

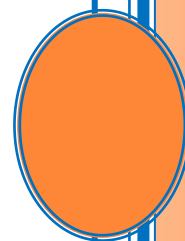
EMPLEADOS DE UNA COMPAÑÍA, PODRÍAN COMETER FRAUDES EN AMBIENTES SIN CONTROL, EL 85% DE LOS DELITOS INFORMÁTICOS SON REALIZADOS POR EMPLEADOS O EX EMPLEADOS !

SEGURIDAD DE LA INFORMACIÓN Y RRHH

Hace algunos años, la función de seguridad informática dependía de la Gerencia de Tecnologías de la Información, ya que la principal preocupación relacionada con la Información eran sus aspectos netamente técnicos, tales como los riesgos de virus, spam, phishing, violación de password, entre otros. Sin embargo, con el paso del tiempo, las Compañías se dieron cuenta que la **Información era un Activo crítico** y relevante para el desarrollo del negocio y que por lo tanto, había que protegerla. Es por esto, que la función pasó a llamarse "Seguridad de la Información", de tal forma que su gestión abarcara no solamente los aspectos técnicos, sino que también el cuidado de la información de toda la Compañía, independiente del medio en que se custodiara. Adicionalmente, comenzaron a aumentar los casos de **fraudes y/o violación de las políticas de seguridad** al interior de la empresa, las que incluso podían efectuar los propios empleados debido al mayor acceso a Información considerada confidencial o crítica. Es aquí, donde consideramos que el área de Recursos Humanos debiera involucrarse en el **Comité de Seguridad de la Información** y en los aspectos de seguridad que afecten directamente a los empleados, como por ejemplo: actualizando el **Reglamento Interno**, cláusulas especiales de seguridad y confidencialidad de la información en contratos de trabajo y anticipándose a la capacitación de usuarios para tener un plan de "evangelización" permanente y de largo plazo.

PARTICIPACIÓN EN EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Posteriormente, al crear un **Comité de Seguridad**, formado por el **Gerente General** y los **gerentes de áreas**, cuyo objetivo principal sea analizar y dirigir la gestión de seguridad de la información integralmente. Es, precisamente, en este comité, donde considero que se debería incorporar como un miembro activo al **Gerente o responsable de la gestión de recursos humanos**. Sin embargo, en



muchos casos se produce una resistencia de participar, debido a que no se sabe cuál es la relación de ésta área (RRHH) con la Seguridad de la Información.

RELACIÓN CONTRACTUAL CON EL EMPLEADO

En cuanto a la relación contractual con los empleados, se debe separar a los usuarios “normales”, de usuarios que manejan información crítica, y de desarrolladores, analistas y programadores; es decir los contratos de trabajo deberían incorporar cláusulas especiales, que hagan alusión a las leyes vigentes, tales como **Protección de Datos Personales (ley 19.628)**, actualmente esta ley está siendo discutida en el parlamento para perfeccionarla, **Delitos Informáticos (ley 19.223)**, en el caso de los desarrolladores rige la **ley 17.336 sobre Propiedad Intelectual**. Cabe señalar, que han existido casos en nuestro país, donde las empresas han despedido a empleados por incumplimiento de normas o delitos informáticos, pero posteriormente al iniciarse un proceso judicial, la sentencia ha favorecido al ex empleado, generalmente por la falta de argumentos o documentación formal de la empresa, sobre el tema.

Por otra parte, cuando un empleado renuncia o es despedido, es común que se pague la indemnización o lo que le corresponde legalmente, pero no se verifica qué elementos de hardware tiene asignado ese empleado. Sin embargo, esto tiene como consecuencia, entre otros, los siguientes problemas:

- a) Si el ex empleado tiene asignado un **Notebook o Laptop**. Este equipo y la Información del disco duro, se lo lleva hasta que alguien lo llame para pedírselo de vuelta a la empresa.
- b) Permanecen habilitadas las **cuentas de acceso** a los sistemas, después de la desvinculación por un tiempo prolongado.
- c) No se elimina su **cuenta de correo**. Acceso al correo electrónico en forma remota posterior a su desvinculación.

Adicionalmente, si una persona ha sido despedida por **robo de información**, violación de políticas de uso de Internet (Ej. pornografía u otro), es importante que la empresa tome resguardos previos, como ejemplo que el área de RRHH haya enviado el reglamento interno y las políticas de seguridad de la información, a la toma de conocimiento de la Dirección del trabajo, de tal forma que cuando el ex empleado acuda a dicho dirección, para acusar a la empresa de un despido arbitrario y declare no haber conocido las políticas, este organismo resuelva en base a los documentos previamente sancionados.

EMITIDO POR PALLAVICINI CONSULTORES, PARA MAYOR INFORMACIÓN VER www.pallavicini.cl