La difícil tarea de la seguridad informática. Análisis de un caso en una organización típica salteña.

Fredi Aprile, Sergio Appendino, H. Beatriz P. de Gallo[1]

(faprile@copaipa.org.ar), (sappendino@copaipa.org.ar), (bgallo@copaipa.org.ar)

Resumen

Las tareas relacionadas con la seguridad informática en cualquier empresa parecen no ser tan simples. La historia que se presenta a continuación, refleja casos reales de acontecimientos surgidos en este ámbito y región, que genera una situación problemática, y de que manera la podemos afrontar.

Palabras Claves: Seguridad - Seguridad informática - Información - Comité de seguridad.

1. La Historia.

La falta de conciencia en la seguridad de los datos es un problema presente en cualquier empresa o institución.

La información procesada, almacenada y consultada por los medios tecnológicos actuales es un recurso más de cualquier organización. En este contexto, la jefatura de una empresa ha confiado en una persona, el *Lic. Juan Seguro*, la responsabilidad de la seguridad informática. Antes de asumir esta tarea, él había ingresado al

[1] Fredi Rene Aprile es Licenciado en Análisis de Sistemas. Analista Senior en el Poder Judicial de Salta en las áreas de seguridad informática, auditorias e informática forense. Es docente de la UCASAL. En el ámbito privado, se desempeña como consultor informático con especialización en la seguridad informática.
Sergio Appendino es Ingeniero en Sistemas, CISA (Auditor Interno de Sistemas Certificado), Docente de UCASAL y Perito Informático en la Corte de Justicia Provincial y Federal de Salta.
H. Beatriz P. de Gallo, es Ingeniera en Computación, Master en Administración de Negocios, docente e investigadora de la UCASAL. Es además perito informático de la Corte de Justicia de Salta. En el ámbito privado, se desempeña en la organización y gestión de proyectos de capacitación in company.

organismo como analista y programador de sistemas, pero siempre se había manifestado interesado en la seguridad informática por su tesis de graduación y algunos cursos e investigaciones que estaba realizando.

Después de dos años de asumir la tarea, Juan se enfrentó con un serio problema: la seguridad de la información es un concepto nuevo en la empresa y por lo tanto observa que existe una “Falta de conciencia generalizada sobre la seguridad de los datos por parte de todos los usuarios”.

2. La inversión.

La magnitud de los riesgos asociados en materia de seguridad informática involucra la inversión de nuevas tecnologías y de recursos humanos. Cada pedido de presupuesto a los niveles superiores debe argumentarse el doble que en las otras actividades.

Sin embargo la inversión se aprobó inmediatamente luego que la página institucional fue hackeada, o aquella vez en que un virus paralizó a toda la organización bloqueando el acceso a los sistemas y al uso de los servicios.

¿Juan deberá esperar que suceda otro incidente de seguridad para que se aprueben nuevas inversiones?

3. ¿Qué es lo que debemos proteger?

Existe abundante información en la empresa. Ante la consulta de Juan de qué información debe proteger, la respuesta de todos los gerentes es “Todo se debe proteger”. Juan pensó en su momento que sería lindo también que su casa estuviese protegida con policías de seguridad en todas las puertas, alarmas, sistemas de vigilancia, investigadores, etc. pero este costo es más elevado que su propia casa.

Lo mismo sucede en cualquier organización, es imposible proteger absolutamente todo o proteger información que por su característica es pública. Por ello se debe definir cuáles son los activos a proteger, cómo clasificar la información, qué dato es público, qué información es privada o sensible, quienes deben/pueden acceder. ¿Quién tiene la responsabilidad de definir qué información es crítica y sensible y definir sus accesos?. ¿Quién es realmente el dueño de los datos?

4. Uso de Internet.

¿Debe permitirse el uso del Chat y del correo electrónico personal?

Se contrató para toda la organización el servicio de Internet, pero por cuestiones de seguridad se limitó el acceso solo a páginas autorizadas y libres de riesgos. A los dos días de implementar esta política, sufrió serios reclamos de los gerentes en el sentido de que se estaba limitando el uso a la información. ¿Debería permitir el uso libre de Internet?. ¿Bajo qué condiciones?

5. Software y licencia de uso.

Después de realizar un análisis de toda la red, Juan detectó numerosos programas instalados vía Internet, mails o medios removibles en la mayoría de los equipos. Por ello se encargó de desinstalar todo y bloquear las futuras instalaciones por una cuestión de seguridad, compatibilidad con los sistemas de la organización y debido a que la mayoría de esos programas no contaban con las licencias legales de uso. Al día siguiente fue acusado con todos los términos posibles que se pueda imaginar por parte de los empleados y gerentes, ya que no podían escuchar música, los protectores de pantalla desaparecieron, no se podía instalar nada, no podían chatear con otros empleados, etc. , etc. . ¿Debería volver atrás con la desinstalación de los programas?. ¿Cómo debe hacer frente a todas las críticas?

6. Los dispositivos removibles

La creciente proliferación de nuevos medios tecnológicos removibles (pendrive, mp3, mp4, memorias de cámaras digitales, etc.) conlleva el riesgo de que cualquier empleado introduzca o extraiga información o programas de/hacia las pcs. Esto tiene un riego adicional si en dichos dispositivos se

encuentran virus informáticos o cualquier programa no autorizado con contenido malicioso que puede causar daños e incompatibilidad en los equipos o los sistemas. Considerando esto, cada vez que bloqueó el acceso a los dispositivos de almacenamiento, tuvo serias quejas de los usuarios porque no podían intercambiar información con otras personas. ¿Debería permitir el uso de medios removibles?

7. Las claves de acceso.

Se habilitó usuario y contraseñas para todas las personas para el acceso a los sistemas, pero algunas de ellas estaban muy molestas ya que tenían una tarea más de recordar esos datos y en algunos casos todos se prestaban o intercambiaban las contraseñas. ¿Cómo debería capacitar a los empleados en este aspecto?. ¿De quién es la responsabilidad de la confidencialidad de las claves?

8. Conflicto de intereses.

Se han producido alteraciones del clima laboral con compañeros de trabajo en cuanto a la operatividad de los sistemas. Cada vez que se adiciona seguridad a las aplicaciones informáticas, se agrega una tarea más a los usuarios y los programadores indican que disminuye la perfomance de los sistemas. La seguridad y la operatividad de los sistemas a veces no se complementan, entonces ¿Quién debería definir ese equilibrio?

Todas las políticas que trata de implementar Juan son consensuadas por la jefatura de sistemas. Aún así, no son bien recibidas por los altos niveles jerárquicos debido a que se imparten desde un área con menor jerarquía en la organización.

Por ejemplo: un gerente general comentó que ningún empleado o subjefe le puede decir a él de que manera debe navegar en Internet o que programa debe instalar. Por otro lado, no es posible aplicar sanciones por incumplimiento a empleados de otros sectores que no sean del área de sistemas.

Sirva esto como ejemplo, para mostrar que los recaudos técnicos que se puedan tomar, no son suficientes para proteger la información, y se requiere de un marco normativo que contenga y establezca las reglas de uso de la información mediante decisiones tomadas, debatidas, consensuadas y aprobadas por los altos niveles jerárquicos

de la organización. ¿Qué organismo, área, unidad organizativa se debería crear? . ¿Qué nivel de jerarquía debería tener?

9. Hasta aquí el problema…

¿Cómo lo solucionamos? pues básicamente con políticas de seguridad que deben ser evaluadas y aprobadas en un organismo interno (Comité de Seguridad), conformado por adecuados niveles de decisión en la organización y que le otorgan al área de seguridad el presupuesto necesario para llevar a cabo la implantación de las políticas, controlar su seguimiento y evaluar acciones correctivas.
El Comité de Seguridad debería fijar en estas Políticas los objetivos que tiendan a:

- Concientizar sobre la seguridad de información. Esta concientización debe incluir un plan de capacitación extenso y profundo, acompañado de una campaña de difusión sobre la importancia de los sistemas informáticos en el negocio de la empresa
- Generar una cultura informática en todos los usuarios dirigida a identificar los “activos intangibles” con el mismo valor que “activos tangibles”.
- Definir responsabilidades de todos los usuarios pertenecientes a la organización.
- Analizar, identificar y definir procedimientos y controles en todos los niveles que involucren riesgos a la seguridad de la información.

El Comité de Seguridad no es un equipo técnico-informático, debe ser un grupo de decisión interdisciplinario en el que tengan competencia todas las áreas de la empresa

10. Conclusiones

No se agota el tema con estas consideraciones, por el contrario, se abre un camino de análisis y preguntas que cada empresa o institución deberá andar por sí misma.

Lo importante es comenzar a crear conciencia en los estamentos de decisión, acerca de la necesidad de formalizar acciones de contención y gestión de la información, que hagan que las tecnologías de la información y la comunicación cumplan con el rol fundamental que hoy tienen en la empresa: la alineación con el negocio.

Bibliografía

Subsecretaría de Tecnologías de Gestión, Secretaría de la Gestión Pública, Año 2005, Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional. ONTI (Oficina Nacional de Tecnologías de la Información).

International Organization for Standarization, Año 2000, Norma 17799– Código de práctica para la administración de la seguridad de la información.

International Organization for Standarization, Año 2005, Norma 27001– Norma para la administración de la seguridad de la información.

Consejo Profesional de Agrimensores, Ingenieros y Profesiones Afines – Universidad Católica de Salta – I-Sec Information Security Education Center, Año 2005, Apuntes "Jornadas de especialización en seguridad de la informacion – curso ISO 17799".

Maestría en Administración de Negocios, año 2006, Apuntes sobre Dirección de Recursos Humanos – Capítulos I, II, III, IV, V, VI - Prof. Edgardo Visñuk.