
El ABC de la Seguridad

Escrito por: Scott Berinato y Sarah Scalet

Traducido al español por: Rafael Sandoval Vázquez

Revisado por: Ing. Alejandro Núñez Sandoval

Artículo extraído de: <http://www.seguridad.unam.mx/plan-becarios/main.dsc?doc=1&op=11>

¿Qué es la seguridad de la información?

¿Qué pasa si no atendemos su importancia?

Pero tenemos firewalls. ¿Eso no es suficiente?

¿Quién debe encargarse de la seguridad?

¿Debiera buscar soporte externo, outsourcing?

¿Qué tecnologías están involucradas?

¿Y sobre las tecnologías inalámbricas?

¿Cuáles son mis obligaciones legales?

¿Cómo me puede ayudar mi seguro?

¿Qué es el ROI?

¿Debo denunciar los incidentes de seguridad a las autoridades?

¿Como han sido las cosas, nadie está del lado de la seguridad?

¿Cuáles son los 10 elementos importantes para una buena seguridad de la información?

Qué es la seguridad de la información?

La seguridad de la información es el proceso de proteger datos contra accidentes, o errores intencionales por personas dentro o fuera de la organización, incluyendo a los empleados, consultores, y si, también, por los muy temidos crackers. Un incidente de seguridad implica cualquier cosa, desde un alteración de la página web, un virus informático, un empleado que inadvertidamente divulgó su contraseña; un ex empleado que sabotee la base de datos de los clientes; o los espías corporativos que descubren cuantos artículos compró su mejor cliente el mes pasado.

Es así que cualquier proveedor de seguridad digno de confianza admitirá, que no existe algo tal como la seguridad perfecta. Para que su organización tenga éxito, necesita permitirle a sus empleados, clientes y a sus socios, tener acceso a la información electrónica, a menudo a través del Internet, y esto genera riesgos. La seguridad de la información, consisten entre balancear estos riesgos con las recompensas de poder hacer transacciones electrónicamente. Y porque sus riesgos y vulnerabilidades están constantemente cambiando, la seguridad es un proceso interminable, no es algo que se realice una vez, y después lo olvide.

En el pasado, muchas compañías confiaron equivocadamente en la **seguridad por oscuridad**, para proteger sus sistemas. Pero considere esto: En un típico día de enero de 2002, un sitio web que seguía tales principios, enumeró 39 modificaciones de páginas web, que habían ocurrido en un solo día, y sólo un culpable que fue un hombre desde su casa. Los ataques más certeros provienen de gente de dentro de la compañía, o del ex empleados, no siempre del estereotipado hacker, con una cara llena de acné y rodeado de cajas vacías de pizza.

Los grandes problemas de seguridad, en organizaciones bien conocidas a veces con datos estimados en millones de dólares- atraen la mayor atención. Pero todo tipo de compañías necesitan protegerse contra las pérdidas financieras, de reputación y de productividad, sin mencionar el tiempo muerto, causado por problemas con la seguridad de la información.

Qué pasa si no atendemos su importancia?

Dependerá de cómo sea atacado, de cualquier forma esto no será agradable. Los virus y gusanos informáticos, como fue el Código Rojo, provocó un periodo largo de tiempo muerto, pérdida en las ventas, y daño de la información en las computadoras- sin mencionar la irritación de los usuarios y el cansancio del grupo de tecnologías de la información. Según Carlsbad, compañía dedicada a la investigación económica de la información, estima que el código malicioso causo más de doce millones en daños solo en el 2001. (Leea "Outbreak" Junio 1, 2001)

Pero al menos contaminarse por un virus no lastima su reputación en la manera que otros agujeros de seguridad lo harían. Los virus tienden a golpear a muchas organizaciones a la vez, y es raro que solo una organización sea seleccionada para ser el blanco de los ataques por un virus. Por otra parte, los medios difusores de noticias, aman divulgar las últimas notas de seguridad sin seriedad, y siempre tienen expertos de seguridad felices de indicar que debió hacer la organización para prevenir que un cracker o un empleado molesto causara daño. La modificación de las páginas web, el equivalente electrónico al vandalismo que a últimas fechas ha sido especialmente problemático, también llamado como **hacktivismo**, es algo usado para que a través de las páginas de otras personas se difundan declaraciones políticas.

Más que perder el tiempo y causar pena, los hoyos de seguridad pueden también conducir a pérdidas financieras severas. Parte de las pérdidas son indirectas: si el incidente erosiona la confianza de los clientes y de los accionistas en como está funcionando la organización. Pero los problemas de seguridad pueden traer daños directos, y estaríamos hablando de pérdidas que podrían afectar de fondo. A principios del 2002, la Associated Press informó que un banco de la ciudad de Nueva York pagó a un cracker ruso diez mil dólares a cambio de no revelar información sensitiva de sus clientes y Éste todavía provocó un daño por \$250,000 dólares. En otro caso reportado en *The New York Times*, un disgustado ejecutivo de tecnología de la información causó más de veinte millones de dólares en daños, cuando este saboteo los sistemas de cómputo de una compañía de químicos de New Jersey, que lo había despedido. Después de un ataque especialmente perjudicial, denegación de servicio, un ISP del Reino Unido, informó el cierre de sus operaciones y puso sus activos en venta. Y por algunas cuentas, el proveedor de software Egghead nunca se recuperó de un incidente de gran magnitud, en donde se informó que más de tres millones de números de tarjetas de crédito pudieron ser robadas por un cracker.

Pero tenemos firewalls. ¿Eso no es suficiente?

Una generación entera de ejecutivos de negocios, vienen de la era en que la noción de los firewalls eran la base de una buena seguridad. La regla no escrita: **Más firewalls, más seguridad**. Pero esto no es justamente la verdad. Aquí hay dos formas en que los firewalls pueden ser vulnerados. Una: Usando fuerza bruta, para inundar al firewall con mucha información de entrada para inspeccionar. El firewall se vendría abajo. Dos: Usar cifrado, herramienta básica de seguridad, para cifrar un correo electrónico que, tenga un virus dentro. El firewall permite el paso de tráfico cifrado tanto de entrada como de salida por la red.

Los firewalls son herramientas necesarias. Pero no son la base de la seguridad de la información. En su lugar las organizaciones deben concentrarse en una arquitectura integral de seguridad. ¿Qué es esto? La seguridad integral significa hacer la seguridad parte de todo y no que esta haga todo. Esto significa que la seguridad no esta añadida a la organización, esto se va realizando dentro de la organización como una aplicación. Aquí un ejemplo. Los que abogan por la no integridad ven las amenazas por virus e inmediatamente comienzan a gastar dinero en software que bloque los virus. El guru de la seguridad integral aplicará una política alrededor del uso de correo electrónico; se suscribirá a los servicios de noticias que emitan alertas acerca de las nuevas amenazas, reevaluará la arquitectura de red, promoverá seminarios para usuarios de las mejores prácticas en los equipos; y usará software que bloque virus, y, probablemente firewalls.

Este es un gran trabajo. ¿Quién debe encargarse de la seguridad?

La seguridad de la información ha sido tradicionalmente parte del trabajo de la gente de las tecnologías de la información, o en ocasiones por parte del departamento de auditoría o finanzas. Donde debiera estar, y quién debiera administrarla son fuente de muchas discusiones. Algunas personas creen que la seguridad necesita un perfil más alto del que puede tener como parte del equipo de tecnologías de la información (TI). Otros se refieren a que es un conjunto de intereses por parte del oficial en jefe de la información (CIO, Chief Information Officer), que a menudo obstaculiza la velocidad o facilidad de su uso. Pero todos están de acuerdo en que el CIO tiene un papel crucial en esto. Esto porque el CIO efectivamente entiende como las computadoras de la organización deben ser instaladas y operadas, y también ellos saben el papel y las limitaciones de la tecnología en la solución de cualquier problema incluyendo la seguridad.

Pero la seguridad es un trabajo grande, así que un número importante de organizaciones

están entregando esta responsabilidad primaria al oficial principal de seguridad (OPS) con un alto perfil, o al oficial de seguridad en la información (OSI). Muchos expertos abogan por que los OPS, deben ser los responsables tanto de la seguridad física como de la información y debe reportar directamente al oficial en jefe ejecutivo (CEO, Chief Executive Officer). Otros recomiendan que los OSI pueden o no informar al CIO y deben trabajar de cerca con quien quiera que este a cargo de la seguridad física.

Al final esto es lo menos importante, los informes del oficial de seguridad, y es más importante que exista alguien encargado de la seguridad que tenga la visión del CEO. El oficial de seguridad necesita tener un contacto directo con el equipo de TI, de seguridad física, auditores, recursos humanos, y del consejero legal. Y aquí existe algo interesante, parte del trabajo del oficial de seguridad es convencer a los empleados de que la seguridad es un trabajo de todos. Hay un viejo refrán que dice que la seguridad es tan fuerte como su eslabón más débil, y este eslabón más débil es aquel empleado que escribe su contraseña en un *post-it* y lo pega en su monitor.

¿Debiera buscar soporte externo?

Un staff de seguridad es difícil de encontrar. Hay poca experiencia y hay muchos impostores. Algunos expertos señalan que hay un verdadero experto por cada 10. Y encontrar el talento es incluso más difícil que pagarlo. Para algunas organizaciones, especialmente aquellas con activos cruciales y extensos activos de información, encontrar y mantener este talento es una dolor de cabeza y además costoso. Pero algunas otras organizaciones realizan estos servicios de seguridad, con otras medidas, los cuales realizan trabajos día a día, como instalar actualizaciones y monitoreo de intrusos.

Estos proveedores caen en dos campos: servicios de dedicados que se centran exclusivamente en seguridad, y organizaciones de servicios que ofrecen seguridad como parte de un paquete. Los servicios dedicados, han atraído a muchos de los grandes expertos en seguridad informática a menudo de las agencias militares y del gobierno, así como de la CIA que han dejado el servicio público para iniciar sus propias organizaciones, y los capitalistas, seguidos por los empleados de confianza. Pero eso condujo a una abundancia: Hubo (y sigue habiendo) muchos proveedores, y han provocado que ese gran perfil se colapse, donde los clientes se encontraron repentinamente sin ninguna seguridad. Compañías más grandes de servicios, generalmente pueden ofrecer más estabilidad y mejores precios, pero los CIO se quejan de que carecen en ocasiones de la experiencia y del servicio de una compañía dedicada única y exclusivamente a la seguridad.

Si usted elige contratar los servicios de una de estas organizaciones, sepa que la seguridad hecha por outsourcing implica más que apenas firmar un cheque cada mes. La seguridad necesita ser abordada fuertemente en los procesos de la organización, y necesita ser alguien de dentro de la misma para manejarla.

¿Qué tecnologías están involucradas?

Cuando se inicia la protección de la organización contra tiempos muertos, o vulnerabilidades de seguridad, el software antivirus, es usualmente usado como primer paso. Este tipo de software busca virus, gusanos, troyanos y otro código malicioso que pueda destruir información y aplicaciones y expenderse, rápidamente de computadora a computadora. El software trabaja buscando comportamiento sospechoso y códigos maliciosos conocidos. Dado que nuevos virus son descubiertos todos los días, el personal de TI necesita estar vigilando permanentemente el que sus usuarios tengan instalados las últimas actualizaciones del software.

Aunque los firewalls son sobrevalorados, ellos siguen siendo cruciales cuando se trata de prevenir problemas de seguridad. Un firewall es un método para proteger la privacidad de la red analizando los datos de entrada como de salida. Los firewalls pueden también proveer de la conversión de direcciones IP (NAT), de forma tal, que una dirección IP de una computadora dentro del firewall permanezca oculta a la vista. Firewalls de filtrado de paquetes, usan reglas en los paquetes de origen, de destino, puerto u otra información básica para determinar si debiera permitirse la entrada o no a la red. Algunos más avanzados, como los firewalls que filtran el estado del paquete, tienen acceso a más información, con lo cual toman sus decisiones. Firewalls tipo Proxy, los cuales buscan el contenido y pueden involucrar autenticación y cifrado, pueden ser más flexibles y seguros, pero son más lentos.

El reconocimiento de que los firewalls son imperfectos, es aprovechado por algunas organizaciones para invertir en sistemas detectores de intrusos (IDS). Los IDS es software que busca actividad no autorizada en un sistema de cómputo, para identificar, reportar y tal vez responder a la actividad sospechosa, así como lo haría una alarma contra ladrones casera una vez que ha sido rota una ventana. Los IDS están por lo regular en dos categorías: los basados en red, los cuales analizan el tráfico de paquetes a través de la red; y los basados en host, que monitorean los archivos de bitácora e información en las computadoras individuales.

Hoy por hoy, la mayoría de los administradores se enfocan al software y hardware de la organización, en busca de malas configuraciones, y huecos que puedan ser explotados por los crackers. Esto implica el no perder de vista las últimas vulnerabilidades, instalando actualizaciones para eliminar estos problemas y asegurarse de que estas actualizaciones no causen problemas. Esto es un proceso crucial, en ocasiones llamado administración de actualizaciones, y es un dolor de cabeza. Existen servicios que envían un increíble y aparente sin fin de advertencias sobre las nuevas vulnerabilidades que afectan a cierta clase de hardware y de software.

Para ayudar a los administradores de seguridad a enfocar sus esfuerzos, el SANS y el Centro Nacional de Protección a la Infraestructura mantienen una lista de las 20 vulnerabilidades más críticas de seguridad. La número uno, son los sistemas operativos que son instalados con las configuraciones por defecto, las cuales proveen un camino fácil para los crackers. Otras vulnerabilidades comunes son las cuentas sin contraseñas, o inadecuadas, otra son la gran cantidad de puertos abiertos. (Para mayor información, visite: SANS).

Y sobre las tecnologías inalámbricas?

Las tecnologías inalámbricas presentan un gran riesgo a la seguridad, por obvias razones puertas, paredes y candados pierden significado cuando la información se transfiere sin cables. Cuando el CIO informó este tema en 2001, se envió a un reportero al distrito financiero de Boston con una computadora portátil, y una tarjeta inalámbrica para LAN, y así podría trabajar fácilmente sobre la LAN sin cables. Al poner en ejecución tecnologías extrema advierta de lo límites de la señal inalámbrica, Cerciórese de que la información está cifrada, Y verifique que la gente que utiliza este servicio inalámbrico esté familiarizada con los procedimientos de seguridad y siga los pasos para las contraseñas adecuadas.

Cuáles son mis obligaciones legales?

Diversas industrias tienen que cumplir diferentes requisitos legales en la protección de la información. Por ejemplo, Gramm-Leach-Bliley Act fija las reglas para la industria de servicios financieros, y la Health Insurance Portability and Accountability Act monitorea a las compañías dedicadas al cuidado de la salud. Además las organizaciones que hacen negocios a través de los mares deben de seguir reglas establecidas en otros países, como en la Unión Europea, con reglas estrictas. Las compañías que no resuelven estos requisitos podrían enfrentar complejas penas o pleitos legales.

Una creciente preocupación, es sin embargo, como las organizaciones pueden ser obligadas para tener una seguridad adecuada. Los expertos temen por los pleitos legales que les pueden ser acarreados por clientes, a los que su información haya sido divulgada, pleitos corporativos causados por la ruptura de la seguridad en la información de los socios, y los pleitos legales llevados a cabo por los accionistas furiosos. Esta clase de problemas esta apenas comenzando a emerger, pero hay varias maneras de proteger a las organizaciones.

Primero fije las reglas de cómo la organización va a proteger y manejar la información, y después comunique estas reglas a los empleados. Escriba los requerimientos de seguridad al momento de hacer contratos con proveedores y al revés, esté seguro de no hacer promesas que no pueda cumplir. Finalmente tenga una auditoría de seguridad realizada. Este es un proceso en el cual una organización independiente, a menudo una firma de auditorías corporativas o a una compañía aseguradora informática, prueba las medidas de seguridad de la organización de las debilidades físicas en la configuración del firewall, como los empleados deben cuidar de los activos para protegerlos, el como los administradores pueden identificar ataques y realizan recomendaciones de cómo la seguridad puede ser mejorada.

¿Cómo me puede ayudar mi seguro?

Las pólizas básicas de seguros, no cubren típicamente los riesgos asociados a tener negocios en línea. El Seguro Informático, es ofrecido por algunos grupos así como por compañías nuevas llamadas e-centric, las cuales tapan este hoyo. Los también llamados seguros de e-commerce, dan una cobertura que permite blindar a su organización de la pérdida financiera causada por ataques de negación de servicios, virus, robo de secretos informáticos o de comercio con los clientes, incidentes relacionados al aislamiento, responsabilidad en pleitos y más. El costo de esta cobertura varía, dependiendo el tamaño y a el alcance de los sistemas informáticos de la organización y como la compañía a tratado a fondo la seguridad.

Estos seguros son relativamente nuevos y no probados. Sin embargo, los expertos predicen que en un futuro, el seguro informático ayudará a construir estándares alrededor de la seguridad informática. Algunas organizaciones de seguros, ya han creado algunas líneas a seguir para los clientes que usen cierto sistema operativo.

¿Qué es el ROI?

Por años, el regreso a la inversión en seguridad (ROSI, return on security investment) no ha sido calculada, como muchos lo habían postulado. Un positivo ROSI fue *no paso nada*. Eso en revisiones de presupuesto está mal. El jefe de finanzas desea una análisis de costo beneficio, lo cual es un problema con la seguridad, pareciera una comparación entre manzanas y naranjas. ¿Entonces? Con la seguridad, los costos son en dólares y los beneficios no existen. Los beneficios en la investigación sobre la seguridad siempre se han caracterizado como conceptos pesados, que viven lejos, en el fondo.

En las noticias se esta viendo una nueva ola de investigación. Esto se demuestra tan pronto como usted construye seguridad dentro del proceso de ingeniería del software, menor costo en la seguridad como sería el costo involucrado en generar un sistema de alarma dentro de los planes de un banco que requiere instalar un sistema de alarma una vez que el banco es construido.

Careciendo de un ROI, se puede justificar el gasto precisamente en base a los problemas que se han tenido. Comience en crear un archivo con los recortes de periódico sobre las compañías que han tenido problemas de seguridad penosos. Hay pocos estudios sobre el costo y la frecuencia de estos problemas de seguridad, pero usted deberá utilizarlos lo mejor posible. Los estudios a menudo citados, son investigaciones realizadas cada año por el FBI y por el Computer Security Institute, y alguna otra organización relacionada a la economía informática, y se enfocan principalmente a los códigos maliciosos. Estos estudios no son científicos por ningún lado, pero son un comienzo.

Debo denunciar los incidentes de seguridad a las autoridades?

Se recomienda que usted considere ampliamente esta opción. Pocos años atrás, la aplicación de la ley ha conseguido mucho más sobre los delitos informáticos. La percepción de los agentes que vienen, es el del marcar el área con cinta amarilla y luego desaparecer con todas sus computadoras, lo cual no es verdad. Como el crimen organizado haciendo uso de computadoras y ahora, con miedo enfocado al terrorismo es importante no dejar que el delito informático siga sin control. Los funcionarios que aplican la ley pueden buscar patrones, recoger evidencia y poner en ocasiones a los hackers tras las rejas, y esto no significa necesariamente hacer que el nombre de su organización sea manchada con lodo. Considere en entrar en contacto con funcionarios de la aplicación de leyes ante este tipo de incidentes. De esta forma, si se presenta algo así usted estará mejor equipado y podrá tomar una decisión. El DSC cuenta con especialistas encargadas de realizar seguimiento a delitos informáticos.

¿Cómo han sido las cosas, nadie esta del lado de la seguridad?

Porque es difícil. Puede estar fuera de la mira de cientos o de miles de supuestos ladrones, pero solo les basta moverse para causar caos. Cuando se investiga sobre seguridad en la información, hay pocos estándares y poca experiencia, y nadie desea hablar de cómo su organización se convierte en un blanco. Pero esto aun es peor, los hackers están dispuestos a compartir noticias sobre las vulnerabilidades y exploits, lo que significa aprender de otros.

La mejor manera de luchar, es conseguir que su compañía hable sobre la seguridad. Esto es fácil de decir, más que de hacer. Esto significa el reconocimiento de que algo podría salir mal, y esto es un proceso doloroso. Gente de la organización necesita pasar tiempo valioso pensando acerca de algo que no generará dinero. Usualmente se pasa más tiempo viendo como figurar hacia fuera, que el que se toma en ver como alguien puede lastimar su compañía. Pero el número de intentos de hackeo sigue creciendo, es tiempo de que las compañías detengan el estar asustados por los huecos de seguridad y comiencen a hacer algo al respecto.

¿Cuáles son los 10 elementos más importantes para una buena seguridad de la información?

Aunque no existe manera de garantizar que su organización no sea vulnerada, aquí están las 10 mejores prácticas para iniciar.

1. Identificar los riesgos. Determine cuales son los activos más críticos de información de la organización, y gaste su tiempo y energía en proteger lo más importante.
2. Consiga que los Directivos se involucren; Una buena seguridad inicia desde arriba, con lo ejecutivos quienes ayuden a crear una cultura corporativa de valores de seguridad.
3. Ponga a alguien a cargo. La seguridad es un trabajo complejo, cerciórese de que alguien esté a cargo de coordinar estos esfuerzos de seguridad.
4. Desarrolle y ponga en marcha políticas de seguridad. Establezca las pautas de cómo su organización maneja y protege sus datos de quien deberá asegurarse de que las actualizaciones están instaladas, de cómo los empleados tienen acceso a sus correos remotamente, con que frecuencia las contraseñas deberán cambiarse.
5. Capacite a los empleados y eleve el conocimiento. Haga del conocimiento de que la seguridad es un proyecto continuo. Los empleados necesitan entender porque su papel es tan crítico.
6. Realice una auditoría de seguridad. Emplee a terceros para evaluar su postura de seguridad y despues aplique las recomendaciones hechas por el auditor.
7. Incorpore seguridad física en el plan. La mejor tecnología de seguridad en el mundo no hará nada si un empleado deja a la persona incorrecta frente al servidores.
8. Recuerde las amenazas internas. La mayoría de los intentos vienen del exterior, pero las intrusiones más eficaces comienzan con la gente que tiene conocimiento del interior. Debe tener un procedimiento de eliminación de cuentas de usuario una vez que estos se fueron.
9. Esté en sintonía. Asegurese de que alguien está al tanto de los desarrollos en seguridad, incluyendo nuevas vulnerabilidades y ataques.
10. Preparese para lo peor. Crear un plan de respuesta a incidentes le ayudará a ahorrar tiempo cuando haya un problema de seguridad. Esto permitirá saber quien debe estar involucrado, cuales son sus funciones, y como se reducirá el daño.