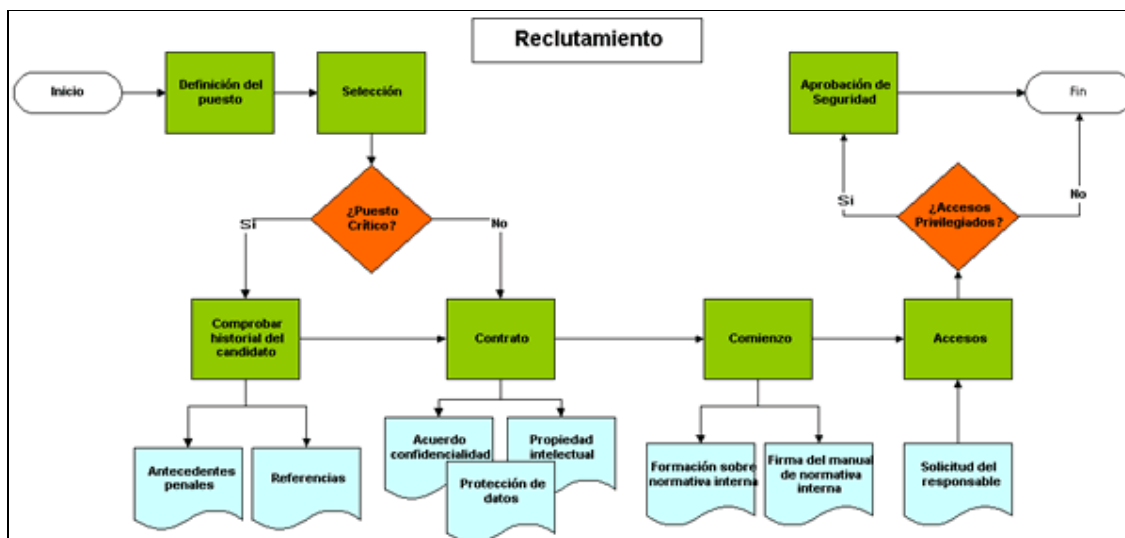
Contrato: El contrato laboral debe incluir los correspondientes acuerdos de confidencialidad, propiedad intelectual y protección de datos.

Comienzo: Durante los primeros días de trabajo, es recomendable que el empleado:

Asista a unas sesiones de formación donde se le introduzca en la normativa interna y de seguridad de la empresa. De este modo todo empleado conoce sus obligaciones de seguridad tales como la protección de sus claves de acceso, uso adecuado del email e internet, clasificación de la información, etc.

Reciba el manual de normativa interna y firme el compromiso de cumplimiento del mismo. Este trámite establece formalmente las normas internas y garantiza que el empleado conoce la normativa existente.

Accesos: Los accesos a la información y sistemas informáticos deben ser solicitados siempre por el responsable directo del empleado al departamento de IT o HelpDesk. Dichos accesos deben ser siempre justificables por la labor que se va a realizar, y en caso de ser privilegiados, el Departamento de Seguridad debe aprobar su concesión.



Salida de empleados

La salida de un empleado es un punto crítico de riesgo para la Organización. En casos de problemas laborales y despidos, un empleado modelo hasta la fecha, puede convertirse en una seria amenaza. La historia reciente está plagada de casos de sabotaje o sustracción de información por parte de empleados “disgustados”.

Lamentablemente, es bastante común que no se gestionen coordinadamente las bajas de los empleados. En muchas ocasiones, Recursos Humanos se encarga de realizar los trámites legales de la baja, mientras que el responsable del empleado es quien trata directamente con él y planifica el traspaso de su trabajo. Por otro lado, IT se ocupa de dar de baja sus accesos (en el momento en que perciben su ausencia). Este escenario acaba degenerando en problemas tales como que los accesos de los ex empleados siguen vigentes durante meses, o que tras la marcha del empleado no es posible recuperar cierta información vital que poseía. Para evitar todo esto, debe existir un procedimiento de bajas que tenga en cuenta los siguientes aspectos de seguridad:

Clasificación de las bajas: El responsable del empleado junto con Recursos Humanos deben clasificar la baja según las circunstancias que la rodean. Un ejemplo de posibles categorías sería:

Baja normal, si se produce en circunstancias normales y sin conflictos.

Baja cautelar, si se produce en circunstancias normales, pero con la que hay que tener una vigilancia especial en los accesos y documentación que obra en poder del empleado: personal con acceso a información sensible, administradores de sistemas, etc.

Baja crítica si se produce en circunstancias especiales: despidos, problemas con el empleado, etc.

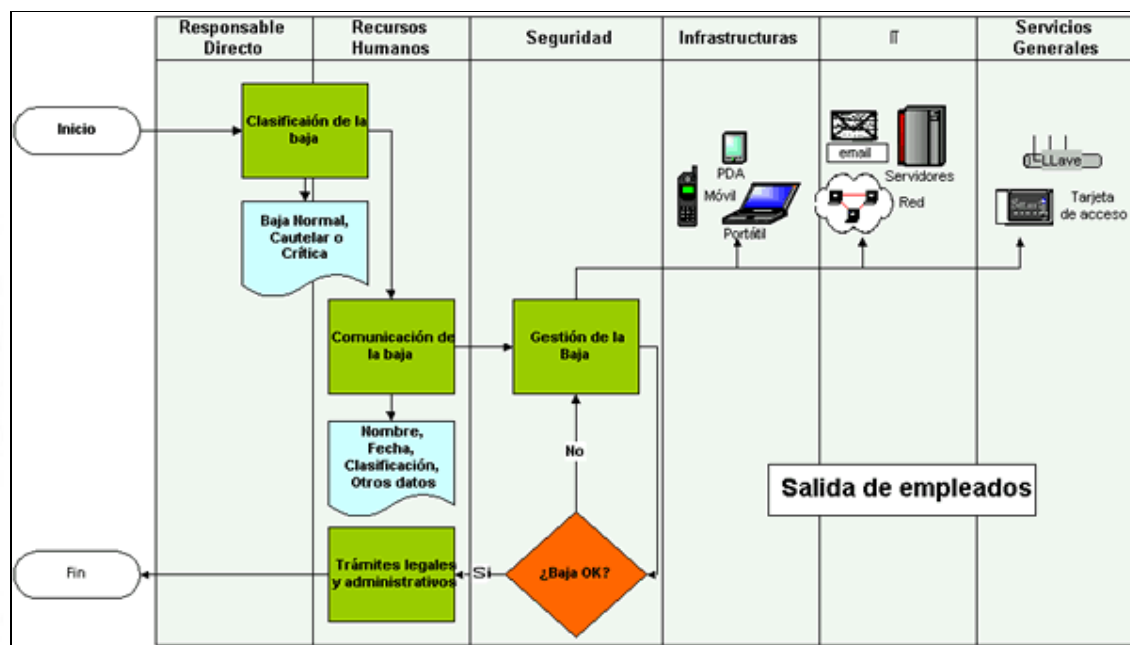
Comunicación de las bajas: Tan pronto como se conozca la baja de un empleado, Recursos Humanos debe comunicar las bajas de personal a Seguridad. En la comunicación se debe indicar el nombre, la fecha efectiva de la baja, su clasificación y cualquier medida o control especial que sea necesario realizar.

Gestión de las bajas: Seguridad debe coordinar que la baja se produzca en el plazo adecuado dependiendo de la clasificación (por ejemplo, una baja crítica debe realizarse de forma inmediata). Debe efectuarse la retirada de:

- accesos físicos (llaves, cajas fuertes, llaves electrónicas)
- accesos lógicos (email, acceso a la red y servidores, etc)
- material de la empresa (portátil, móvil, etc)

La gestión de la baja también puede incluir otras medidas dependiendo de la clasificación de la misma:

- realización de copias de seguridad de la información sensible
- supervisión de los accesos hasta el día de la baja
- cancelación preventiva de los accesos más críticos



Es fundamental que todos los empleados asuman su responsabilidad en el cumplimiento de la normativa interna de seguridad en la empresa. No hay política de seguridad que funcione por sí sola: es necesario que los empleados la conozcan, entiendan y respeten.

Normativa interna y *compliance*

En este aspecto, Recursos Humanos debe participar activamente en el soporte al cumplimiento normativo:

Definición: las normas de seguridad deben estar alineadas con la Estrategia Corporativa y de Recursos Humanos.

Las normas de seguridad deben facilitar la Gestión de Recursos Humanos (temas como la regulación del uso del e-mail o Internet pueden influir directamente en el rendimiento y satisfacción de los empleados).

Además, las normas deben ser compatibles con la legislación laboral aplicable. No es posible imponer obligaciones o sanciones que se opongan a

libertades y derechos del empleado. En este sentido, tanto Recursos Humanos como el área Legal deben validar la normativa de seguridad.

Algunos puntos básicos que se deben cubrir con la normativa interna son:

- Clasificación de información
- Intercambio, almacenamiento y destrucción de la información
- Protección de datos personales
- Uso de claves
- Uso del e-mail
- Uso de equipos
- Control de virus

Comunicación: la normativa de seguridad debe ser publicada oficialmente y ser accesible por todos los empleados. Es recomendable asegurarse de que todos los empleados conocen la normativa mediante sesiones informativas al incorporarse a la empresa, seminarios de refuerzo periódicos y la firma de un manual de cumplimiento en el que se detalle toda la normativa interna.

Responsabilidad: la responsabilidad de la seguridad de la información es de todos y cada uno de los empleados. Todos los empleados son responsables de salvaguardar la información que reciben, crean o controlan.

Cada empleado ha de cumplir las normas, pero la cadena de responsabilidad no acaba ahí. Cada superior directo es responsable de la supervisión del cumplimiento y de poner los medios organizativos necesarios para que todos sus empleados puedan cumplir con sus obligaciones. Asimismo los Directores de Área o Departamento deben asegurarse de que existan los medios materiales y organizativos necesarios, ya que son los máximos responsables del cumplimiento normativo por parte sus empleados.

Sanciones: las sanciones disciplinarias derivadas del incumplimiento de las normas de seguridad han de ser públicas y guardar una proporción razonable. La naturaleza de estas sanciones es principalmente coercitiva, pero no debe dudarse en aplicarlas cuando sea necesario.

Procedimientos de emergencia

En caso de emergencias o desastres, una correcta planificación puede marcar la frontera entre la desaparición y la supervivencia del negocio. Y lo que es más importante, puede salvar la integridad de los propios empleados.

Tras los sucesos acaecidos el 11 de Septiembre, se comprobó que muchas de las empresas que no habían previsto este tipo de situaciones en un plan de continuidad de negocio fueron abocadas a su desaparición. La coordinación en la evacuación de un edificio o la organización de las medidas de recuperación del negocio tras un desastre no son tareas que se puedan dejar a la improvisación. Un buen plan de continuidad de negocio ha de ser diseñado, comunicado y probado con antelación.

Acompañando a las medidas técnicas tales como la realización y externalización de *backups* con la información crítica, se han de definir una serie

de medidas organizativas destinadas a salvaguardar y proteger a los empleados y sus capacidades:

Plan de evacuación: cada edificio debe tener un plan de evacuación mediante el cual todos los empleados sepan qué deben hacer en caso de emergencia, se definan responsables de coordinar dichas situaciones y se establezca un punto de reunión seguro.

Para ser efectivos, los planes de evacuación se han de probar periódicamente y ser fácilmente accesibles. Publicar la información en la intranet o la distribución de tarjetas con el diagrama de evacuación y los teléfonos de emergencia son medidas muy útiles.

Funciones críticas: la identificación de las funciones críticas para reestablecer el negocio puede simplificar las tareas de recuperación ante desastres. Desde Recursos Humanos se debe fomentar la definición de las funciones críticas de cada área y las personas encargadas de su realización. De este modo, después de una contingencia se pueden centrar los esfuerzos en reestablecer lo antes posible aquellas funciones más importantes.

Asimismo, es una buena práctica designar a una persona de respaldo para cada función. Se debe evitar el riesgo de que sólo una persona sea capaz de realizar una función crítica o de que información vital esté sólo en poder de un empleado.

Lugar de respaldo: la previsión de un lugar de respaldo alejado de la zona del desastre, con puestos de trabajo preparados para su uso, permite que se retomen las actividades en un espacio de tiempo mucho más corto. Cada Organización debe elegir la estrategia de recuperación que más se ajuste a sus necesidades. Las posibilidades varían mucho en función del tiempo de respuesta buscado y el coste que se puede asumir, desde tener preparados puestos de trabajo alternativos para todos los empleados, hasta acordar con un tercero el alquiler de algunos puestos para el caso de una emergencia. Una solución razonable en términos de coste/beneficio es la siguiente:

Definir con cada departamento el número de puestos e infraestructura mínima necesaria.

Si se dispone de varios edificios en la Organización, definir en cada uno de ellos qué puestos podrían ser utilizados por otros empleados en caso de emergencia, de modo que el edificio dañado pueda alojar al personal mínimo necesario en otro lugar y el edificio anfitrión funcione con el mínimo definido.

Si no se dispone de varios edificios en la Organización, llegar a un acuerdo con un tercero que nos garantice el número de puestos necesarios en un lugar suficientemente alejado (existen empresas que ofrecen estos servicios).

La información interna del departamento de Recursos Humanos

Hasta ahora hemos analizado cómo desde Recursos Humanos se puede ayudar a proteger la información de la Organización, pero no debemos olvidar que el propio departamento de Recursos Humanos es uno de los que mayor información sensible maneja.

Información como el sueldo de los empleados, desempeño profesional o bajas laborales, pertenece al departamento de Recursos Humanos y es considerada confidencial en cualquier sector.

La necesidad de proteger los datos personales excede el mero interés empresarial. Desde hace más de una década la legislación española protege el honor y la intimidad de los datos personales y familiares. Primero mediante la derogada Ley Orgánica 5/1992 conocida como LORTAD, y más recientemente con la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, conocida como LOPD. La LOPD otorga una serie de derechos a las personas cuyos datos sean objeto de tratamiento, y establece las obligaciones de quienes efectúen dichos tratamientos.

Por la naturaleza intrínseca de los datos de Recursos Humanos las obligaciones establecidas en la LOPD deben ser consideradas con sumo rigor.

En primer lugar debemos tener en cuenta el tipo de datos que se manejan en el departamento. Según la ley existen tres niveles: nivel bajo (cualquier dato personal), medio (infracciones administrativas o penales, hacienda pública, servicios financieros) y alto (ideología, religión, creencias, origen racial, salud, o vida sexual). Cuanto mayor sea el nivel de los datos, mayores son las posibles sanciones (de hasta 600.000 € por dato) y las medidas de seguridad exigidas.

Como mínimo, en Recursos Humanos se manejan datos de nivel medio (datos financieros), pero es muy común que el nivel realmente sea el alto: información sobre bajas laborales o discapacidades otorgan al fichero de empleados el nivel alto y convierten al departamento de Recursos Humanos en el de mayor importancia en la protección de datos personales.

Sería muy complejo entrar a detallar las medidas de seguridad que deben estar presentes. El mejor consejo podría ser analizar la situación con el departamento de Seguridad o especialistas externos e implementar las medidas correspondientes. El área de Recursos Humanos debe ser proactivo en el cumplimiento de la ley y la protección de sus datos.

Por último, no conviene olvidar que, según el artículo 12 de la LOPD, aunque la gestión de nóminas o trámites legales esté subcontratada, la titularidad de los datos y responsabilidad final no puede ser delegada. Existe la obligación de asegurar que cualquier tercera parte protege la información adecuadamente.