MODELO DE SEGURIDAD DE LA INFORMACIÓN

Sandra M. Bonilla
Bancolombia
Medellín, Colombia
smbonill@bancolombia.com

Jaime A. González
GrupoMide SA
Medellín, Colombia
jgonzalez@grupomide.com

(Tipo de Artículo: **Reflexión**. Recibido el 01/11/2011. Aprobado el 12/01/2012)

RESUMEN
Para implementar un modelo de seguridad en las organizaciones, se debe seguir unos pasos esenciales para una adecuada toma de decisiones y elevar así los niveles de seguridad en la información. Este artículo hace un recorrido por las diferentes configuraciones para el diseño de la seguridad, empieza por la identificación de las amenazas informáticas, que constituye el primer paso para una buena protección de los flujos de datos que se manejan en las organizaciones. Continúa con el análisis e identificación de los riesgos, para mitigar el impacto en caso de la materialización de los mismos, generar los controles y políticas de seguridad las cuales pueden ser fácilmente cuantificadas y diseñadas de acuerdo con lo establecido en el paso anterior, para así tener un adecuado control sobre los impactos en la seguridad. Finaliza con el modelo de seguridad, donde se identifican los requerimientos y se desarrolla la arquitectura de la red.

Palabras Clave
Arquitectura de red, aseguramiento de red, políticas de seguridad, seguridad informática.

SECURITY MODEL OF INFORMATION

ABSTRACT
To implement a security model on corporate organizations, there are some essential steps that need to be taken into account in order to achieve adequate decision-making, thus increasing security levels on the information. This article makes a review on different configurations for security designs; it begins by identifying the informatics risks, which constitutes the first step for proper protection of data stream managed by organizations. It continues with the analysis and identification of the risks to mitigate their effect it they become real, and creating controls and security policies, which in turn can be easily quantified and designed according to all that has been established on previous steps, thus having and adequate control over the security risks. Finally a security model is presented, where the requirements are identified and the network architecture is developed.

Keywords
Computer security, network architecture, network assurance, security policy.

MODELE DE SECURITE DE L'INFORMATION

RÉSUMÉ
P*our implémenter un modèle de sécurité de l'information dans les entreprises, il faut donc de suivre des procèdes essentiels pour prendre des décisions de manière adéquate et d'augmenter le niveau de sécurité de l'information. Cet article fait une révision des configurations pour la conception de la sécurité, d'abord avec l'identification des menaces informatiques, qui constitue le premier pas vers une bonne protection des flux de données qu'ont des entreprises. Après on analyse et on identifie des risques, pour mitiger l'effet si les risques deviennent réels, aussi créer des contrôles et politiques de sécurité qui peuvent être quantifiés et conçus facilement d'après ce qu'on a dit dans le pas antérieur, ainsi avoir un bon contrôle de leurs effets. Finalement, on présente le modèle de sécurité, en identifiant les nécessités et en développant l'architecture du réseau.*

Mots-clés
Architecture de réseau, affermissement de réseau, politiques de sécurité, sécurité informatique.

1. INTRODUCCIÓN

En la actualidad, las oportunidades de negocio se apoyan en el uso de las nuevas tecnologías, las cuales vienen acompañadas de riesgos significativos en el manejo de la información. Esto hace que su administración tenga un papel importante, porque debe partir de una adecuada identificación de elementos críticos y, sobre todo, tener claro cuáles son los riesgos y clasificarlos; para luego diseñar estrategias y controles apropiados de mitigación en cuanto a su seguridad y poder alcanzar una buena toma de decisiones.

En el mercado actual, las organizaciones deben basar sus procesos en sistemas informáticos que cada día dependen más de la tecnología. Para garantizar la permanencia y la competitividad del negocio en el mercado, es necesario proteger esa infraestructura tecnológica. También es común que se disponga de pocos recursos para las áreas tecnológicas, pero esto no debe justificar dejar de implementar e invertir en seguridad.

Muchas organizaciones tienen el pensamiento paradigmático de no destinar fondos para el componente de seguridad de la información, pues según la mayoría, éstos elevan los costos de la misma. Pero lo que no es tenido en cuenta a la hora de llegar a estas conclusiones es que, no contar con ello, puede generar sobrecostos representados en la afectación de la imagen, la realización de re-procesos, riesgos en el manejo de los datos y de los recursos financieros, entre otros.

Por lo tanto, en un mundo donde los sistemas cobran cada vez mayor importancia, considerar este aspecto dentro de la planeación estratégica constituye en un factor clave para el éxito de las organizaciones.

2. AMENAZAS INFORMÁTICAS

Con la aparición y masificación del uso de las redes informáticas y en especial de Internet, las organizaciones implementaron gran variedad de servicios para facilitar el manejo de la información e incrementar sus posibilidades de negocios. Desafortunadamente, al mismo tiempo surgieron individuos que realizan actividades ilegales con el objetivo de irrumpir en los flujos de información privados y confidenciales, haciendo que esas redes se convirtieran en un entorno inseguro.

Ninguna industria está exenta de esto, porque puede presentar vulnerabilidades que arriesguen la integridad, confidencialidad y disponibilidad de los datos, al ser atacados por entes externos o internos de la misma organización, mientras ella no tiene el conocimiento o los sistemas necesarios para su detección. Por tal motivo, se han orientado esfuerzos en procura de investigar acerca de las diversas amenazas informáticas y con el ánimo de alertarlas y motivar en la búsqueda de una protección integral contra esta latente, sigilosa y peligrosa amenaza [1].

2.1 Clasificación de las amenazas informáticas

Las organizaciones deben contar con suficiente experiencia para identificar los diferentes riesgos tecnológicos que pueden vulnerar su continuidad en el negocio. Estos riesgos se pueden clasificar como amenazas internas o externas; las primeras son generadas por factores internos de la organización y las segundas por factores externos.

*Amenazas externas***.** Se originan al interior de la organización y algunas de las más frecuentes son: virus —gusanos, caballos de Troya—, *spam*, represalias de ex-empleados, espionaje industrial o ingeniería social [1].

*Amenazas internas***.** Se generan al interior de la organización por los mismos usuarios, ya sea con o sin intención. Pueden ser muy costosas debido a que el infractor, por ejemplo un empleado descontento, conoce muy bien la estructura organizacional, tiene mayor capacidad de movilidad dentro de la misma, mayor acceso y perspicacia para saber dónde reside la información sensible e importante.

Dentro de estas amenazas también se incluye el uso indebido del acceso a Internet por parte de los empleados, así como los problemas que podrían ocasionar al enviar y revisar material ofensivo a través de la red [1]. Cuando una de estas amenazas se hace efectiva se convierte en un ataque, el cual puede ser activo o pasivo. El primero sucede cuando el ataque se vuelve evidente y directo a los servicios tecnológicos de la organización y el segundo cuando el riesgo está orientado a la pérdida de información secuencial y progresiva [1].

Este tipo de amenazas deben ser identificadas oportunamente mediante un seguimiento exhaustivo a los patrones de comportamiento, tanto de los sistemas como de los usuarios internos y externos de la organización, de manera que se puedan identificar irregularidades en el proceso continuo de la información.

Es muy importante que las organizaciones inviertan y adopten mecanismos de seguridad que permitan resguardar su activo más importante, la información. Cada día las amenazas informáticas aumentan en número y complejidad, para lo cual se debe estar preparado.

2.2 Estado actual en Colombia

En los resultados de la XI Encuesta Nacional de Seguridad Informática, realizada a través de la Web por la Asociación Colombiana de Ingenieros en Sistemas ACIS y en la que participaron 215 personas de diferentes sectores productivos y varias organizaciones especializadas en seguridad, se revela información sobre los tipos de incidentes o fallas tecnológicas en seguridad informática más frecuentes y las causas de las mismas.

En la Figura 1 se muestran los incidentes de seguridad presentados en los últimos años —2009, 2010 y primer semestre del 2011—. Según los estudios realizados, en el año 2009 se reportó que el mayor número de incidentes presentados fueron causados por virus y por la instalación de software no autorizado. En el 2010, estos incidentes se disminuyeron notablemente, pasaron de 70 incidentes causados por virus a 20 y disminuyeron progresivamente en el transcurso de 2011. Lo mismo se puede identificar con la instalación del software no autorizado, en 2009 se evidenciaron 60 incidentes a causa de esta falla en seguridad, disminuyó a 20 incidentes o menos en 2010 y 2011 [2].

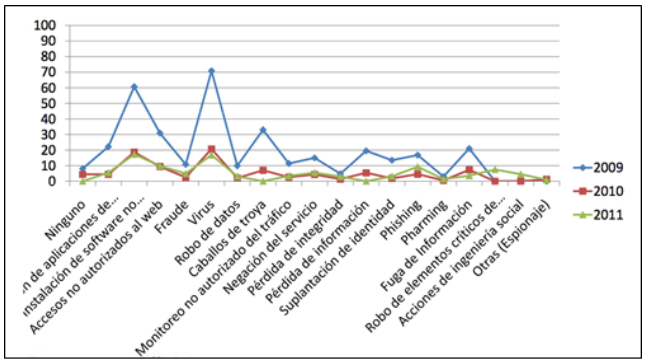

Fig. 1: Incidentes de seguridad [2]

En la Figura 2 se muestra el aumento en los niveles de inversión, durante los años de 2009, 2010 y 2011, que han hecho las empresas para mejorar la seguridad, lo cual se ha visto reflejado en la disminución de incidentes [2]. Para lograrlo se necesitó de una inversión en elementos de control que permitieran incrementar la seguridad en las organizaciones. Si se hace un buen análisis de las necesidades y de los riesgos tecnológicos, es posible optimizar los recursos para las necesidades según los requerimientos de la información a proteger.

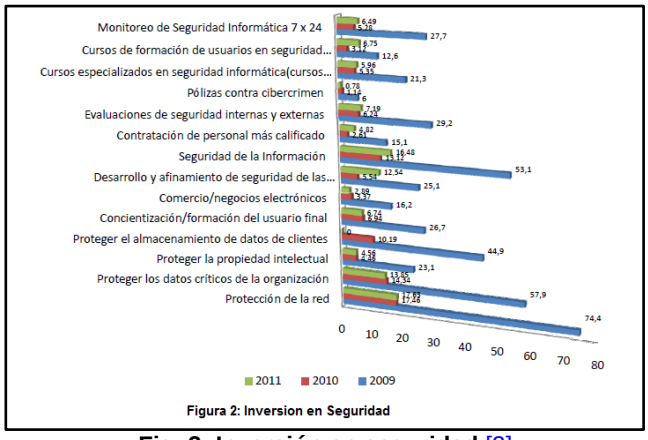

Fig. 2: Inversión en seguridad [2]

Los resultados de la encuesta muestran cómo las organizaciones han venido mejorando e invirtiendo en mecanismos y dispositivos para asegurar su información, mediante la implementación y uso de buenas prácticas en la protección y en controles de seguridad.

3. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

La identificación y análisis de riesgos es una metodología que se enfoca en cómo evitar o reducir los peligros asociados con la seguridad de la información. Para ello, es necesario realizar una evaluación cuidadosa de todos los factores internos y externos que intervienen o afectan los servicios de la organización.

Para tener un conocimiento de lo que se debe asegurar y tomar la mejor decisión en las herramientas, metodologías, o prácticas a utilizar, es importante hacer una evaluación consiente y profunda del riesgo. Lo primero es identificar los riesgos, es decir, recopilar todos los activos informáticos de la organización y seleccionar cuáles son los elementos críticos que pueden ser afectados por algún riesgo, la probabilidad de que ocurra y los costos que involucran. Luego, se identifican todas las amenazas informáticas, tanto internas como externas.

Al momento de hacer el análisis de riesgos, se toman las amenazas y se analizan con cada uno de los activos que se tiene; esto se evalúa por medio de una calificación de riesgos y con base en lo que afecta, el costo involucrado y el tiempo que se requiere para corregirlo. Posteriormente, se identifican los mecanismos para tratar los riesgos en cuanto a cómo reducirlos, evitarlos, mitigarlos o transferirlos. Estos mecanismos se implementan en diseños de seguridad, funcionalidades, políticas, configuraciones, monitoreo y seguimientos periódicos.

El principal objetivo de la evaluación de riegos es garantizar la supervivencia de la organización, minimizando las pérdidas de información y, sobre todo, garantizando el riesgo mínimo en cada elemento de red o software que se emplee para su protección [3]. Para ello se debe hacer el análisis de riesgos para identificar las vulnerabilidades del sistema, en qué riesgos se esta incurriendo y cómo mitigarlos.

Las empresas han venido utilizando un modelo *reactivo* al momento de presentarse un incidente que afecte su estabilidad tecnológica, lo cual genera re-procesos y que estos incidentes, al no ser medidos, alcancen un alto impacto en la continuidad del negocio. Uno de los problemas es que no manejan una base de datos de conocimiento que permita reconocer patrones de errores, lo que puede generar alertas tempranas para identificar oportunamente los incidentes de seguridad y que permitan crear indicadores de seguimiento en su resolución. Muchas de las pérdidas financieras en las organizaciones se deben a la falta de un adecuado control e implementación de políticas de seguridad [4].

Algunas organizaciones, al notar que tenían perdidas o que incurrían en riesgos por incidentes tecnológicos, optaron por la creación de equipos de trabajo especializados que se encargan de ellos. Estos grupos inter-institucionales se denominaron gerencias de continuidad del negocio o gerencias de manejo de

riesgos de TI y su principal objetivo es prevenir, mediante herramientas, que se generen datos medibles, valores estadísticos y valores históricos de los posibles riesgos, tanto a nivel físico o tecnológico, inherentes a la propia naturaleza del negocio.

Hoy en día con la integración e interconexión de infraestructuras, las organizaciones deben implementar métodos y técnicas que permitan mejorar esos controles de seguridad. Actualmente existen controles tecnológicos basados en software o en hardware, como firewalls, sistemas para detección y prevención de intrusos, sistemas de control de acceso, entre otros. Estos controles se deben integrar con las plataformas existentes en la organización y hacer un plan de divulgación a las demás áreas, de tal forma que toda la organización participe activamente para generar una cultura que permita cubrir los diferentes frentes de inseguridad o vulnerabilidades que se pueda tener [5].

En algunas organizaciones se tienen implementados procesos que deben ser re-ajustados a políticas y técnicas nuevas, con el objetivo de implementar una adecuada seguridad. El cambio de estos procedimientos puede generar inconformismo o rechazo por parte de los empleados o de las diferentes áreas de la empresa y, para evitarlo, se debe hacer un plan de concientización donde se expongan los riesgos en los que se esta incurriendo y sus posibles consecuencias [3].

Una organización, que no tenga implementada una base de conocimiento sobre incidentes y riesgos tecnológicos, se ve afectada repetitivamente por los mismos, debido a que no realiza una adecuada identificación y evaluación del riesgo que le permita medir el impacto que pueda legar ocasionar.

Conocer las vulnerabilidades e implementar procedimientos para combatirlos es importante, sin embargo, hasta ahora no se cuenta con medidas de seguridad que garanticen completamente una protección total. Por tal motivo es importante evaluar los métodos a utilizar para minimizar de manera sustancial los riesgos que se tienen en las organizaciones [6].

4. MODELO DE SEGURIDAD PROPUESTO

El modelo de seguridad expuesto a continuación, es la base para implantar una arquitectura de seguridad eficiente, invirtiendo en lo que se necesita y logrando así un retorno de la inversión a corto plazo. Para la implementación del modelo de seguridad se deben seguir los siguientes pasos:

1. Identificar y analizar los riesgos
2. Definir las políticas de seguridad
3. Diseñar la arquitectura de red

4.1 Identificar y analizar los riesgos

Lo más importante para poder iniciar con la implementación de un sistema de seguridad es tener claro qué se va a proteger. De este análisis se puede identificar los riesgos presentes en la organización y evaluar su impacto para establecer los controles y de esta manera mitigar los impactos más significativos.

4.2 Definir las políticas de seguridad

Desde la arquitectura de los sistemas de información se puede cuantificar fácilmente los riesgos. Este modelo puede cubrir aspectos gerenciales, operacionales o puramente técnicos y puede ser diseñado para evaluar el riesgo de seguridad asociado con diferentes arquitecturas de red, o para evaluar el impacto en las diferentes políticas diseñadas para la seguridad organizacional.

Las políticas de seguridad son una declaración de lo que se puede o no se puede hacer dentro de la empresa, por ello se debe contemplar, sin limitarse:

- El nombre del dueño de la política y que es el responsable de que se cumpla.
- El grupo de personas que deben acatarla.
- Enunciar la política, tener un procedimiento claro y un objetivo.
- Debe tener sanciones por el incumplimiento de las políticas, lo que le dará más validez.

4.3 Diseñar la arquitectura de red

Dentro del diseño de esta arquitectura se analizan factores como: identificación de requerimientos, desarrollo de la estructura de la red, aprovisionamiento de hardware, diseño de elementos de seguridad, implementación y monitoreo.

La *identificación de los requerimientos* se genera de acuerdo con las necesidades que surgen en la etapa de identificación y análisis de riesgos. En el *desarrollo de la estructura de red* se debe tener en cuenta la integración de los dispositivos con la arquitectura de seguridad, para lo cual se realizan dos subdivisiones, una que es hacia internet o redes externas y otra que es la red interna de la organización.

Es importante identificar los servicios más críticos para la organización, para ello se evalúa cuáles son los procesos más importantes, si los procesos internos o los procesos de cara a los clientes, como las páginas Web u otras herramientas. Después de esto se sabrá qué proteger, para lo cual se deben tener claros los conceptos de DMZ, o Zona desmilitarizada y MZ o Zona militarizada o red interna. La primera es la red que se utiliza para hacer las interconexiones a las redes externas. Todas las redes internas deben tener conexiones hacia redes externas a través de la DMZ y viceversa. La segunda, es aquella red donde se encuentran todos los elementos internos de las organizaciones y no requiere una conexión directa con las redes externas.

Estas dos zonas son las que existen en todo tipo de organización o red y que se deben asegurar. Con base en los resultados arrojados por el análisis de riesgo e identificada la zona esencial para el funcionamiento de

la organización, se debe implementar mayor inversión en la seguridad, sin descuidar la otra zona, la cual debe tener una protección básica. En la Figura 3 se muestra una topología básica de una red en la que se puede identificar las diferentes zonas.

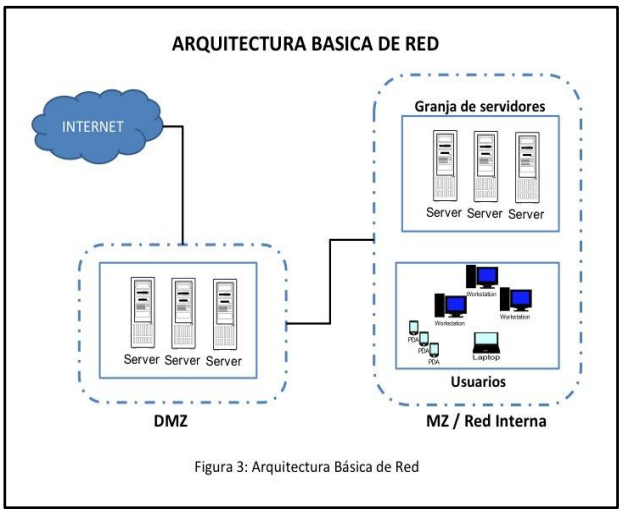

Fig. 3: Arquitectura Básica de Red

A continuación se describe el aseguramiento para cada una de las zonas y cómo realizar la protección interna para la MZ y la externa para la DMZ.

4.3.1 *Aseguramiento interno*

Para la red interna se habla de un diseño en el que incluya la red de todos los usuarios y las granjas de servidores, la protección de las conexiones de redes externas y de la red de usuarios y el flujo de datos que salen y entran. Es importante tener claridad en que no se debe establecer una conexión directa con las redes externas, pues ello genera vulnerabilidad en la infraestructura. Una arquitectura de seguridad básica y sencilla en una organización está conformada por un firewall, un enrutador o modem y la red interna.

Todas las redes poseen una DMZ y una MZ, algunas veces la primera no está bien identificada porque no se tienen servidores de cara a internet. En estos casos la DMZ es un modem que suministra el proveedor de internet (ISP), y la MZ es el resto de la red de la organización. Cuando se tiene un sitio web informativo se debe proteger con un firewall, porque a través de él se permite la comunicación entre la red interna y la externa. Es decir, todas las solicitudes que vienen desde y hacia internet. Es entonces cuando la DMZ se encarga de resolver las consultas Web, sin exponer la seguridad de la red interna en la que se encuentra la información de la organización.

El diseño de seguridad debe puntualizar la seguridad de la red interna, donde se realizará el análisis de los puntos críticos a proteger, y que cubre la granja de servidores, con todos los aplicativos y bases de datos de la empresa, al igual que la red de usuarios.

A continuación se listan algunos de los puntos claves que se deben tener en cuenta a la hora de implementar una red interna y de esta forma no comprometer la seguridad de la organización:

- No se puede hacer consulta directa a la red interna desde una red externa.
- Se debe implementar una solución de red que incluya segmentación y listas de control de acceso según los servicios de la organización:
  - Segmento de red para servidores.
  - Segmento de red para administración de dispositivos.
  - Segmento de red según los diferentes perfiles de usuarios:
    - Infraestructura o granjas de servidores.
    - Telecomunicaciones o dispositivos de red.
    - Monitoreo.
    - Áreas de trabajo (cada área debe estar en un segmento de red para control de privilegios).
    - Invitados.
- Perfilar la navegación y consultas a los aplicativos según segmentos de la red y usuarios.
- Navegación contralada por medio de proxy. Esta también es por perfiles de navegación.

Los elementos y dispositivos de seguridad son esenciales y se deben tener en cuenta en toda red:

Firewall. Es un enrutador programado que se ubica entre redes y que re-envía, direcciona y filtra flujo de datos que pasan de una red a otra, mediante reglas como direccionamiento, protocolos y puertos, entre otras [7].

Evita que los usuarios accedan a un host o a servicios específicos y ayuda a proteger la red de ataques como denegación de servicios [7]. Para la seguridad interna se recomienda montar un firewall en el perímetro de la red, con las reglas necesarias para la comunicación entre los segmentos.

En el mercado se encuentra gran variedad de ofertas, tanto en software como en hardware. Algunos, como Juniper Networks, Barracuda y Cisco son muy robustos y con capacidad para múltiples configuraciones tanto básicas como avanzadas. También existe el IPTABLES, que es gratuito y que permite diversas configuraciones. Para un tráfico moderado, es decir, para pequeñas y medianas empresas, éste es un firewall recomendado; es una herramienta software que se puede instalar en un computador en la red.

Enrutador. Es el punto donde se conectan dos o más redes [7] y se usa básicamente para la conexión a internet, pero también puede ser utilizado para separaciones de tráficos internos en organizaciones muy grandes. En una pequeña o mediana empresa se recomienda la implementación y configuración de un enrutador para la conexión con el proveedor o proveedores de internet y para el control del tráfico interno se puede utilizar un firewall. También se puede hacer por medio de switches, si soportan VLAN y listas de control de acceso.

Red Inalámbrica. Si se posee un servicio inalámbrico, es importante tener en cuenta que en estas redes se

conectan muchos dispositivos, como equipos móviles, portátiles y equipos de invitados, por esto se recomienda tener al menos dos redes inalámbrica, con el objetivo de separar la red de empleados, con sus segmentaciones respectivas, y la red de invitados. Esta última de debe configurar sólo con permiso de navegación y restringiendo también el perfil en el proxy. Adicionalmente se debe restringir el resto de servicios que se ofrece en la red de la organización. En la segmentación también se recomienda utilizar listas de control de acceso, para incrementar la seguridad en la red. Ambas redes deben tener contraseñas, las cuales deben ser diferentes.

Todas las redes inalámbricas deben tener configurado un cifrado, con el fin de garantizar la seguridad en las conexiones. En las redes inalámbricas internas se recomienda el WPA2 con AES para la autenticación de los usuarios y que estén configurados en un servidor RADIUS; para los usuarios externos o invitados se puede implementar WPA o WEP.

Red cableada. En esta infraestructura se recomienda restringir los puertos de los dispositivos de red a un número finito de conexiones de equipos; normalmente a un puerto sólo se conecta un equipo. Si existen áreas en la organización en las que se necesite una configuración diferente, se hace un estudio para implementar un número finito que pueda soportar las necesidades y que cumpla con la seguridad. Se recomienda utilizar *swhitches* que soporten listas de control de acceso y VLAN para la segmentación de la red, de acuerdo con los perfiles y permisos de los usuarios. En lo que tiene que ver con la administración y el monitoreo se recomienda hacer revisiones del consumo de la navegación y de los segmentos de la red, para evaluar un cambio no esperado y para detectar posibles ataques externos o acciones indebidas realizados por usuarios internos.

Antivirus. Es un elemento fundamental en las organizaciones. Es una herramienta para la que no se debe limitar o restringir la inversión, pues no tenerla puede traer costos muy altos como pérdida de información, suspensión de servicios de producción, entre otros. Se recomienda tener instalado el antivirus en cada uno de los equipos de la red y no olvidar que ciertos dispositivos móviles también lo necesitan.

Algunos de los antivirus más recomendados, de acuerdo con el sitio pcworld.com, son: Symantec Norton Antivirus, BitDefender Antivirus Pro, G-Data AntiVirus, Kaspersky Lab Anti-Virus, entre otros [8].

*IDS/IPS***.** Es un sistema usado para detectar intrusiones dentro de los sistemas de cómputo y redes [9]. El IDS, o sistema de detección de intrusos, es una herramienta que genera alertas de posibles ataques o incidentes en la red. Es recomendable utilizar más de uno, con el objetivo de poder generar alertas y hacer una correcta correlación de eventos después de ocurridos y para ver si fue una falsa alarma o un ataque. Para esto es importante hacer un monitoreo de alertas, porque sin esto sería una herramienta inútil y, en caso de nos ser posible, por lo menos tener programada una revisión periódica. Los sitios más recomendables para su instalación son: en la entrada de la red, ya que es por donde inician los ataques, en la red de usuarios y en la granja de servidores. Si hay más de una red de usuarios se debe implementar un IDS por cada red que existe en la organización.

Los IDS son un conjunto de reglas que detectan patrones de navegación y que se deben configurar de acuerdo con lo que se esté revisando; por ejemplo, si se revisa la red de usuarios con sistemas Windows, las reglas se deben configurar para este sistema. Es importante establecer las reglas que deben ir en cada uno de los IDS para disminuir el número de falsos positivos y para ayudar a la revisión de eventos.

Existen muchas herramientas para este fin, por lo que se debe analizar correctamente el tráfico que se va a procesar antes de elegir una de ellas. El SNORT es muy utilizado para pequeñas y medianas empresas y es un IDS muy robusto que tiene comunidades actualizando continuamente las reglas y que cada usuario puede implementar según el conocimiento que tenga y la necesidad de la organización. Es una herramienta gratuita.

Sistemas de monitoreo. Son herramientas para visualizar *logs* y eventos que, cuando se implementan con una herramienta de correlación de eventos, proporcionan información clave para la identificación de incidentes de seguridad. El costo para sostener una herramienta de éstas es alto, debido a que su mantenimiento que depende de días de monitoreo.

Dependiendo del objetivo de la empresa y del riesgo estudiado, se debe evaluar si es necesario implementar un sistema de monitoreo o no. Si no es muy crítico se recomienda, al menos, tener un registro de esta información para hacer una revisión periódica y hacerle ajustes al sistema. También se debe configurar el registro de *logs* y el envío de alertas en los dispositivos de red, con el fin de poder reaccionar a tiempo ante un ataque o evento inesperado.

Proxy. Es una herramienta que direcciona los requerimientos de los usuarios hacia internet, de tal forma que permite hacer controles en la navegación [9]. Esto ayuda en la seguridad al navegar en sitios no deseados, a evitar riesgos para la compañía y, además, se puede asignar puertos para la navegación y otros servicios a través de internet.

Existe gran variedad de proxy basados tanto en software como en hardware; algunos tienen licenciamiento por número de usuario, ancho de banda o equipos y otros que no tienen ningún costo, como el Squid, que es una herramienta versátil y robusta que posee gran número de funcionalidades como caché, filtrado de contenido, estadísticas de navegación,

definición de perfiles para usuarios o grupos de usuarios, perfiles de subredes, administración de ancho de banda, entre otras.

Controlador de dominio. Este sistema permite controlar y definir perfiles, permisos de acceso a los usuarios y autenticación de dispositivos de la empresa dependiendo del cargo o responsabilidades del empleado y de esta forma garantiza la seguridad de los sistemas. Gracias a esta herramienta se pueden administrar los perfiles de los usuarios y controlar todos los accesos a aplicativos, archivos, almacenamiento, entre otros elementos de la empresa. De acuerdo con los permisos se puede evitar la instalación de software no deseado, la realización de diferentes configuraciones de los equipos, entre muchas otras funcionalidades que ayudan a proteger la red.

VPN o Red privada virtual. Es una red lógica y segura que se establece sobre una red existente [7]. Su funcionalidad permite, solamente cuando es necesario, establecer conexiones remotas seguras hacia la red interna. Existen muchas herramientas para la configuración de una VPN, tanto en software como en hardware, igual que licenciadas o gratuitas.

4.3.2 *Aseguramiento externo*

En el aseguramiento de la red externa o DMZ se tienen los servidores que prestan servicios hacia Internet, los cuales están de cara al cliente, es decir, servidores de FrontPage, servidores de correo, FTP, entre otros. Son servidores que no se pueden cerrar a la visualización de personas en redes externas y, por tanto, se debe tener una protección diferente. Si el objetivo del negocio depende de estos servicios y si existen riesgos muy críticos en la DMZ, es de vital importancia proteger esta área, porque está expuesta en internet a todos los públicos. Los servidores que están ubicados en esta zona pueden ser vulnerados por los usuarios externos o empleados de la red interna. Con el fin de evitar posibles fallas de seguridad, se debe implementar una solución que garantice la protección de la red externa DMZ.

El diseño de seguridad para la red externa DMZ debe garantizar la disponibilidad sin vulnerabilidad y es necesario tener en cuenta los diferentes factores que se listan a continuación para su protección:

- Ofrecer una conexión directa a los servicios prestados en Internet.
- De cara al cliente debe haber una visualización de los servicios, pero no el aplicativo o el servidor directamente, es decir, deben pasar por un proxy reverso.
- Sólo deben estar disponible los puertos con los servicios ofrecidos.
- La administración estará restringida y sólo los administradores tienen acceso a la misma y se debe realizar desde sitios seguros o a través de una VPN.

Los elementos y dispositivos de seguridad que se recomienda instalar y configurar en una DMZ son: proxy reversos, firewall, VPN, antivirus y detección de intrusos.

Firewall. En este caso se utiliza para proteger la DMZ y para permitir la conexión administrativa sólo desde sitios seguros o de la MZ y la configuración de las conexiones a los servicios únicamente por los puertos deseados, bloqueando el resto. El firewall se debe configurar de tal forma que pueda registrar eventos relacionados con número de conexiones, intentos de conexiones, entre otras configuraciones que permitan identificar, controlar, administrar y prevenir posibles ataques, sean internos o externos.

Antivirus. Esta herramienta se instala con el fin de proteger la información que se despliega a los clientes o que llega a los servidores; debido a esto los antivirus se instalan en los equipos directamente o específicos para los servidores. El antivirus, además de proteger los servidores, protege a los usuarios que acceden a los aplicativos o servicios. Son esencialmente de red, o si se tiene un servidor Windows, instalar un antivirus adicional en él.

IDS/IPS. La implementación de estos dispositivos es igual a la de la red interna. Los IDS/IPS tienen reglas exclusivas para el funcionamiento de los servidores que varían dependiendo de los servicios ofrecidos y de los sistemas utilizados.

Sistemas de monitoreo. Su configuración es igual a la de la red interna. Los costos involucrados para un buen monitoreo se deben evaluar según la necesidad de la empresa, aunque es importante hacer revisiones periódicas y generar un sistema de alarmas de posibles ataques, consumo de recursos y disponibilidad de los servicios.

Servidores de despliegue o proxy. Para prestar los servicios a los clientes es recomendable usar servidores proxy reversos, porque estos sistemas trabajan haciendo un direccionamiento desde la DMZ a la MZ de forma segura, sin necesidad de tener directamente los aplicativos en la DMZ. También se puede trabajar el despliegue de la información y las consultas a los aplicativos por la red interna, las dos técnicas o la combinación de éstas ayuda a proteger tanto los aplicativos como la información.

VPN (Red privada virtual). Este tipo de conexión se utiliza para realizar la administración de los servidores o la conexión a la red interna. Cuando se habla de VPN en la red interna, la conexión se hace directamente desde la DMZ o desde Internet.

Switch. Para tener mayor seguridad estos elementos deben estar separados de los de la red interna y, para soportar el número de conexión que puede existir en internet, deben poseer una buena capacidad de tráfico.

5. BENEFICIOS DE LA IMPLEMENTACIÓN

Para implementar una buena arquitectura de seguridad en las organizaciones se debe pasar por la identificación y el análisis de riesgos, para conocer las necesidades y poder realizar un diseño de seguridad adecuado, cubriendo los requerimientos de seguridad y dejando a un lado las inversiones innecesarias que incrementan los costos de la seguridad. Se debe invertir en lo realmente sea necesario, se elegirán las herramientas adecuadas para ofrecerles a los clientes eficientemente y con mayor calidad los servicios y adquiriendo un nivel aceptable de prevención de los riesgos.

Es importante recordar, como se ha descrito en este artículo, que todas las herramientas o diseños son beneficiosos, siempre y cuando se haga una correcta evaluación de las diferentes herramientas ofrecidas en el mercado, antes de seleccionar la más adecuada para lograr mitigar los riesgos organizacionales. Las herramientas de bajo costo no siempre logran economizar, al igual que no siempre las de mayor costo son las de mejor funcionamiento. Puede ocurrir que las primeras no tengan un buen funcionamiento y se deba invertir nuevamente en otras, o que las segundas no cumplan las expectativas para las que fueron adquiridas. Por eso se debe tener claro el riesgo para el que se adquieren y si con ellas se llega a un nivel aceptable de protección para la organización.

Hay que recordar también que si se va a proteger información que genera una utilidad determinada al año, toda la organización necesita un equilibrio entre lo financiero y lo tecnológico y que si, por ejemplo, lo que se piensa utilizar para proteger ese activo cuesta más que la utilidad, no es viable invertir en esa herramienta, por esto es de gran importancia saber qué se va a proteger y los niveles aceptables para realizar la inversión.

5.1 Costo-beneficio

Para decidir si una herramienta o elemento de seguridad es necesario en una organización se requiere un buen análisis del riesgo. Ahora bien, si se analizan los virus informáticos en los equipos de la organización se puede observar que la probabilidad de ocurrencia es alta y que su impacto se evalúa por el tiempo que se perdió reparando el equipo, o por la información perdida debido a un daño en el mismo. Si se habla de un virus que se propagó por toda la empresa, el impacto sería desastroso; por lo tanto los controles en este caso sería un buen antivirus comercial, que garantice el control y unas políticas claras de manejo de archivos, ya sea desde internet o desde unidades de almacenamiento removibles. También hay que analizar lo contrario, es decir, si para un riesgo bajo con una probabilidad baja y un impacto casi nulo, es necesario invertir mucho tiempo y recursos en su protección.

Al evaluar el costo por la perdida de la información y el tiempo de indisponibilidad de los servicios, entre otras medidas, se puede obtener un mapa de riesgos para compararlo con los incidentes generados en el año inmediatamente después de estar protegidos y para sustentar las inversiones hechas y las futuras. Von este procedimiento se puede ver claramente el retorno de la inversión y por lo tanto el costo-beneficio.

6. RECOMENDACIONES

Para la implantación y puesta en marcha del modelo de seguridad propuesta se deben identificar y analizar los riesgos, definir las políticas de seguridad y diseñar la arquitectura de red. La siguiente lista enumera los pasos que se recomienda seguir para la implementación de una infraestructura segura:

- Identificar y analizar los riesgos.
  - Listar los activos.
  - Listar todas las amenazas de la empresa.
  - Cruzar los activos con las amenazas.
  - Generar tablas de probabilidad y la frecuencia con la que se va a medir.
  - Generar tablas de impacto: financiero, operacional, información (disponibilidad, confiabilidad, integridad), imagen de la organización, en el mercado o clientes.
  - Calcular el riesgo como la probabilidad de ocurrencia contra el impacto de que ocurra.
  - Evaluar la aceptabilidad y la inaceptabilidad.
  - Generar los controles.
- Definir políticas de seguridad.
- Diseñar la red.
  - Análisis de requisitos.
  - Arquitectura de la red.
  - Diseño de seguridad.
  - Aprovisionamiento e instalación de los elementos de seguridad y de la red.
  - Monitoreo y control de incidentes

7. CONCLUSIONES

En vista de la necesidad de tener un diseño de seguridad adecuado para la organización y un retorno de la inversión a corto plazo, se debe implementar un diseño de seguridad eficiente. Para esto es fundamental identificar y analizar correctamente los riesgos.

Al tener claro los riesgos más significativos y qué proteger, se puede implementar un diseño de seguridad sin necesidad de hacer inversiones en equipos que no se requieren, esto sin descuidar la protección para el buen funcionamiento de la organización.

No basta con implementar un buen sistema de seguridad que incluya a los controles, la arquitectura y las políticas, si no se realiza el seguimiento, el monitoreo y la evaluación a la solución implementada, porque las herramientas solas no hacen el trabajo. Por esto es importante la verificación continua y los ajustes que se puedan realizar.

8. REFERENCIAS

[1] C. A. Parra & H. Porras D. "Las amenazas informáticas: Peligro latente para las organizaciones actuales". *Gerencia tecnológica Informatica*, Vol. 6, No. 16, pp. 85-97, 2007.

[2] J. J. Cano et al. "III Encuesta Latinoamericana de Seguridad de la Información". Online, 2011.

[3] R. Bernard. "Information Lifecycle Security Risk Assessment: A tool for closing security gaps". *Computers & Security*, Vol. 26, No. 1, pp. 26-30, 2007.

[4] A. C. Johnston & R. Hale. "Improved Security through Information Security Governance". *Communications of the ACM*, Vol. 52, No. 1, pp. 126-129, 2009.

[5] W. T. Yue et al. "Network externalities, layered protection and IT security risk management". *Decision Support Systems*, Vol. 44, No. 1, pp. 1-16, 2007.

[6] B. Karabacak & I. Sogukpinar. "ISRAM: information security risk analysis method". *Computers & Security*, Vol. 24, No. 2, pp. 147-159, 2005.

[7] L. L. Peterson & B. S. Davie. "Computer networks: A systems approach". Morgan Kaufmann, 2011.

[8] N. Mediati. "Top 10 Paid Antivirus Programs for 2011". Online, 2011.

[9] J. M. Kizza. "Computer Network Security". Springer, 2010.