LA SEGURIDAD EN LAS REDES DE COMUNICACIONES

SECURITY IN COMMUNICATION NETWORKS

¿Cómo establecer la seguridad en una red?

"Principales aspectos a considerar"

[*]Ing. Jaime Alirio González

[**]Msc. Carlos Alberto Vanegas

Resumen

El propósito de este artículo es presentar algunas guías y políticas de seguridad que requiere una organización, con el fin de minimizar los riesgos a los que se encuentra expuesta la información durante el proceso de comunicación. Se tratan aquí los aspectos más relevantes que intervienen en la consecución de una red con unas políticas de seguridad claras con la intención de mantener seguros los datos durante el proceso de emisión, transporte y recepción.

Palabras Clave: amenaza, vulnerabilidad, riesgo, activo, plan de seguridad, política de seguridad

Abstract

The purpose of this article is to present some guides and safety policies that an organization requires, in order to minimize the risks to which the data are exposed during a communication process. The most

[*] Ingeniero en Redes de Computadores, Universidad Distrital Francisco José de Caldas. Administrador de los Laboratorios de Informática de la Facultad Tecnológica. jagonzalezg@udistrital.edu.co

[**] Ingeniero de Sistemas, Universidad Incca de Colombia, Especialista en Ingeniería de Software, Universidad Distrital Francisco José de Caldas, Magíster en Ingeniería de Sistemas, Universidad Nacional de Colombia, docente tiempo completo de la Universidad Distrital Francisco José de Caldas adscrito a la Facultad Tecnológica. cavanegas@udistrital.edu.co

relevant aspects intervening in the attainment of a network with clear safety policies are considered here, in order to keep secure the data during the process of emission, transport, and reception.

Keywords: threatens, vulnerability, risk, active, safety plan, safety politics

1. Introducción

La información es una herramienta útil en la toma de decisiones de una organización, por su valor incalculable, es necesario protegerla. Con el avance de la tecnología que cada día se perfecciona, específicamente en el campo de las comunicaciones y con la capacidad del computador para comunicarse con otros dispositivos remotos y para comunicar entre si computadores físicamente separados en los que llamamos una red de transmisión de datos, la cual es importante en el diseño de muchos sistemas de información. Pero esta información si no esta debidamente protegida cuando se realiza el proceso de transmisión de datos puede generar perdidas costosas e importantes a diversas organizaciones, lo que generaría riesgos e incertidumbre en la exactitud de la información, por esto es muy importante desarrollar políticas de seguridad claras con la intención de mantener seguros los datos durante el proceso de emisión, transporte y recepción.

2. Seguridad de la información en la Red

Se puede entender la seguridad como la necesidad de proteger. En una red se deben proteger todos los equipos que posibilitan el proceso de la comunicación, las personas que producen, acceden y distribuyen los datos y finalmente la información que es considerada como uno de los activos más

importantes de las organizaciones[1]. Para mantener segura la información que viaja a través de la red esta debe cumplir con tres requisitos:

- **Integridad**: Requiere que los recursos sean modificados por quienes están autorizados y que los métodos y los procesamientos de la información sean salvaguardados en su totalidad y con exactitud.
- **Confidencialidad**: Se debe garantizar que la información sea accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación
- **Disponibilidad**: Se requiere que la información esté disponible en el momento exacto para quienes están autorizados a acceder a ella.

2.1. Ataques a la seguridad de la red

Dentro del proceso de comunicación existen dos tipos de ataques a la red de transmisión de datos a saber [9]:

- **Ataques pasivos**: Son oidores o monitoreos de las transmisiones. El objetivo de quienes realizan ese tipo de ataque es obtener la información que se esta transmitiendo. En este tipo de ataque se pueden encontrar:
    - **Divulgación del contenido de un mensaje**: es un tipo de ataque pasivo por medio del cual el atacante se entera de la información transmitida; como por ejemplo escuchar una llamada telefónica, leer un correo electrónico abierto.
    - **Análisis de Tráfico**: Este tipo de ataque pasivo se realiza cuando el atacante puede determinar la localización e identidad de quienes se están comunicando y determinar el mensaje que esta siendo transmitido aun cuando este protegido por medio de cifrado.
- **Ataques activos**: Suponen modificación de los datos o creación de flujos de datos falsos. Dentro de este tipo de ataques se pueden encontrar:

[1] Norma ISO 17799

- **Enmascaramiento**: Es un tipo de ataque activo que tiene lugar cuando una entidad pretende suplantar a otra para obtener información confidencial.
- **Repetición**: Se realiza con la captura de unidades de datos que se vuelven a retransmitir para producir efectos no autorizados.
- **Modificación de Mensajes**: Se modifican los mensajes para producir efectos no autorizados.
- **Denegación de Servicios**: Previene o inhabilita el uso normal de las facilidades de comunicación, usualmente se hace para obtener un fin especifico o para obtener perturbaciones sobre la red desmejorando su rendimiento o incluso inhabilitando la misma.

2.2. Herramientas de seguridad

Existen métodos o herramientas tecnológicas que ayudan a las organizaciones a mantener segura la red. Estos métodos, su utilización, configuración y manejo dependen de los requerimientos que tenga la organización para mantener la red en un funcionamiento óptimo y protegido contra los diferentes riesgos [1]. Los más utilizados son:

Autenticación: Identifica quien solicita los servicios en una red. Esta no hace referencia solo a los usuarios sino también a la verificación de un proceso de software.

Autorización: Indica que es lo que un usuario puede hacer o no cuando ingresa a los servicios o recursos de la red. La autorización otorga o restringe privilegios a los procesos y a los usuarios.

Auditoria: Para analizar la seguridad de una red y responder a los incidentes de seguridad, es necesario hacer una recopilación de datos de las diferentes actividades que se realizan en la red, a esto se le llama contabilidad o auditoria. Con normas de seguridad estrictas la auditoria debe incluir una bitácora de todos los intentos que realiza un usuario para lograr conseguir la autenticación y autorización para

ingresar a al red. También debe registrarse los accesos anónimos o invitados a los servidores públicos, así como registrar los intentos de los usuarios para cambiar sus privilegios.

Cifrado: Es un proceso que mezcla los datos para protegerlos de su lectura, por parte de otro que no sea el receptor esperado. Un dispositivo de cifrado encripta los datos colocándolos en una red. Esta herramienta constituye una opción de seguridad muy útil, ya que proporciona confidencialidad a los datos. Se recomienda el cifrado de datos en organizaciones cuyas redes se conectan a sitios privados a través de Internet mediante redes privadas virtuales.

Filtros de paquete: Se pueden configurar en routers[2] o servidores para rechazar paquetes de direcciones o servicios concretos. Los filtros de paquete ayudan a proteger recursos de la red del uso no autorizado, destrucción, sustracción y de ataques de denegación del servicio. Las normas de seguridad deben declarar si los filtros implementan una de las siguientes normas:

- Denegar tipos específicos de paquetes y aceptar todo lo demás
- Aceptar tipos específicos de paquetes y denegar todo lo demás.

Firewalls[3]: Es un sistema o combinación de sistemas, que exige normas de seguridad en la frontera entre dos o más redes.

Vlan: En una red LAN se utilizan los switches[4] para agrupar estaciones de trabajo y servidores en agrupaciones lógicas. En las redes, las VLAN se usan para que un conjunto de usuarios en particular se encuentre agrupado lógicamente. Las VLAN permiten proteger a la red de potenciales problemas conservando todos los beneficios de rendimiento.

Detección de Intrusos: Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos

---

[2] Un **router** (*enrutador*) es un dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI.

[3] Un **firewall** (cortafuegos), es un elemento de hardware o software utilizado en una red de computadores para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.

[4] Un **switch** (conmutador) es un dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

pueden utilizar debilidades en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autenticación. . Una intrusión significa:

- Acceder a una determinada información.
- Manipular cierta información.
- Hacer que el sistema no funcione de forma segura o inutilizarlo.

2.3. Activos

Un activo es todo aquel elemento que se encuentra inmerso en el proceso de la comunicación. Desde la misma información, el emisor, el medio y el receptor, como en la economía, también en la seguridad de una red. Estos activos poseen un valor para la organización, en mayor o menor medida, más o menos relevantes en el proceso. Son tres los elementos denominados como activos en el proceso de la comunicación [8]:

- **La información**: todos los datos que se encuentren en cualquiera de las presentaciones.
- **Los equipos**: el hardware, el software, e infraestructura organizacional que permite el trasporte de los datos
- **Las personas**: producen, distribuyen y acceden a la información.

2.4. Vulnerabilidades y Amenazas

Los activos en una red a menudo contienen fallas o huecos en la seguridad. Estos huecos o vulnerabilidades desembocan en un problema de seguridad y representan un riesgo para los activos. Una amenaza es cualquier evento de seguridad capaz de utilizar una vulnerabilidad para atacar o dañar un activo [7]. Las amenazas se pueden dividir en tres grupos:

- **Naturales**: cualquier evento de seguridad producido por un fenómeno como terremoto, incendio, inundación, etc.

- **Intencionales**: eventos de seguridad causados deliberadamente sobre un activo con la firme intención de causar daños o perdida, fraudes, etc.
- **Involuntarias**: eventos de seguridad producidos accidentalmente

2.5. Riesgos y medidas de seguridad

Un riesgo es la probabilidad de que ocurra un evento en contra de la seguridad de la red o uno de sus activos causando daños o pérdidas. Un análisis de riesgos permitirá a la organización especificar cuales riesgos son más probables de ocurrencias, cuales serán más destructivos y cuales serán los más urgentes de minimizar. Las medidas de seguridad son las acciones que toma una organización para disminuir los riesgos de seguridad [10]. Las medidas de seguridad se dividen en:

- **Preventivas**: son las medidas que tienden a disminuir el riesgo de que una amenaza ocurra antes de producirse.
- **Perceptivas**: estas medidas consisten en realizar acciones que revelen riesgos no detectados.
- **Correctivas**: son las medidas que se toman cuando ha ocurrido una amenaza.

2.6. Políticas de seguridad

Las políticas de seguridad son los lineamientos y formas de comunicación con los usuarios, que establecen un canal de actuación en relación a los recursos y servicios de la red. Esto no significa que las políticas sean una descripción técnica de mecanismos y tecnologías de seguridad específicas y tampoco términos legales que impliquen sanciones. Las políticas son una descripción de lo que se desea proteger y la razón por la cual debe hacerse. Estos lineamientos deben abordar aspectos como la evaluación de los riesgos, protección perimétrica, control de acceso, y normas de uso de Internet y correo electrónico, protección contra virus y copias de seguridad entre otros [8].

3. Análisis de seguridad de la red

3.1 Identificar los activos de la red

Para identificar los activos de una red se deben tener en cuenta los diferentes tipos de activos que se encuentran en ella [8]:

- **Los equipos:** son todos aquellos elementos de hardware que hacen posible la comunicación de datos en la red y la infraestructura de la misma. Identificar estos equipos de acuerdo a sus características como equipos activos y pasivos es determinante a la hora de valorar el riesgo al que se encuentran expuestos cada uno de estos activos. Entre estos equipos se tienen terminales de usuario, switches, routers, centrales telefónicas, firewalls, etc. Cada uno de estos tiene unas características específicas y una funcionalidad en la red que determinan su importancia y el impacto que produciría un fallo en alguno de estos equipos. Por ejemplo, la mala configuración del firewall de la red permitiría el acceso a servicios no autorizados para empleados o personas externas a la red accediendo a información a la que no se encuentran autorizados, también el firewall permitiría el paso de virus o software malicioso capaz de atacar a los diferentes tipos de usuarios y su información.
- **El software**: se debe tener un control con el software debido a que en aplicaciones se pueden encontrar huecos de seguridad por donde se pueden producir ataques que se propagan al resto de la red como virus y accesos a puertas traseras o puertos abiertos que deja algún tipo de software y especial cuidado con las aplicaciones de uso abierto que en la mayoría de casos no presentan ningún control y menos un soporte adecuado. En aplicaciones de uso específico en la organización se debe tener en cuenta el tipo de información que esta suministra, procesa y distribuye y quienes tienen acceso a ella.
- **El personal**: se debe identificarse como un activo debido a que son quienes ejecutan los procesos para mantener la continuidad del negocio y son quienes tienen acceso a la red y a su

información con mayor o menor restricción. Determinar que tipos de permisos tienen cada usuario y grado de confianza que representa un empleado en la organización ayudará a que las medidas de seguridad sean más de tipo preventivo que correctivo. Un empleado de un departamento de ventas que tiene permiso para acceder a la nómina y cambiar los datos de salario representaría una amenaza de seguridad o un mensajero que tiene acceso a la información específica de un nuevo producto podría entregar esa información a la competencia generando así una fuga y una falla de seguridad.

- **La información**: debe clasificarse de acuerdo al nivel de importancia que representa en la continuidad del negocio. Los niveles de clasificación de la información determinarán el grado de protección al que esta debe estar sometida y quien o quienes pueden tener acceso a ella. No tendría efectividad proteger a los diferentes activos de la red si la información que por ella viaja esta expuesta a cualquiera que quisiera acceder a ella.

3.2 Análisis de riesgos

Existen diferentes métodos de análisis de riesgos de seguridad. Métodos cuantitativos y métodos cualitativos. El uso de uno u otro depende de la organización y la efectividad que cada uno de estos representa [10].

En un enfoque cuantitativo se calculan las perdidas en valor monetario que generaría la ocurrencia de un evento de seguridad, es decir, una amenaza. En esta metodología se toman los valores de los activos como punto de partida, los costos que generaría una falla de estos activos para solucionar un problema y las perdidas que representan para la organización. Un activo puede contener varios riesgos implícitos, cada uno con unas consecuencias, medidas de pérdidas y costos totalmente diferentes. En este orden, para cada riesgo en el que se encuentre un activo es necesario calcular los distintos costos que se generan por la acción de un evento de seguridad, lo que en una organización donde la cantidad de activos es considerablemente alta, este enfoque resultaría más dispendioso y menos factible de realizar,

puesto que, la cantidad de recursos humanos y de tiempo en el que la totalidad de cálculos se pueden realizar es cada vez mayor, y con el paso del tiempo un activo puede ir perdiendo su valor lo que significaría que al final de todos los cálculos estos ya no serian de utilidad o estarían erróneos para un instante determinado. En una evaluación de riesgos cualitativa, no se asignan los valores monetarios a los activos y tampoco se relacionan sus costos en cuanto a la ocurrencia de un evento de seguridad. En este enfoque, mediante un estudio cuidadoso, se priorizan los activos asignándoles un valor relativo de acuerdo a la función que cumplan dentro de la red de la organización. En este método se hace necesario que los clientes internos de la organización participen en forma directa en el proceso. Para tal fin, por medio de encuestas que permitan determinar el valor relativo de los activos se hace más sencilla una aceptación de la importancia de cada activo para la organización y los riesgos a los que se encuentra expuesto.

La finalidad especifica del análisis de riesgos, en cualquiera de los enfoques, cuantitativo, cualitativo o híbrido, es dar prioridad a los riesgos que mayor impacto causarían en la organización para así determinar cuales controles son más importantes implementar.

3.3. Matriz de control

Una matriz de control[5] es un sistema que nos permite priorizar riesgos. Los campos que se deben considerar para generar la matriz de control son:

- **Activo**: Corresponde al activo determinado en el estudio.
- **Amenaza**: Evento en contra de la seguridad
- **Consecuencia**: Efecto que causaría la ocurrencia de la amenaza.
- **Probabilidad de ocurrencia**: Es la probabilidad estimada de que ocurra una amenaza. El valor se encuentra entre 0 y 1.
- **Impacto**: Efecto que causa un evento de seguridad en la organización con respecto a perdidas[6] y los traumas a los procesos. De acuerdo con la guía de Administración de Riesgos de Seguridad

[5] Metodología de diseño de redes de Fitzgerald
[6] tangibles o intangibles

de Microsoft [7] cada uno de los activos tiene un valor específico de importancia dentro de la red que permite valorar su jerarquía. Con este valor se puede determinar el impacto que causaría la ocurrencia de un evento sobre el activo. Para la matriz de control la organización podría modificar este rango, que para Microsoft se encuentra en 0 y 5, al rango entre 0 y 10, siendo 0 el valor menos importante que se puede asignar a un activo y 10 el mayor.

- **Capacidad de reacción**: es la rapidez para resolver un problema que se presenta al ocurrir un evento de seguridad de acuerdo al criterio propio, ya que depende de los recursos humanos, físicos, operativos y económicos de la organización. El rango se encuentra entre 0 y 10, siendo 0 la mínima y 10 la mayor capacidad de solucionar un problema.
- **Vulnerabilidad**: es el estado en el que se encuentra un activo con respecto a una amenaza y corresponde un valor calculado así:

Vulnerabilidad = Probabilidad de Ocurrencia * Impacto

Figura 1. Matriz de control

ITEM	ACTIVO	AMENAZA	CONSECUENCIA	PROB. DE OCURRENCIA	IMPACTO	CAPACIDAD DE REACCIÓN	PROB * IMPACTO
1	Servidor DHCP	DAÑO	CAIDA DE LA RED	0,3	10	2	3
		DESCONFIGURACION	CAIDA DE LA RED	0,7	10	4	7

Fuente: autores

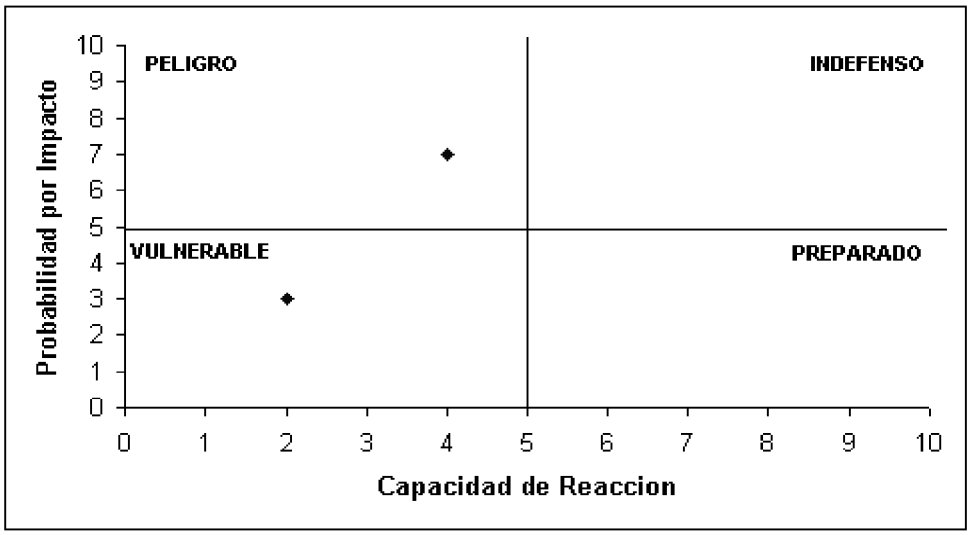
3.4. Estimación de la Vulnerabilidad

La matriz de control permite estimar los grados de vulnerabilidad con el fin de priorizar los riesgos que requieren de controles más rápidos y efectivos para determinar las acciones de seguridad adecuadas y .la implementación de controles a fin de brindar protección contra dichos riesgos. El proceso de estimación de la vulnerabilidad en el método utilizado se realiza con los datos de probabilidad de ocurrencia, impacto y capacidad de reacción con el fin de dar un valor cuantificable que permite a su vez dar el grado de vulnerabilidad que puede corresponder a uno de cuatro estados: Peligro, indefenso, vulnerable y preparado [2].

- **Peligro**: es el estado más critico que indica que el riesgo es inminente y sucederá, en cuyo caso la capacidad de reacción para superar el evento de seguridad es muy baja lo que causará grandes traumas y perdidas. En este estado los controles deben ser rigurosos para cambiar a otro estado menos crítico.
- **Indefenso**: indica que al presentarse un evento de seguridad será difícil reaccionar para salvaguardarlo debido a que la inexistencia de controles y políticas sobre estos riesgos dificultan el proceso.
- **Vulnerable**: es un estado de mucho riesgo y cuidado que indica que la capacidad de reacción en caso de suceder un evento de seguridad es relativamente baja y deben aplicarse controles con el fin de evitar que su estado se vuelva peligro.
- **Preparado**: es un estado que se podría llamar ideal siempre y cuando los controles y políticas de seguridad que se apliquen sean continuos y ayuden a mantener siempre controlados los riesgos.

El gráfico de mapa de ocurrencias se genera colocando cada resultado de probabilidad por impacto en el eje Y, enfrentado a la capacidad de reacción en el eje X. El mapa se divide en cada uno de los estados de vulnerabilidad, en donde cada resultado queda colocado en un punto del plano. En el ejemplo realizado anteriormente y que se muestra en la figura 1, se consiguieron dos resultados. Estos resultados se grafican de acuerdo a los parámetros del mapa de ocurrencias dando así como resultado la priorización de los riesgos a los que cada activo se encuentra expuesto.

Grafica 1. Mapa de Ocurrencias



Fuente: Autores

3.5 Requisitos de la seguridad

Con la priorización de riesgos, la organización ya está en capacidad de determinar cual son los requisitos que necesitan para llevar a cabo un plan de contingencia a fin de minimizar los riesgos y en que aspectos debe tener mayor énfasis. Dentro de los requisitos a tener en cuenta están:

- **Entrenamiento a los usuarios en cuanto a las normas, procedimientos y objetivos de acceso a la red**: Este entrenamiento permitirá disminuir las vulnerabilidades propias al factor humano que corresponden a un gran porcentaje dentro de los riesgos en las organizaciones.
- **Protección de los equipos de la red**: Permiten disminuir las vulnerabilidades propias del factor tecnológico.
- **Procedimientos**: permiten mantener minimizados los riesgos a los que la organización se expone con sus activos.

Teniendo en cuenta estos tres factores, se debe determinar el plan de seguridad y las políticas respectivas, que permitan disminuir las vulnerabilidades y fortalecer los estados ideales de los riesgos a los que se encuentran expuestos los activos de la red.

4. Controles

4.1. Plan de seguridad

Un plan de seguridad debe contemplar diferentes aspectos acerca de cómo se mantendrá la seguridad en la red [6]. Este plan debe contener:

- **Tiempo, Gente y Recursos**: Un plan de seguridad debe ejecutarse de forma permanente. No existe un tiempo limitado o especifico para ejecutar una asignación de esta política, puesto que el mejoramiento en la prestación de los servicios y minimización de las amenazas a la seguridad debe realizarse de forma continua. Se contemplan en este plan los servicios que presta o deberá prestar la red teniendo en cuenta que estos pueden cambiar, aumentar o en caso dado disminuir por la entrada de nuevos servicios, lo que implica que las políticas de seguridad que se desprendan de este plan puedan cambiar a medida que los servicios cambien. La puesta en marcha de este plan de seguridad dependerá de la apropiación que hagan de este todos los involucrados en su desarrollo, uso y beneficiarios del mismo.
- **Topología de la red y servicios**: Un plan de seguridad debe contener de manera detallada la topología de la red, explicación de los servicios que la red presta tanto a usuarios internos como externos, detalles de dependencias y tecnologías de comunicación.
- **Especificación de Funciones**: Las funciones de los usuarios deben estar bien especificadas con el fin de dar responsabilidad a cada uno en los procesos que le son pertinentes en cuanto a la seguridad de la red. Estas funciones deben desprenderse de las políticas generadas a partir de este plan y deben contemplar procesos de actuación concreta de cada uno de actores. Se deben especificar: recursos y procesos asignados a cada usuario, definición de niveles de autorización o permisos, responsabilidades específicas y tipos de usuarios.

4.2. Políticas de seguridad.

No todas las organizaciones desean llevar a cabo una certificación en procesos de seguridad de la información, pero si todas, desean protegerse y proteger sus activos. La norma ISO 17799 contempla varios parámetros en los cuales se especifican de manera general un punto de partida para lograr el objetivo. Basados en la norma se producen las políticas de seguridad para la organización, cuyo fin es generar la base de normas mínimas para el correcto desempeño en la prestación de servicios a los involucrados en el uso de la red con un mínimo de seguridad que otorgue a los usuarios la confidencialidad, integridad y disponibilidad de información que ellos necesitan. La apropiación de estas políticas debe ser hecha por parte de todos los usuarios que acceden a servicios en la red de la organización, pues de su universalización depende la disminución de riesgos y vulnerabilidades a los que la red se encuentra expuesta. Se contemplan en estas políticas los aspectos básicos de seguridad en cuanto a comunicaciones se refiere, cuyo objetivo principal es garantizar el funcionamiento correcto y seguro de las instalaciones de la red:

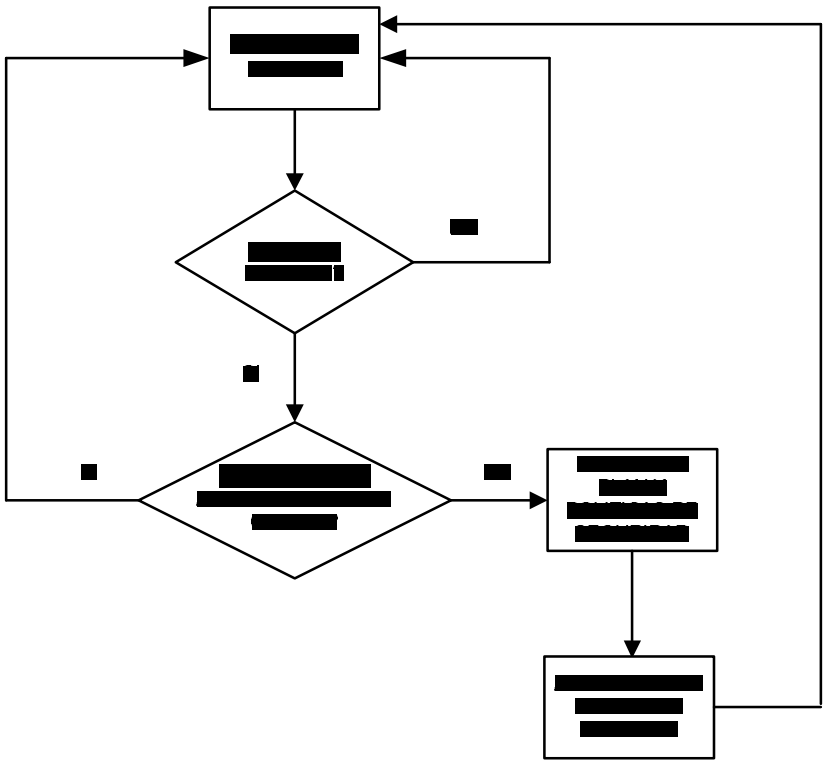
- Procedimientos y responsabilidades.
- Planificación de la capacidad y aprobación de nuevos accesos o servicios en la red.
- Protección contra software malicioso.
- Mantenimiento de la información y servicios.
- Administración de red.
- Medios de almacenamiento.
- Intercambio de información.
- Control de accesos.

El seguimiento de las políticas y la consecución del plan de seguridad es responsabilidad no solo de los administradores de red, sino de todo aquel que tenga acceso a los servicios de red en mayor o menor medidas sin importar tipo de usuario, servicio o tiempo de uso del mismo.

4.3. Revisiones y actualizaciones de las políticas de seguridad

El plan de seguridad y las políticas generadas a través del mismo deben mantenerse acordes a los cambios de personal, tecnológicos y de procedimientos propios de la red con el fin de minimizar los riesgos que se pudieran generar debido a estos cambios. Por esta razón la gestión de seguridad debe mantenerse al tanto de cualquier evento ocurrido sobre la infraestructura de red que ocasione un cambio significativo. La gestión de seguridad no es solo deber de los administradores de la red o de los coordinadores. Desde el nivel más alto de administración de la organización hasta los usuarios menos concurrentes en los servicios de red se deben apropiar de este plan y políticas con el fin de generar nuevas revisiones, pautas de cambio y actualizaciones.

Figura 2. Proceso de actualización de políticas



Fuente: autores

4.4. Etapas de la implementación

Pueden existir diferentes formas de implementación del plan y políticas de seguridad. Aquí se presenta una forma sencilla con unos pasos muy específicos para llevar a cabo una implementación por etapas:

ETAPA 1 – INICIO: El objetivo de esta etapa es asignar la duración de la implementación y determinar los actores encargados de dirigir y gestionar el plan de seguridad y sus políticas. En esta etapa deben asignarse los roles y responsabilidades de cada uno de los participantes en el proceso de implementación. También debe definirse el director del proyecto, el auditor del proyecto, los responsables de implementación operativa, los encargados de capacitación usuarios. Además se deben definir los tiempos reales que aseguren una implementación limpia sin contratiempos o traumas a las actividades de la organización. Este punto es de vital importancia, ya que es la base para superar las etapas posteriores.

ETAPA 2 – INSTALACIÓN: Durante esta etapa se instalan los componentes tecnológicos necesarios para la consecución del proyecto, tales como, cableado, switches, routers, servidores, firewall, etc.
El consultor debe verificar que los requerimientos básicos, necesarios para un adecuado funcionamiento del sistema, sean cumplidos. El sistema será entonces instalado y se realizarán una serie de pruebas cuyo objetivo es asegurar el correcto funcionamiento de la solución.

ETAPA 3 – CAPACITACIÓN OPERATIVA: El entrenamiento de esta etapa cubre en un alto nivel las principales características del modelo de seguridad, explora el alcance de la solución, los documentos a utilizar y refuerza la metodología a emplear, con el fin de tener una base sólida para el desarrollo de la siguiente etapa.

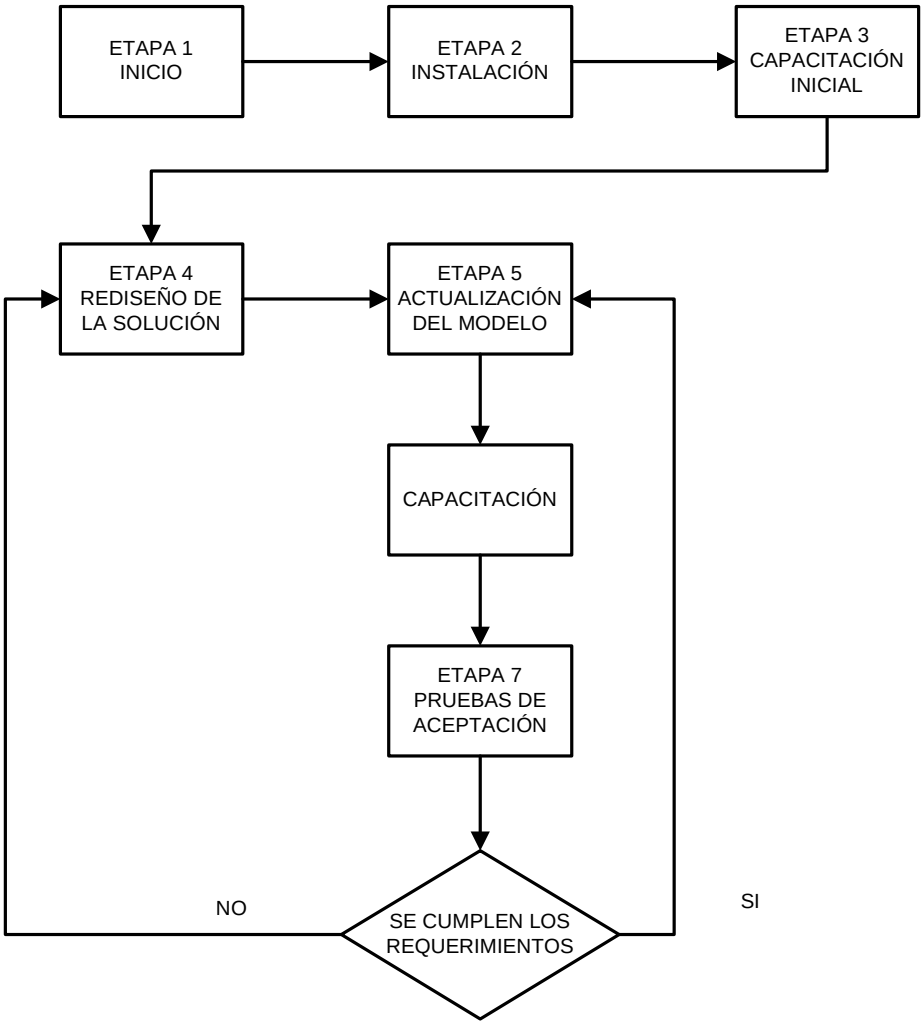
ETAPA 4 – REDISEÑO DE LA SOLUCIÓN: El proceso se basa en la toma de decisiones sobre como el modelo de seguridad debe integrarse a la organización y como debe ser dispuesto o modificado para cumplir con los requerimientos de los usuarios. Todos los nuevos requerimientos deben ser documentados y deben ser conocidos por los implicados con el fin de realizar las modificaciones al plan y a las políticas de seguridad. en caso de encontrar que estos requerimientos no se encuentran plasmados en las mismas.

ETAPA 5 – ACTUALIZACIÓN: Basados en la documentación tomada de la etapa anterior, el equipo de implementación incluirá los cambios necesarios que deban realizarse agregando nuevos parámetros al plan como diseño de seguridad, nuevas políticas, modificar las existentes, etc., documentando de nuevo los cambios necesarios.

ETAPA 6 – CAPACITACIÓN A USUARIOS: Durante esta etapa se capacita a todos los usuarios del nuevo sistema, su alcance y funcionalidades, derechos de los servicios, restricciones a los mismos y ventajas para el desarrollo de las actividades y minimización de riesgos de seguridad.

ETAPA 7 – PRUEBAS DE ACEPTACIÓN: Los usuarios, de acuerdo a un tiempo acordado, deberán hacer uso del sistema con un objetivo específico: verificar sí este cumple con los requerimientos necesarios y es aceptado de manera parcial o total con el fin de hacer retroalimentación y realizar las modificaciones necesarias.

Figura 3. Metodología de implementación



Fuente: autores

5. Conclusiones

- La información de una organización por tener un valor incalculable es necesario protegerla contra las diferentes amenazas a las que se encuentra expuesta, examinando las vulnerabilidades y minimizando los riesgos.
- Para mantener un buen funcionamiento de la red y protegerla contra los diferentes riesgos es necesario que existan herramientas de autenticación y autorización de usuario para el ingreso a al red. Como también el cifrado de la información que viaja por la red.

- Un análisis de riesgos de los activos de una red permitirán a la organización especificar cuales riesgos son más probables de ocurrencias, cuales serán más destructivos y cuales serán los más urgentes de minimizar.
- Las políticas de seguridad de la red deben abordar los aspectos de evaluación de riesgos y los controles de acceso.
- La organización debe estar en la capacidad de determinar cuales son los requisitos que se necesitan para llevar a cabo un plan de contingencia a fin de minimizar los riesgos.
- Se deben generan políticas de seguridad con unas de normas mínimas para el correcto desempeño en la prestación de servicios a los involucrados en el uso de la red que otorgue a los usuarios la confidencialidad, integridad y disponibilidad de información que ellos necesitan.
- El plan de seguridad y las políticas se deben revisar continuamente para detectar nuevas y posibles amenazas en la red.

Bibliografía

[1] CISCO SYSTEMS, Guía del 2do año CCNA 3 y 4, páginas 805-810, tercera edición.

[2] FITZGERALD Jerry, Dennis Alan, Business Data communications and networking", eighth edition, chapter 11, page 354, Jhon Wiley & Sons, 2006.

[3] INSTITUTO ARGENTINO DE NORMALIZACIÓN, Esquema 1 de Norma IRAM-ISO IEC 17799, Buenos Aires.

[4] STALLINGS William. Comunicaciones y redes de Computadoras, Sexta Edición, Madrid, Prentice Hall. 1997.

[5] TANENBAUM, Andrew. Redes de Comunicaciones, Tercera Edición. México, Prentice Hall. 1995.

[6] TOP-DOWN NETWORK DESIGN CISCO, Fundamentos de comunicación de datos, Bussiness Data Comunications and Networking.

Infografía

[7] Academia latinoamericana de seguridad informática, Microsoft Technet
www.mslatam.com/latam/technet/cso/html-es/home.asp

[8] Academia latinoamericana de seguridad informática, curso de seguridad informatica
www.mslatam.com/latam/technet/cso/html-es/frontedn/users

[9] Amenazas a la seguridad.
www.iec.csic.es/criptonomicon/seguridad

[10] Guía de administración de riesgos de seguridad de Microsoft
www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx