TESIS

# LA INFORMACIÓN

# El Activo Fundamental

Alumno: Lucas Dubini

Tutor: Ing. Pablo Guarna



**2005**

## CONTENIDO

**INTRODUCCIÓN** ..... 3
**LA INFORMACIÓN** ..... 8
Características de la información ..... 8
Metodología para el Desarrollo de Políticas y Procedimientos de Seguridad de Información ..... 8
¿Cómo deben elaborarse las políticas? ..... 10
La longitud del documento sobre las políticas ..... 12
Las Políticas de Seguridad ..... 13
**COMPONENTES DE UN SISTEMA INFORMÁTICO** ..... 15
**OBJETIVO DE LA SEGURIDAD INFORMATICA** ..... 20
**ÁREAS DE LA SEGURIDAD INFORMATICA** ..... 22
**RIESGOS DE UN SISTEMA INFORMATICO** ..... 23
**HERRAMIENTAS DE SEGURIDAD INFORMATICA** ..... 25
Control de acceso ..... 25
Virus y Antivirus ..... 25
Sistema de Backup ..... 26
Plan de Contingencia ..... 26
**REDES** ..... 28
¿Qué es una red? ..... 28
Objetivos de las redes ..... 28
Seguridad de Redes ..... 29
**CONCEPTO DE SEGURIDAD INFORMATICA EN INTERNET** ..... 31
Grado de seguridad informática en Internet ..... 31
Riesgo de Seguridad Informática en Internet ..... 32
**VIRUS** ..... 33
¿Que es un virus? ..... 33
Evolución histórica de los virus ..... 33
¿Que daños produce? ..... 34
¿Quién hace los virus? ..... 34
Definición de tipos de virus ..... 35
¿Qué se puede hacer? ..... 35
Importancia del problema ..... 36
Función de un antivirus ..... 37
Características de un buen antivirus ..... 37
**FIREWALLS** ..... 39
Beneficios de un firewall en Internet ..... 39
**FIRMA DIGITAL** ..... 41
Ventajas ofrecidas por la Firma Digital ..... 41
**ENCRIPTACIÓN** ..... 45
**HABEAS DATA** ..... 46
Caracteres generales del Hábeas Data en la ley 25.326 ..... 48
**CONCLUSIÓN** ..... 50
**BIBLIOGRAFÍA** ..... 54

## INTRODUCCIÓN

El poder de los grupos humanos a nivel mundial dependió, en un primer momento, de la cantidad de tierras que poseían, luego de la capacidad de producción agrícola-ganadera, más tarde de la capacidad industrial y tecnológica y actualmente de la información de que disponen, la cual (a diferencia de los mencionados factores de poder) es intangible.

En este sentido, se puede definir a la información como un activo que, al igual que el resto de los recursos importantes de la organización, tiene valor para la misma y por consiguiente debe ser debidamente protegido, situación que por estos días no ocurre en la mayoría de las compañías.

A lo largo del presente trabajo, se expondrán las principales consideraciones a tener en cuenta respecto del valor de la información y se detallará de la forma más clara posible, con qué herramientas contamos para asegurarnos que nuestra información está correctamente resguardada de terceros, e incluso, de nosotros mismos.

He tenido la oportunidad de trabajar para empresas de distintos ramos y de distinta magnitud, habiendo encontrado en ellas un factor común, que es la falta de conciencia del personal respecto de lo crucial que puede resultar la información que manejan. Esto en mayor medida, junto con la creciente relevancia que este tema viene adquiriendo en los últimos años a nivel mundial, es lo que motiva la elección de este tema. Por estos días gran parte de nuestra información es almacenada en computadoras, pero en la mayoría de los casos, los usuarios no están familiarizados con las consecuencias de un inapropiado o insuficiente uso de los recursos de seguridad con los que cuentan.

Pensemos en una jornada normal de trabajo en la que finalmente hemos concluido un reporte que nos ha mantenido ocupados por varios días. Ahora pensemos que de un momento a otro se borran por completo todos los archivos sobre los que hemos trabajado por acción de un virus ingresado en alguno de los tantos e-mails que recibimos ese día, o peor aún, por un virus que ingresó en la computadora de otro empleado conectado a la misma red. Esto no sólo podría afectar nuestro trabajo y resultar una pérdida de tiempo, sino que además afectaría al resto del personal que depende de nuestra información.

Si bien es claro que existen situaciones que no podemos evitar, ésta en particular se pudo haber evitado simplemente instalando un programa antivirus, que por estos días resulta bastante accesible a los usuarios en general. Pensemos que en los casos de Pymes o de ambientes domésticos, sólo involucraría una mínima intervención de un profesional de sistemas que participe en la parametrización del mismo, y fundamentalmente, la conducta de los usuarios de actualizarlo todas las veces que sea necesario dado que, como veremos más adelante, la evolución de esta amenaza es constante.

Si lo vemos desde el contexto de una gran empresa, debemos concientizarnos sobre la necesidad de descargar e instalar las actualizaciones de las definiciones de virus que el personal de sistemas envía frecuentemente, lo que sólo tomaría unos pocos minutos.

Uno de los objetivos que tiene el presente trabajo es el de entender que todos (cualquiera sea nuestra profesión o incluso en nuestros propios hogares) debemos conocer las medidas básicas de seguridad que redundarán en una utilización más eficiente de los recursos con los que contamos y en una minimización de los riesgos a los que nos vemos expuestos.

Normalmente la mayoría de los usuarios de la información damos por sentado la existencia de normas de seguridad en las empresas en las que trabajamos, o no le damos la importancia que el tema merece en caso de tratarse de organizaciones más pequeñas.



En los últimos años, quienes tienen el control de la información, ocupan una posición privilegiada en el mercado.

Esto es así debido a que contar con ella en forma anticipada al resto de los usuarios, resulta fundamental no sólo con el fin de garantizar la continuidad del negocio, sino además para minimizar los riesgos, maximizar el retorno de las inversiones y aprovechar las oportunidades que se nos presentan.

Hoy, la información es un activo fundamental, entendiéndose por estos, a los que están relacionados con la continuidad del negocio, como pueden ser planes estratégicos, fórmulas magistrales, diseño de prototipos, contratos, pólizas y demás datos que son los bienes que más nos interesa resguardar bajo la perspectiva de la seguridad de la información.

Por estos días, si bien en muchos casos se cuenta con respaldo en papel de la información más relevante, no podemos negar que la información circula y se almacena en computadoras y a través de redes como las que cualquiera de nosotros utiliza a diario. Y está bien que así sea.

De este modo, otro de los objetivos, sino el principal, del presente trabajo es entender que la seguridad informática no es ajena a nuestra profesión. Me refiero a que, como Contadores Públicos, nuestra responsabilidad no se limita sólo a la confección de estados contables y a la liquidación de impuestos entre otras tareas.

Consideré al momento de encarar este trabajo la posibilidad de tratar otros temas que se podría pensar están más estrechamente vinculados con la carrera de Contador Público, como podría ser el impacto de la carga impositiva en determinados sectores, o la suficiencia o no de normas contables adecuadas.

Pero finalmente me pareció que el tema elegido, además de estar estrechamente vinculado con el avance sostenido de la tecnología en los últimos años, es una problemática común, aplicable al entorno laboral en general.

Sin embargo, no todos los profesionales tienen conocimiento de los peligros que afrontan y las herramientas que cuentan para combatirlos, las cuales serán expuestas a lo largo del presente trabajo.

Hoy en día, la mayoría de las empresas y de los profesionales utilizan como soporte de su información a las computadoras, y puntualmente los Contadores Públicos necesitamos de herramientas adecuadas de cálculo y resguardo de la información de nuestros clientes, ya que pueden verse comprometidos tanto los negocios de estos como nuestro futuro profesional.

Si pensamos en un contexto de pequeñas o medianas empresas, quizás debamos ser nosotros mismos quienes tengamos que proteger la información.

Del mismo modo, en caso de formar parte de una gran empresa, no podemos desconocer la existencia de normas básicas de manejo de la información que podrían afectar a toda la organización y no solamente nuestro trabajo.

Podría darse incluso el caso de que formemos parte de la Junta Directiva, Gerencia o Comité de Auditoria que deba opinar y tomar decisiones respecto de esta problemática, ya que es común que los mismos estén también integrados por personas ajenas a sistemas.

Existe información que debe ser pública, para que con este conocimiento los ciudadanos puedan determinar si el accionar de sus autoridades resulta correcto o no.

Por otro lado existe información que debe ser privada, como por ejemplo los antecedentes médicos, o más orientado a este trabajo, los planes y recursos con los que cuenta una empresa.

La seguridad de la información, no es competencia exclusiva de los expertos en sistemas. Existe una intensa e inmediata necesidad de capturar a estos efectos la atención de la Gerencia y la Junta Directiva.

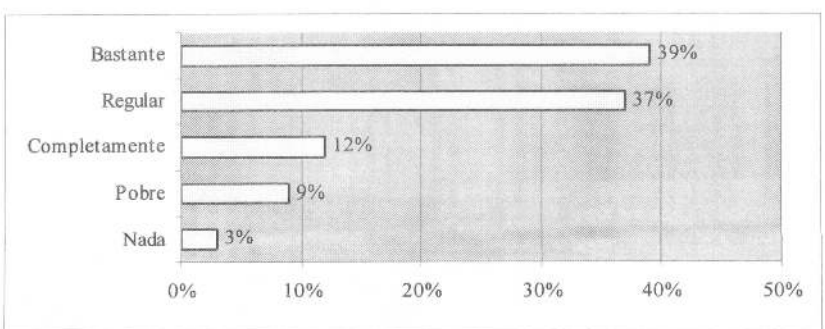
La fragilidad de la información está dada por el medio que la contiene, por los problemas técnicos que presenta dicho medio y por su exposición al alcance de personas que quieran dañarla.

En el caso de la información manejada con computadoras -la más común por estos días- su fragilidad está dada por su procesamiento y almacenamiento (fallas técnicas, catástrofes, impericias) y por la amenaza de intrusos (saboteadores, hackers y virus como acción de daño a distancia).

Con el fin de adoptar una postura efectiva de seguridad de la información, las grandes empresas necesitan alinear el presupuesto de seguridad con sus objetivos, y de esta manera respaldar esta política de resguardo de sus activos digitales invirtiendo en seguridad.

A continuación se expone un gráfico obtenido de una encuesta realizada a nivel mundial sobre el grado de alineamiento de los objetivos de las grandes empresas con el presupuesto de seguridad informática.[1]






[1] Según la encuesta "Global Information Security Survey 2003" realizada por Ernst & Young.