"Sobrevivir en la economía del conocimiento - Seguridad Informática"

Álvaro José Trujillo M.

Cuando niño… mi mamá me decía… mira a lado y lado de la calle antes de cruzar, no le recibas nada a extraños, no hables con extraños, igual al final con su maternal sonrisa, me "*echaba*" la bendición y me encomendaba a los santos…

Hoy, cada vez que me levanto, hago lo que ella hacía por mí, enseño a mis hijos a hacerlo y estoy convencido de que sin esa incesante devoción de mi madre por mi seguridad, no sería quien soy y probablemente no estaría aquí.

Durante más de 15 años trabajando en el negocio de las TIC[1], he visto nacer y morir muchas tecnologías y cada día veo cómo avanzamos vertiginosamente hacia una dependencia total de la información, y no sólo en los entornos laborales, sino también sociales; no por nada decimos estar en la economía del conocimiento.

Cuando miro hacia atrás, observo y recuerdo cuando Internet era apenas una red con una visión poco clara de su futuro, compitiendo con redes de alta trayectoria, con protocolos altamente confiables, con capacidades altas de crecimiento y compitiendo con redes de conocimiento ya establecidas.

Al inicio, pensábamos como sería posible integrar tantas redes, si localmente era una fantasía llegar a

sitios remotos de la ciudad; y, más complejo todavía, con ciertas zonas del país a unos costos altísimos y con unos riesgos de seguridad y orden público mayores. Trabajábamos con este objetivo… conectividad.

Recién habían empezado a aparecer elementos como los Bridges y los Routers y difícilmente un computador podía tener múltiples protocolos de red; empezábamos a pensar qué tan procedente iba a ser a largo plazo integrar o utilizar protocolos como IPX/SPX[2] y SNA[3] con el que se extendía en las plataformas UNIX, llamado TCP/IP[4] que, a diferencia de los otros, utilizaba no sólo unos definidos claramente a partir del estándar OSI[5], sino que aparecía como una familia de protocolos basada en un estándar desarrollado para unas funciones básicas de conectividad, y al cual se le iban agregando funcionalidades como parches, con base en las necesidades.

En realidad, no veía claro el futuro de un protocolo que a diferencia de los otros tenía menos capacidad de direcciones para los computadores, de redes, y estaba orientado a la conectividad y no a la seguridad; y, se estaba proponiendo para integrar las redes a nivel mundial.

Sin embargo, rápidamente se fue adoptando TCP/IP como la base de lo que hoy es Internet, no sin crear y desechar protocolos e ideas (por decir algo de aquellos que se van dejando en el olvido como Archie[6] y Gopher[7]).

"Al mismo tiempo que empezábamos a ver estas integraciones en una red única, otro fenómeno estaba pasando, la proliferación de aquello que hoy es uno de los más normales casos de inseguridad: los virus informáticos."

Al mismo tiempo que empezábamos a ver estas integraciones en una red única, otro fenómeno estaba pasando, la proliferación de aquello que hoy es uno de los más normales casos de inseguridad: los virus informáticos. En un principio y aunque tuviésemos redes, nosotros éramos los encargados de transportarlos de una a otra máquina en los discos flexibles que, entre otras cosas, eran los medios a través de los cuales se

lograba el funcionamiento de los computadores.

Empezamos desde entonces a buscar cómo evitar que los discos fuesen infectados por los virus, como uno de los puntos más importantes de la seguridad local, pues aún esta, aunque era una preocupación en los centros de datos, todavía no lo era en la gran mayoría de las oficinas de gerencia de las organizaciones. Aún teníamos la información en los libros y anaqueles y no se entendía la potencia que podían darnos el computador y la información digitalizada.

Además, los sistemas operativos y aplicaciones disponibles estaban "diseñados con niveles de seguridad y con altas normas técnicas, por expertos y pensando en todos los riesgos que podrían acaecer"; esto era lo que se pensaba y en realidad la cantidad de problemas de pérdida de información o destrucción de la misma, se daban más por fallas físicas de los dispositivos, que por robo o fraudes… De eso estábamos seguros, por eso vivíamos pendientes de la integridad de los datos, pues la confidencialidad estaba garantizada por la fábrica, con los privilegios que asignábamos.

Era pues una época en la que estábamos atentos a la conectividad y concentrados en lograr que las computadoras llegaran a todos los lados de nuestras organizaciones y que los incipientes usuarios, asumieran tales tecnologías como propias y entendieran las ventajas de contar con los computadores a su servicio.

Fue una época de enseñar que los equipos de computación eran buenos, que se podían integrar y que gracias a ellos, las organizaciones serían más productivas y tendrían un alto valor de oportunidad de la información, toda vez que tendríamos nuestra información completa en tiempo real.

"…¿Como lograr que sólo pudieran acceder a la información a la que sabíamos que deberían consultar?"

Este énfasis en uso y conectividad, nos descuidó de una característica que muy pronto empezamos a ver. Ya no queríamos que todas las personas de la organización tuviesen acceso a la información completa, algo de lo que antes no nos teníamos que preocupar, pues no tenían computador; ahora es una imperiosa

necesidad. ¿Como lograr que sólo pudieran acceder a la información a la que sabíamos que deberían consultar?

Se observó entonces, que no era suficiente aquello de crear usuarios y claves con privilegios, y que se estaba generando un problema de índole mayor, al intentar controlar de la manera convencional un nuevo problema.

Se empezó a analizar que las secretarias tenían las cuentas de los gerentes para ayudarles a hacer sus tareas mediante el computador "que ellos no habían tenido el tiempo de aprender", debido a sus más importantes labores, y era el momento de tomar las riendas de las empresas, en la medida que cobraba fuerza la información.

Fue entonces cuando se dio un segundo aire que dio lugar a un entorno generalizado. Se quería tener el control de todo lo que estaba pasando y se requería que la información, no sólo estuviera disponible para quien la necesitara y donde la necesitara, sino para la persona autorizada.

Además de pensar en nuestras fallas físicas, también empezamos a pensar sobre quiénes podrían tener acceso a nuestra información, pero en un contexto de empresa. Y, sólo hasta la integración con Internet, fue posible que las diferentes empresas empezaran a escuchar sobre los muchos riesgos informáticos y la necesidad de evitar conectarse a la red sin ningún elemento de protección.

Apareció el término firewall, muros de fuego, elementos de control que nos ayudarían a conectarnos a Internet y a evitar que alguna cibernauta pudiera entrar a nuestra organización. Se trataba de una época inicial en la que todavía los servicios no estaban en el ciberespacio, la red en la que al poco tiempo encontraríamos más información y empezáramos a utilizar para poner nuestra información publicitaria en servidores que arrendaban espacio para tal fin. Ese es el uso más común de esta nueva red.

"Además de pensar en nuestras fallas físicas, también empezamos a pensar sobre quiénes podrían tener acceso a nuestra información, pero en un contexto de empresa..."

“Más tarde, empezamos a experimentar otras necesidades: que no bastaba con publicitar, también requeríamos buscar información y cada vez con mayor celeridad...”

Más tarde, empezamos a experimentar otras necesidades: que no bastaba con publicitar, también requeríamos buscar información y cada vez con mayor celeridad; que nuestra información estuviera actualizada; que estuviera en línea y que los datos fueran vistos por nuestros clientes con la misma rapidez en que los generábamos; y, que tal información estuviera integra y disponible en forma confidencial.

Y fue cuando nos dimos cuenta que no era tan fácil y que requeríamos obtener servicios de Internet. Que deseábamos mayor comunicación, correo electrónico, videoconferencias, teleconferencias, acceso a la información de nuestros proveedores, entrega de información a nuestros clientes, acceso a redes de pares, para evaluar lo que estaban haciendo, control de múltiples funciones y múltiples servicios, y todo esto en tiempo real. Y hoy, Internet, comunicación en línea y datos en tiempo real no son una opción, son una necesidad; y, para mantenernos en el negocio, se requiere asegurar que estos procesos y esta información estén adecuadamente protegidos.

Es el momento en que sin darnos cuenta Internet y las redes de computadores han creado una nueva sociedad, donde la información entra a ser parte de la cadena de producción, donde esta controla en gran parte la economía mundial y donde la necesidad de protegerla se hace tan imperiosa o más que proteger los bienes tangibles.

Ya no basta con antivirus y firewalls, estos han evolucionado a antimalware e IPS, que ya no solo evitan los contagios de virus, sino las nuevas amenazas. Muchas de ellas buscan el acceso a nuestra información, logrando que la entreguemos en sitios indebidos, para luego hacer uso de las contraseñas en nuestras propias bases de información. Otros, como los piratas informáticos, buscan a partir de acciones con alto conocimiento técnico, burlar la seguridad brindada por los elementos de control para apoderarse de nuestros secretos.

Así mismo, queremos tener más información sobre lo que hacen los usuarios, y podemos utilizar los elementos que contemplan los controles de seguridad para permitirnos avanzar con tranquilidad en este nuevo mundo y tomar decisiones; no con la intuición de nuestros padres o abuelos, sino con la información adecuada para orientar en gran medida la intuición.

Gestión de la seguridad de la información

Vamos llegando a la necesidad de saber si estamos haciendo lo que debemos y entendiendo que hay un movimiento mundial al respecto, y se abre el panorama. No basta con poner una serie de controles tecnológicos para lograr que nuestra información esté segura, pues hemos encontrado que no es fácil estar pendiente de tantas cosas y al mismo tiempo hacer que el negocio logre sus cometidos. Es necesario empezar a gestionar la seguridad de la información.

En este sentido y entendiendo que es una necesidad mundial, se inicia por la evaluación de los diferentes espacios donde se discute el tema, de ahí que se empiecen a ver los esfuerzos importantes de grupos de profesionales, los cuales son escritos en diferentes publicaciones como los libros de ITIL[8], y otros tantos con orientaciones especiales como las descritas por la BS7799-1[9] y BS7799-2[10].

A finales del siglo pasado tales acciones empiezan a dar a sus frutos, pero con una problemática adicional, nos acabábamos de dar cuenta que muchos de los desarrollos, aplicaciones y sistemas que creíamos perfeccionados, tenían pequeños grandes problemas, no estaban preparados para el siglo 21 y dejarían de funcionar el 31 de diciembre de 2000.

“Ese riesgo generó una amplia atención por parte de todo el sector de las TICs, y frenó un poco los esfuerzos en la gestión de la seguridad, porque la necesidad inmediata era permanecer en el siglo 21.”

Ese riesgo generó una amplia atención por parte de todo el sector de las TICs, y frenó un poco los es-

fuerzos en la gestión de la seguridad, porque la necesidad inmediata era permanecer en el siglo 21.

Fue luego del 2000 cuando se incrementaron los esfuerzos de seguridad y se empezó a pensar fuertemente en la gestión, no sólo de la seguridad informática, sino en un concepto más amplio. Es decir, se dio un salto de la seguridad informática a la seguridad de la información. Debíamos ser muy cautelosos, pues cuando la información salía de los sistemas a través de una impresora, para citar un ejemplo, se perdía el concepto de seguridad informática y se podría perder el control de la misma.

"Luego de iniciado el nuevo siglo y controlados los efectos sobre el cambio de milenio, la ISO terminó con sus labores de evaluación del estándar británico y adaptación a la norma internacional, creando lo que hoy día es la familia ISO27000."

Luego de iniciado el nuevo siglo y controlados los efectos sobre el cambio de milenio, la ISO terminó con sus labores de evaluación del estándar británico y adaptación a la norma internacional, creando lo que hoy día es la familia ISO27000.

Hoy día se realiza la gestión de la seguridad informática, con una visión del negocio, tendiente a recuperar el control de la información, y pensando en un modelo cíclico de mejora continua, para estar tranquilos de que hemos tenido en cuenta aquellos aspectos en los que se podría comprometer la seguridad de la información y cómo esto podría afectar el negocio.

Y mientras más recuerdo todo el proceso, me encuentro todo el tiempo con las frases que mi mamá me decía cuando niño, las cuales siguen siendo vigentes desde la era de la información y la economía del conocimiento. No recibas nada de extraños, no hables con extraños, mira para lado y lado antes de cruzar la calle. Lo sigo haciendo en el uso del correo electrónico, durante las largas horas de navegación, en el acceso a mi red social, cuando respondo mensajes y veo que seguimos siendo las personas las que logramos que el planeta sea seguro, aún en el ciberespacio.

Pero por si acaso, aún “me echo la bendición y me encomiendo a los santos”.

Notas de pie de página

[1.] Siglas de Tecnologías de la Información y las Comunicaciones.

[2.] Protocolo difundido ampliamente por Novell en sus productos Netware.

[3.] Protocolo difundido ampliamente por IBM y basado en el estándar OSI.

[4.] Protocolo que actualmente tiende a ser el único, gracias a ser el protocolo base de Internet.

[5.] Modelo de interconexión de sistemas abiertos, definido por la organización internacional para la estandarización y que es utilizado como modelo de referencia y de estudio de las comunicaciones digitales. Es un modelo basado en 7 niveles y analiza la comunicación desde la parte física hasta las aplicaciones.

[6.] Sistema que mantiene un índice de los datos de un servidor y permitía localizarlos a través del índice, hoy día en desuso .

[7.] Sistema que permite el acceso a la información a partir de menús, hoy día en desuso. Tanto el Archie, como el Gopher, son innecesarios debido a l sistema actual de Internet y los hiperenlaces.

[8.] ITIL : Siglas de Information Technology Infrastructure Library. Es un marco de buenas prácticas para la gestión del servicio de Tecnología de información, hoy día es la base del estándar ISO2000

[9.] BS7799-1: Estándar británico que contiene el marco de buenas prácticas para la gestión de la seguridad de la información, luego fue adoptado por la ISO como ISO17799 y posteriormente se convirtió en la ISO27002

[10.] BS7799-2: Estándar británico que contiene la definición de un Sistema de Gestión de Seguridad de la Información, luego fue adoptado por a ISO como ISO27001

Álvaro José Trujillo Mejía. *Ingeniero Civil egresado de la Escuela Colombiana de Ingeniería con estudios en Alta Dirección del Inalde. Su experiencia profesional ha estado vinculada como gerente NewNet S.A., empresa enfocada en la prestación de servicios y soluciones en las TIC´s, con una visión multidisciplinaria de los procesos que la empresa ejecuta, lo que le ha permitido desarrollar destrezas en el campo de la planificación, la organización, la dirección, el control y la coordinación del Talento Humano y recursos materiales para el logro de los objetivos empresariales.*

Esta columna fue escrita con el apoyo de:

Jaime Augusto Zuluaga U. *Consultor de Innovación en NewNet S.A., ABCP, ITSM, CISM, CISA, PMP. Ingeniero Informático de la Universidad Católica del Norte; con más de 18 años de trabajo en el sector de las Telecomunicaciones; amplia experiencia en redes, comunicaciones, seguridad de la información, consultoría en ITIL, gestión del cambio empresaria, y planes de continuidad del negocio.*