	FASE 1 **Objetivo** En esta semana estudiaremos de manera general qué es un modelo de comunicación, cuales son las características principales de las redes, y qué son las políticas de seguridad informática.

	REDES Y MODELO OSI **Objetivos del tema** • Conocer de manera general los protocolos de comunicación • Identificar el modelo OSI y los diversos tipos de redes. • Conocer la "capa 8" y la necesidad de generar políticas de seguridad informática (PSI) • Definir qué es una política de seguridad informática y por qué es necesaria para una organización.

REDES Y MODELO OSI

Transmisión de información:

La característica principal de los seres humanos es que son entes comunicativos. En todo momento están interactuando entre sí para poder vivir de una manera organizada y eficiente para la mayor parte de elementos de la sociedad. Esta comunicación permite decirles a otras personas nuestros deseos, órdenes, emociones, o para comunicarle datos de utilidad para el otro o para varias personas. Permite también trabajar en conjunto para alcanzar un

bien común mayor al que se alcanzaría si cada persona trabajara sola, y esta capacidad de trabajo conjunto no ha pasado desapercibida para la humanidad. Ha sido la base de la organización social humana durante siglos, y lo sigue siendo aún en la actualidad. Aun mejor, este esquema de trabajo colaborativo basado en la comunicación está siendo usado en la tecnología para optimizar el trabajo de las organizaciones, hacerlas más eficientes (partiendo del trabajo en comunidad) y sobre todo, hacerlas más productivas en términos económicos. Pero ¿cómo se puede usar el mismo esquema de trabajo colaborativo en la tecnología? Antes que nada, debemos entender cómo transmitimos información nosotros mismos, y así, modelar este mecanismo para usarlo en nuestros sistemas tecnológicos.

Modelo transmisor-receptor.

Supongamos la situación en la que un amigo y usted están hablando en un paradero de buses. El amigo le está contando sobre su nuevo trabajo y usted está dándole opiniones al respecto. Su amigo piensa aquello que le va a decir, luego, se lo dice, y usted lo escucha atentamente para luego analizar lo que su amigo le dijo y responderle. Esto pasa con relativa naturalidad y usted no se detiene a pensar en el cómo pueden hablar a pesar de todo ese tráfico.

Pero detengámonos un momento a analizar todos los elementos que intervinieron en este acto tan simple como el hablar con otra persona.

Primero, su amigo “pensó” lo que debía decirle, es decir, generó la **información** que iba a ser enviada. Pero su amigo no es su boca, esta solo es el medio con el que se pronuncia lo pensado. Es por eso que la mente de su amigo, la que genera la idea o la información, es la **fuente.**

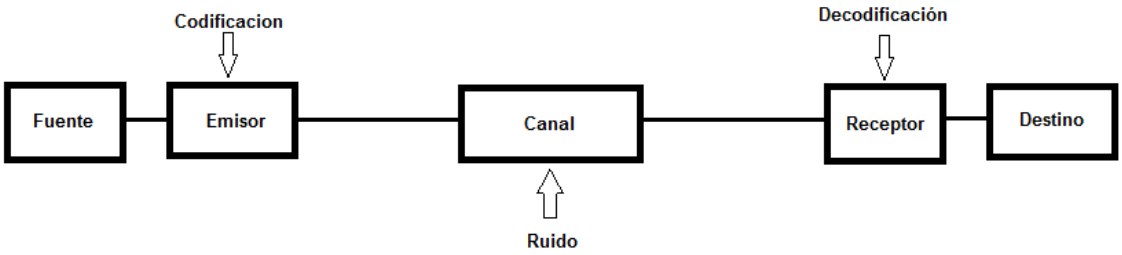
La boca pronuncia entonces la información que la fuente generó. Sin embargo, debe pronunciarla de manera tal en que usted, al escucharla, pueda

entenderla. Es por esto que dicha información debe usar un **código**, es decir, luego de pensada, debe ser codificada en un esquema que ambos, emisor y receptor, puedan entender. Este código, en nuestro caso, es el idioma que ambos hablan. La boca, como pronunciadora de la información codificada en la fuente, se convierte en el **emisor** de los datos a transmitir.

La información pronunciada por la fuente viaja a través del aire hasta sus oídos. El aire, el medio en que se transmite la información codificada, es llamada **canal**. Vemos que ese canal no es estable ni mucho menos. La gran cantidad de autos que los rodean generan sonido que no permite escuchar bien la información de su amigo. Este sonido molesto de los autos es llamado **ruido**, y nunca ningún canal está exento del mismo. Sus orejas y oídos, los encargados de recibir la información y convertirla en impulsos nerviosos para su cerebro, hacen las veces de **receptor**. Esta información es decodificada en su cerebro, comunicando la información a transmitir, al **destino**, es decir, su conciencia o la parte racional de usted.

Este es entonces el esquema tradicional de comunicación de datos entre 2 elementos, un emisor y un receptor, o un productor y un consumidor.

La fuente codifica información enviada por el emisor a través del canal. Esta información se combina con ruido en el canal y llega al receptor, que la decodifica para entregarla al destino.



Es así como, mediante este modelo, se ha desarrollado toda una serie de protocolos y sistemas de comunicación entre computadores y entre incluso organizaciones. Y es de acá que parte el concepto de red.

¿Redes?

Cuando nos dicen “red” es posible que pensemos en una telaraña, o en una red de pescar. Podemos también imaginar las neuronas de nuestro cerebro, o incluso el facebook. Pero ¿Qué es en suma una red?

Imaginemos que mientras hablamos con nuestro amigo, a él le entra una llamada por el celular. Supongamos también que usted conoce la persona que llama a su amigo, y al no poder hablar directamente con ella, le manda saludos. Su amigo le comunica a la llamada que tú le mandaste saludos, y esta, a su vez, te devuelve el saludo. Resulta que la llamada es nada menos que la esposa de tu amigo, y se encuentra en este momento recogiendo a los niños del colegio (3 niños) en su carro. Cuando los niños se montan, usted escucha el sonido de ellos hablando por el celular de su amigo, y también les manda saludes. Su amigo le dice a su esposa que le diga a sus niños que usted les manda saludes, por lo que ella les dice a todos los niños. La llamada termina y ustedes siguen hablando en el paradero de buses.

En esta situación intervinieron más de 2 personas, en realidad, 6. Se podría decir que su amigo y usted están “conectados” a través de la conversación que tienen, porque el medio (el aire) se los permite. Cuando la esposa de su amigo llamó, la comunicación se amplió, y a través de su amigo, usted mandó un mensaje a ella. En ese momento, el destino se convierte nuevamente en una fuente, y se comunica la información por la red celular hasta llegar al aparato de la esposa. Como su amigo hizo de intermediario entre usted y la esposa, su amigo se convierte en un **nodo**, es decir, en un punto en el que confluyen

varias conexiones. Cuando la esposa manda saludes a sus hijos, no les dice a cada uno de manera individual, sino que les dice a todos por igual, con un sonido alto. En ese momento, ella es un nuevo nodo, y le comunica a varios elementos al mismo tiempo el mensaje. Este tipo de comunicación se llama **broadcasting**, y el medio permite que a todos les llegue entonces el mensaje.

Usted, y los niños, también son nodos, porque tienen el potencial de poder comunicar lo que reciben a otra persona en cualquier momento, y así es como se forma una red:

Una red es un conjunto de nodos interconectados entre sí, que comparten información.

En nuestro caso, los nodos serán computadores, y nos contextualizaremos con respecto a las redes para hablar de redes de computadoras. Es así como podemos definir una red de computadoras como “un conjunto de ordenadores conectados entre sí que comparten información”.

Existen entonces muchos tipos de redes dependiendo de cómo se conecten los nodos y cómo se comuniquen. Acá veremos algunos tipos de conexión.

Tipos de redes

Las redes se pueden clasificar de muchos tipos, dependiendo de su naturaleza. Las podemos clasificar en los siguientes tipos:

- Por Alcance
- Por medio de conexión
- Por relación funcional
- Por topología
- Por la dirección de los datos

Veremos cada una de estas clasificaciones:

Por alcance.

Las redes pueden clasificarse según la cobertura que tengan, así:

PAN (Personal area network): Redes de area personal. Son redes que cubren un radio pequeño, de pocos metros, donde los nodos deben estar cerca entre si.

LAN (Local area network): Redes de area local. Son redes limitadas a los 200 metros, o a computadoras conectadas en un solo edificio o establecimiento.

CAN (Campus area network): Redes de area de campus. Estas redes son las que cubren un campus completo, como una universidad o una organización amplia.

MAN (Metropolitan area network): Redes de area metropolitana. Son redes cuya cobertura abarca un area geográfica extensa, como un municipio o una ciudad. También es aplicable para conectar varias sucursales de una organización en una misma ciudad.

WAN (Wide area network): Redes de area amplia. Redes que cubren un país o un continente.

Por medio de conexión

Medio guiado: Se define una red así cuando los medios por los que se conectan los computadores son físicos, como cables.

Medio no guiado: Esta es una red cuya conexión se hace de manera inalámbrica.

Por relación funcional

Relacion cliente-servidor: Este tipo de red se maneja cuando un computador, al que llamaremos cliente, hace una petición para usar un programa o un servicio, a otro computador que controla dicho programa, al que llamamos servidor. Esta topología es la más usada en las organizaciones, pues a través del servidor se hace todo un seguimiento a la seguridad de la red.

Relación igual a igual (P2P: peer to peer): En esta red, no hay servidores, sino un conjunto de nodos que se comportan iguales entre si.

Por topología de red

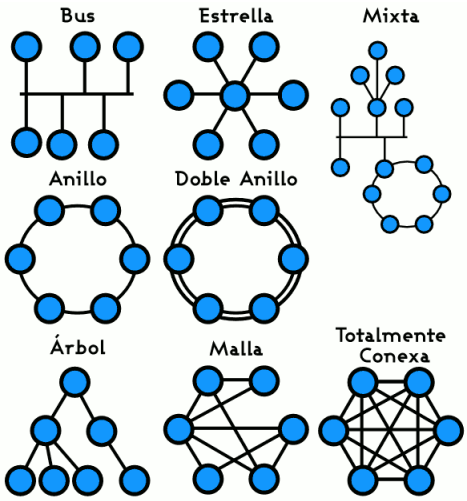
Topología en bus: Todos los computadores están conectados a un cable central o “bus” de datos, y a través de él se genera la comunicación.

Topología en estrella: Un computador central recibe las conexiones de todos los otros computadores que lo rodean, de manera que todo el tráfico (el tráfico se define como el paso de datos por los medios de conexión) de la red es escuchado por el computador centra.

Red en anillo: En esta topología, todos los computadores hacen parte de un “anillo de comunicación”, donde cada máquina solo tiene contacto con su máquina “a la derecha” y a la “izquierda”.

Red en malla: Los computadores están conectados entre sí, mediante conexiones parcialmente organizadas. Una sola máquina puede estar conectada a otras 5, otra máquina solo a 3, otra a 4, etc.

Red en árbol: En esta red, toda la información llega a un computador central a través de computadores secundarios, que a su vez están conectados con varios computadores terciarios, que a su vez están conectados…



Por la dirección de los datos:

Simplex: En esta configuración, el productor genera información y el consumidor la usa, no hay otro camino.

Half dúplex: Esta configuración permite que el equipo productor, luego de haber producido y transmitido la señal, se convierta en consumidor, y pueda recibir información. Ambas cosas no pueden hacerse de manera simultánea, solo un equipo transmite a la vez.

Full dúplex: Ambos equipos pueden transmitir de manera simultánea.

Conociendo así los tipos de redes que se usan en computadores, ahora debemos preguntarnos: ¿cómo se transmite entonces la información por una red de computadores? Si bien tenemos un modelo de comunicación básico, este modelo no es lo suficientemente completo para poder explicar de manera satisfactoria la forma en la que 2 computadores comparten información. Existen varios modelos para explicar cómo se transfiere información entre 2 ordenadores, pero nosotros estudiaremos el modelo más usado en el mundo, que se llama “modelo OSI”

Modelo OSI.

El modelo OSI (Open system interconection) es un modelo de conexión creado con el fin de estandarizar todas las conexiones de red existentes a la fecha de su lanzamiento (1984), ya que el desarrollo de las redes era muy desordenado en ese entonces, y una red no podía comunicarse con otra debido a que lo hacían en diferentes “idiomas”. Este modelo surgió entonces como una posible solución a este problema.

Este modelo consta de una serie de protocolos, separados por “capas”, en las que cada capa genera un determinado trabajo sobre los datos para garantizar una transmisión confiable, segura y eficiente de los mismos.

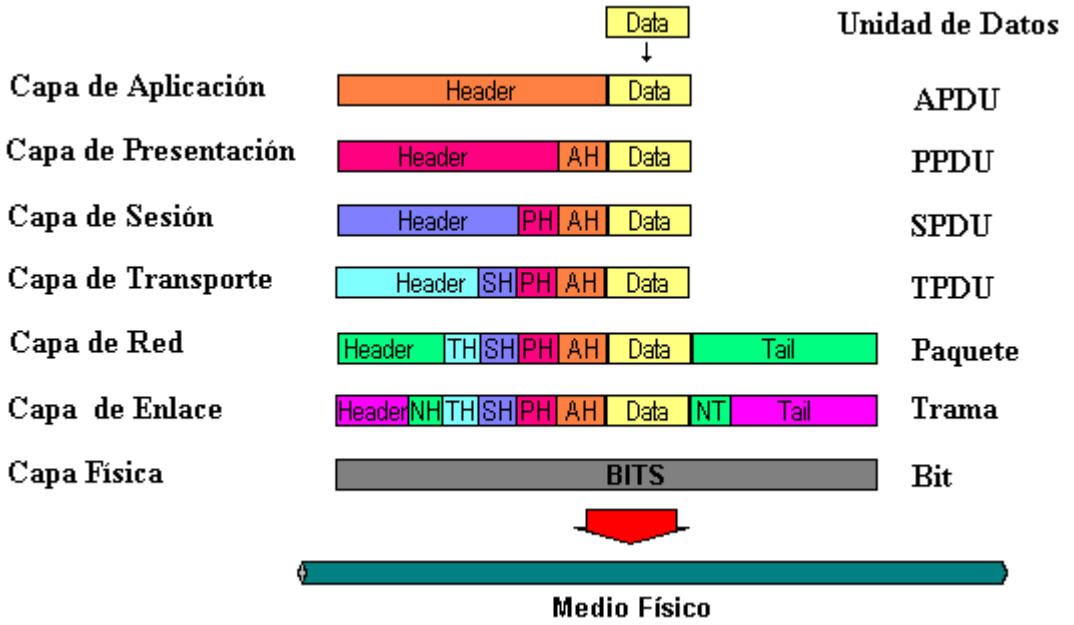
El modelo fue definido en 7 capas, las cuales veremos a continuación:

LA PILA OSI

1. Nivel físico: Esta capa es la encargada de controlar todo aquello referente a la conexión física de los datos, como el tipo de cable a usar, o el espacio sobre el que se moverán las indas de la red inalámbrica, el tipo de señal a usar para enviar los datos, etc. En esta capa, a la información se le trata como bits y bytes
2. Nivel de enlace de datos: Este nivel es el encargado de que la información sea transmitida libre de errores entre 2 máquinas. Para esto, agrupa los bytes en tramas, y les agrega información adicional. Esta información adicional sirve para la detección y corrección de errores, control de flujo entre los equipos (para que un pc más lento que otro no se "desborde" por no tener la velocidad requerida para procesar la información) y para asignarle una dirección que indica hacia que computador debe dirigirse.

3. Nivel de red: Este nivel o capa es el encargado de que los datos lleguen desde el origen específico hasta el destino apropiado. En esta capa se selecciona la ruta para que las tramas, ahora agrupadas en datagramas o paquetes, puedan llegar desde un computador a otro, aunque no tengan conexión directa. En este nivel funcionan los enrutadores o "routers", que leen los datagramas, y de acuerdo a la información adicional que agrega esta capa sobre los datos, "decide" sobre la dirección del mismo.
4. Nivel de transporte: Este es uno de los niveles más importantes del modelo OSI. Define el esquema en el que 2 computadores establecen contacto y comunicación. En esta capa, los datagramas se llaman "segmentos", y su principal función es garantizar la comunicación entre 2 equipos, independiente de la red que usen para su conexión.
5. Nivel de sesión: Es el encargado de mantener la conexión entre 2 computadores que están "dialogando" a través de sus aplicaciones. Sirve principalmente para organizar y sincronizar el diálogo entre máquinas.
6. Nivel de presentación: Esta capa, en pocas palabras, es un traductor. Es el encargado de representar la información transmitida entre computadores con diferentes topologías de datos.
7. Nivel de aplicación: Es la capa en la que las aplicaciones acceden a los otros servicios del modelo OSI para comunicar información.

La forma en la que funciona entonces el modelo OSI es la siguiente:



Las aplicaciones mandan datos, a los que se le agrega información adicional (headers) que le indicarán al computador destino en qué aplicación observarlos. La capa de presentación agrega otro header a los datos para indicar el tipo de codificación usada. La capa de sesión toma la información anterior y le agrega otro header usado para organizar el flujo de información entre los sistemas a comunicar. La capa de transporte toma los datos, y les agrega un header en el que se indica el protocolo a usar para transmitir la información en las redes. Luego, la capa de red toma la información, agregándole otro header y una cola (Tail: Usada para indicar dónde termina el paquete de datos), usados por los routers para encaminar los paquetes. La capa de enlace toma estos paquetes y le agrega otro header y otra tail para controlar los errores en la transmisión de segmentos, y finalmente estos segmentos son expresados en bits para enviarse a través de la red por os medios físicos de la misma.

Los datos a transportar son entonces solo una pequeña parte de toda la trama transferida entre computadores. Es un poco irónico, pero así funcionan la gran mayoría de redes de computadores.

Sin embargo, algunas personas indican la posibilidad de una octava capa (a modo de broma para algunos, pero muy importante para nosotros), llamada la "capa 8". Explicaremos brevemente por qué es importante y cómo la usaremos en nuestro estudio de la seguridad de las redes.

Una nueva capa ¿capa 8? – Políticas de seguridad

Supongamos que un usuario, en su oficina, está enviando un mensaje de texto a su jefe en el trabajo. Digamos que hablan, por ejemplo, sobre un servidor de la compañía que no funciona, y sobre el cual se debía hacer un diagnóstico y volver a la misma luego de avisar a su jefe. El mensaje que envía el usuario es el siguiente:

"Señor muerto, esta tarde llegamos".

Cuando en realidad el mensaje a enviar era

"Señor, muerto está, tarde llegamos"

En este error, curioso pero real (sucedió en una obra de teatro), nos damos cuenta que el sistema de comunicación puede funcionar perfectamente, pero si el usuario usa mal dicho sistema, sencillamente, todo el esquema falla. Es ahí, en esta "octava capa", o "capa usuario", donde ocurren la mayor parte de problemas de seguridad de una compañía, y es por esta razón que se nos hace necesaria la creación, de manera prioritaria, de políticas de seguridad informática, que le indiquen a las personas cómo interactuar con los sistemas.

Conceptos de seguridad

La seguridad informática se ha convertido en un tema de especial importancia en las organizaciones de la actualidad. El avance tecnológico no solo se ha visto aplicado en aparatos de última generación, sino que también ha impactado la productividad de las empresas actuales, al permitirles interconectar todos los sistemas de la organización, para una mayor eficacia en la comunicación y velocidad de respuesta ante los cambios externos. Esta interconexión, aunque abre grandes posibilidades (como el control “ubicuo”, o desde cualquier lugar, el “teletrabajo” o trabajo desde casa, y las comunicaciones unificadas), también plantea nuevos retos y amenazas en la manipulación de la información y, en suma, en los fines de la organización.

Estas amenazas han hecho que las empresas creen documentos y normativas para regular el nivel de seguridad de su estructura interna, protegiéndolas así de ataques externos o de negligencia por parte de los propios empleados. Estos documentos y directrices, no son más que las “Políticas de seguridad informática”, o procedimientos que se llevan a cabo para crear y reforzar la seguridad de las redes.

Estas políticas, aparte de establecer normativas y restricciones, tienen como objetivo principal crear conciencia en los miembros de la organización en cuanto al valor e importancia de aquel bien intangible sobre el cual se aplican todos estos procedimientos y normas, aquel bien que define en suma el valor de una red y la naturaleza de una organización. ¿Qué es aquello que necesitamos proteger tanto, y que tiene tanto valor? Los datos.

¿Qué tan valiosos pueden ser los datos?

El valor de los datos es un tema muy relativo. Debido a que son intangibles, su valor no puede determinarse fácilmente, cosa que no pasa con los enseres de la organización, como computadores, escritorios, entre otras cosas. Y aparte de todo, cuando se aplican medidas de seguridad en las redes, estas no generan mayor productividad en la organización. Debido a esta razón, las organizaciones son muy negativas a la hora de asignar presupuesto a la seguridad.

Un ejemplo del valor de seguridad puede verse en una compra por internet. En esta compra, debemos ingresar nuestro número de tarjeta de crédito y nuestra contraseña. Esta información, debe viajar por la red, pasando por gran cantidad de zonas no seguras, y compartiendo el mismo espacio que documentos, música, imágenes, entre otros datos.

Sin embargo, el momento más crítico en cuanto a la seguridad se ve en el momento en que mi información de la tarjeta de crédito, junto con los datos de otros miles de usuarios, llega a una base de datos y es almacenada. Si un usuario malintencionado accediera a esta base de datos, no solo accedería a mis datos, sino a la de miles de usuarios más.

Y los accesos no autorizados a una red no son los únicos riesgos que se pueden tener. También se encuentran los virus, el spam, entre otros. Estos ataques, aunque pueden parecer leves, no lo son en absoluto. Hace una década, los costos asociados a los ataques informáticos ascendían a 100 millones de dólares, con un máximo de 800 millones de dólares. Si a eso sumamos la digitalización actual en las empresas, el comercio electrónico, las empresas basadas en información y las estadísticas que indican que solo 1 de

500 ataques son detectados y reportados, podemos dimensionar entonces el verdadero valor de estos delitos.

Es entonces indispensable, casi exigible, que toda empresa que maneje redes de información y tenga sistemas computarizados, cree una normativa y una serie de políticas que garanticen la seguridad de sus datos y su información valiosa. **Ese es, entonces el propósito de este curso, dar un acercamiento a los aprendices en cuanto a la creación de políticas de seguridad para las organizaciones.**

¿Qué es la seguridad en redes o seguridad informática?

Haremos el ejercicio de construir el concepto de seguridad en redes basándonos en el significado de cada una de las palabras que componen dicho concepto. Al consultar los significados en internet, podemos encontrar los siguientes resultados:

- Seguridad: Ausencia de riesgo o confianza en algo o alguien
- Información: Conjunto organizado de datos procesados, que constituyen un mensaje sobre determinado fenómeno o ente.
- Red: conjunto de equipos conectados, que comparten recursos, información, servicios, incrementando la eficiencia y productividad de las personas.

Si unimos estas definiciones, podemos crear una definición macro de lo que es la seguridad en redes o seguridad informática:

Seguridad en redes: Es mantener libre de riesgo o confiables los datos procesados que se comparten en un conjunto de equipos.

Si a esta definición, le unimos el conocimiento básico que tenemos sobre “políticas de seguridad” comentado arriba, obtenemos lo siguiente:

Seguridad en redes es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.

Pero esta seguridad debe aplicarse a todos los recursos informáticos de una organización, estén o no interconectados entre sí, ya que las políticas de seguridad deben aplicarse en la totalidad de la organización, independiente de que sus secciones estén separadas entre sí. Es a esto a lo que se le llama “Seguridad global”

¿Qué es la Seguridad Global?

La seguridad global es aquella que se aplica sobre todos los componentes de una organización. A todos estos componentes se les llama “red global”, y pueden ser los siguientes:

- Redes de área local (LAN),
- Redes de área metropolitana (MAN),
- Redes nacionales y supranacionales (WAN),
- Computadoras personales, minis y grandes sistemas.

No importa que dichos componentes no estén interconectados entre sí, todos manejan información de la organización, y por tal, deben estar cobijados en la política de seguridad informática. Hemos de tener en cuenta que dichas

políticas deben ser aceptadas por las personas de la organización, que en suma, serán las que las lleven a cabo.

Recordemos que la octava capa de un modelo de comunicación son las personas, y es en esta capa que se aplican las políticas de seguridad informáticas (PSI)

Son estas personas las que deben concientizarse de los usos, conceptos y costumbres relacionados con los conceptos de seguridad. Dicha conciencia requiere un trabajo arduo con los usuarios, un trabajo que al mismo tiempo sea capaz de mostrar los beneficios de implantar un plan de seguridad en la organización. El trabajo con las personas de la organización permite indicarles qué deben hacer cada uno frente a las políticas, que desviaciones pueden suceder, y de producirse un fallo, este trabajo con los usuarios permite detectar fácilmente en que sector se produjo la vulnerabilidad.

¿Cómo trabajar fácilmente con los usuarios? Una estrategia muy usada es la de generar grupos de trabajo, en los que se informan las características de las medidas de seguridad. Este trabajo personalizado permite que los usuarios se sientan comprometidos e informados, desembocando en una aceptación y uso de las medidas asignadas.

¿Cómo afectan las medidas de seguridad a la organización?

Aunque las medidas de seguridad surgen para hacer más confiable un sistema, tienen el inconveniente principal de que, aparte de no aumentar la productividad de la organización, incrementa la complejidad de las operaciones llevadas a cabo dentro de la misma.

Un ejemplo claro de este aumento en la complejidad es el del uso de internet en redes de la organización. Antes de instalar políticas de seguridad, el acceso a internet era transparente para el usuario. Ahora, para el control de acceso, la persona debe acceder un nombre de usuario y una contraseña por cada acceso a internet que deba llevar a cabo, esto con el objeto de controlar las páginas visitadas y evitar un posible robo de información. Estos “logines” hacen más complicado el proceso de acceso a la red, y, si algún cambio fuera a hacerse en estos accesos, debe comunicarse a todo el personal a través de medios diversos, lo cual aumenta el trabajo del área administrativa, técnica y de comunicaciones.

Origen de errores, visibilidad del proceso e implementación

En un reciente estudio de Datapro Research Corp. se resumía que los problemas de seguridad en sistemas basados en redes responden a la siguiente distribución:

- Errores de los empleados 50%
- Empleados deshonestos 15%
- Empleados descuidados 15%
- Otros 20% (Intrusos ajenos a la Empresa 10%; Integridad física de instalaciones 10%)

Se puede ver que el 80% de los problemas, son generados por los empleados de la organización, y, éstos se podrían tipificar en tres grandes grupos:

- Problemas por ignorancia
- Problemas por haraganería
- Problemas por malicia

De estos 3 problemas, el de la ignorancia es el más fácil de atacar. Se deben llevar capacitaciones y entrenamientos periódicos a los usuarios en las áreas digitales, y, aunque obvio para algunas personas, recordar de tanto en tanto, cosas que todos deben conocer.

La haraganería, más que un problema, es una tentación, tanto para los usuarios, como para el administrador de las políticas. Sin embargo, cuando las personas ven las metas de los sistemas de seguridad y ven en la organización un ambiente no de censura sino de focalización de soluciones, tienden a evitar la haraganería o pereza, descargando gran cantidad de trabajo en la administración y en la gerencia, entes responsables por la productividad de los empleados.

Finalmente, la malicia se debe combatir con el desarrollo de lealtad en los trabajadores por su trabajo.

Como vimos anteriormente, el 80% de los problemas de seguridad de una organización surgen de los empleados. Es por esto que ellos deben estar comprometidos con el desarrollo de las políticas. No nos cansaremos de enfatizar que el primer y último elemento de la comunicación son las personas. De este apartado surge el concepto de **visibilidad**, cuya idea principal es la de permitir que los usuarios puedan aportar en el desarrollo de dichas políticas y sean siempre conocidas las acciones tomadas, evitando así la “unilateralidad” de las decisiones y pudiendo llegar a obtener soluciones más efectivas de las que se iban a tomar en un principio, al sopesar perspectivas diferentes a las planteadas por los expertos.

Igualmente, es necesario comunicar lo más pronto posible cualquier cambio en las políticas de seguridad, comentar posibles modificaciones en los grupos de trabajo anteriormente sugeridos, recibir asesoría en la parte legal para poder definir sanciones adecuadas a la norma impartida y hacer que los usuarios acepten las políticas, remarcando los beneficios de las mismas.

Antes que nada, debe entenderse que la implementación de dichas políticas es un proceso que une la parte técnica con la parte administrativa. Si la gerencia no colabora de manera activa y fuerte en la implantación de estas normas, la implementación en toda la organización de estas puede verse truncada o limitada. De igual manera, si la parte técnica genera gran cantidad de complicaciones en el acceso a la información, el costo comparativo entre complejidad y ganancias en seguridad puede ser disparejo y pueden, finalmente, dejarse de lado las estrategias de seguridad planteadas.

Si no existe compromiso entre la parte gerencial y la parte técnica de la organización, cualquier documento de seguridad que sea creado caerá por su propio peso. La haraganería, antes que un problema, es una tentación que también puede afectar la administración y la gerencia.