# Gestión de seguridad en redes corporativas

**Juan José García Pagan**

*Vicepresidente de Operación de Redes de Telefónica del Perú*

**Resumen**

*Este artículo tiene como objetivo incentivar al lector para que tome conciencia de la importancia de aplicar conceptos de seguridad en sus redes o sistemas informáticos. Para ello, Telefónica del Perú se apoya en cuatro pilares, en los cuales basa todas sus operaciones de seguridad. Para la solución de este tipo de incidentes Telefónica cuenta con ingenieros altamente calificados, que se desenvuelven en procesos certificados con el ISO 27001, además de formar parte de organismos internacionales de seguridad (FIRST), para colaborar en la difusión de una conciencia de seguridad, junto con los principales proveedores del servicio de internet del mundo.*

*Palabras clave:*
*Seguridad de la información, seguridad empresarial, seguridad de redes, servicios de seguridad, seguridad gestionada, ingeniería social, TSOC-Telefónica Security Operation Center.*

## 1. Introducción

La seguridad ha sido y es una de las prioridades del ser humano moderno. Nos protegemos a nosotros mismos, a nuestras familias y a nuestros bienes más preciados de posibles intrusiones o ataques indeseados. En definitiva, es una necesidad sentirnos seguros. No escatimamos esfuerzos para tener una vida tranquila y segura.

Si extrapolamos esta situación a nuestras redes o sistemas informáticos, somos conscientes de que dejar de aplicar políticas de seguridad mantiene vulnerabilidades que pueden ser explotadas por terceros para tener acceso a información confidencial y de mucha importancia para cualquier organización.

La preocupación que manifiestan las organizaciones o empresas, tanto públicas como privadas, por los inminentes ataques a la seguridad de sus redes corporativas nos coloca en un escenario de extrema alerta. En ese sentido, TdP, como el proveedor de servicios de internet con mayor participación en el mercado local, es consciente del papel trascendental que juega en la tarea de asegurar la confidencialidad, integridad y disponibilidad de la información.

Las redes corporativas de alto impacto requieren de una estructura técnico-operativa de altísimo nivel de especialización en temas de seguridad, por lo que TdP cuenta con una organización que le permite afrontar los diferentes incidentes.

## 2. Tendencias

La seguridad es un factor fundamental dentro del desempeño de los sistemas de Tecnologías de Información (TI) y se relaciona con todos los aspectos de la empresa, desde la continuidad de sus actividades hasta sus procesos administrativos.

Según algunas auditorías elaboradas por el CSI (Crime Scene Investigation) y el FBI (Federal Bureau of Investigation) a 500 corporaciones y agencias de gobierno norteamericano, demostraron que de estas el 90% detectó intrusiones en su red, el 80% reconoció pérdidas económicas, el 40% cuantificó su pérdida financiera en más de US$500 mil y el 40% detectó penetración desde fuera.

Según Gartner, a finales del 2007 el 75% de las empresas se verán infectadas con *malware* no detectado, creado con fines financieros y dirigido a blancos muy específicos. El número de organizaciones que de-

nuncian ante la policía o los juzgados las incidencias de seguridad es poca. La causa aducida es evitar la mala publicidad, no obstante un 80% de las organizaciones realiza auditorías de seguridad.

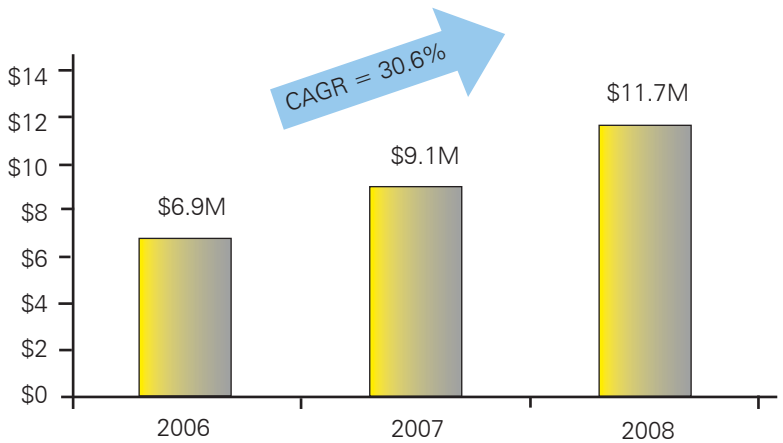
Ante el aumento de las incidencias causadas por los distintos códigos maliciosos, la seguridad empresarial se torna cada vez más compleja y costosa, lo cual se traduce en una mayor demanda de recursos que requieren ser administrados, pero son pocas las empresas que cuentan con los recursos suficientes para mantenerse a la par con el ritmo de avance que han demostrado tener las amenazas provenientes de internet, que ponen en riesgo a muchas compañías.

En este contexto, la seguridad es una prioridad para las organizaciones; por ello, tienden a destinar entre el 3% y el 6% del gasto total de TI a este rubro, habiéndose generalizado la utilización de criterios económicos en la toma de decisiones de adquisición de elementos de seguridad. Un 55% aplica criterios de cálculo del retorno de la inversión (ROI).

El IDC, en su último reporte, pronosticó un crecimiento del mercado nacional de 32,93% para el presente año, cifra que representaría 9.108.828 dólares en valor.

La mayor demanda se encuentra en el sector de banca y finanzas, porque la información es percibida como un activo bastante importante.

Peru System Infrastructure Software
Market (US$M) 2006-2008



Pese a la positiva variación en el gasto para salvaguardar los activos de las compañías, todavía hay un buen porcentaje de empresas en las que la partida para seguridad, respecto al total de los presupuestos destinados a TI, seguirá siendo baja, pero esto cambiará con la toma de conciencia de que las amenazas informáticas no discriminan a nadie, ya que están presentes en todos lados.

## 3. Amenazas: Código malicioso y ataque de aplicaciones

En la actualidad existe una gran cantidad de formas de vulnerar un sistema, por lo que se tratará de dar a conocer aquellos que son los más usados para infligir algún tipo de daño a los sistemas que se encuentran vulnerables:

### 3.1 Código malicioso (virus)

Dentro del código malicioso está incluido un amplio rango de amenazas de seguridad programadas por computadora, que explotan las vulnerabilidades de la red, los sistemas operativos, software y la seguridad física para propagar el código malicioso entre los sistemas por computadora.

Inicialmente, la fuente de este código malicioso fueron personas expertas en el desarrollo de software, quienes tomando ventaja de su posición creaban nuevas técnicas de ataque. De hecho, actualmente la mayoría de tales personas se encuentran colaborando en la advertencia de vulnerabilidades de sistemas operativos o paquetes de software.

En estos tiempos, en los que la tecnología ha alcanzado un gran avance, abundan aquellos que "juegan" con programas ya desarrollados, y que sin entender el completo funcionamiento de estos lanzan ataques a sistemas remotos, pudiendo desencadenar innumerables problemas a los usuarios de Internet en general. Esto permite que cualquiera, con un mínimo nivel de experiencia, cree nuevos virus y los desate en todo el sistema de internet.

Entre los tipos de códigos maliciosos podemos encontrar la *bomba lógica*, que es un virus que se mantiene en "descanso" por un periodo, y se activa en el momento en que se le programó en todos los sistemas que se infectaron. Un ejemplo claro es el virus Michelangelo, que fue programado para activarse el 6 de marzo del 2007, procediendo a formatear el disco duro de los sistemas afectados y a destruir la información que se encuentre en estos.

Otro tipo de código malicioso es el conocido como *Caballo de Troya.* En este caso el usuario es engañado mediante el uso de la ingeniería social. Cuando piensa que ha descargado el programa que necesitaba, se le instala automáticamente otro programa, que parece ser tan inocuo como una ventana emergente con propaganda comercial, pero abre *back-doors* (puertas traseras) para tomar el control de la máquina afectada de forma remota.

El *gusano* es un tipo de código malicioso que posee el mismo potencial destructivo que otros tipos de virus, pero con una cualidad especial: es capaz de propagarse por sí mismo sin necesidad de la intervención humana. Este tipo de virus causó el primer incidente grave de seguridad en el Internet.

## 3.2 Ataque de contraseñas

Una técnica simple usada por los *hackers* para obtener acceso ilegal a un sistema es conseguir, de cualquier manera, el nombre de usuario y la contraseña de un usuario del sistema; una vez dentro, y con las herramientas necesarias, es posible incrementar el nivel de acceso al sistema o usarlo como puente para un objetivo mucho más atractivo que se encuentre en la red.

Un método bastante utilizado es el de adivinar el *password*, ya que —sin importar el nivel de educación del usuario— lo más probable es que se usen contraseñas demasiado débiles (fáciles de adivinar). Un método más elaborado es el ataque de diccionario, el cual consiste en una lista con miles de posibilidades de password, luego son encriptados con el mismo *script* usado para encriptar las claves, se comparan, y si se encuentra alguna coincidencia se conoce rápidamente el usuario y la clave, con lo que se obtiene el acceso al sistema.

## 3.3 Ataque de denegación de servicios (DoS)

Este tipo de ataques atenta contra la posibilidad de que los usuarios autorizados tengan acceso a los recursos. Es bastante similar a decir: "¡Si yo no puedo tenerlo, nadie lo tendrá!", debido a que normalmente es usado por los *hackers* luego de haber fallado en el intento de ingresar al sistema. Algunos de estos métodos hacen uso de la fuerza bruta para ocasionar que el sistema se sobrecargue ante tantas peticiones, que no pueda atender a aquellas legítimas y dejar de lado aquellas que provienen de un ataque.

Uno de los métodos más conocido es el "ping de la muerte". Una forma sencilla de entender este ataque es la siguiente: el paquete ICMP más largo permitido es de 65,536 bytes; sin embargo, no se tomaron precauciones en el caso de paquetes de mayor tamaño; por ello, los desarrolladores diseñaron programas que enviaban paquetes ICMP más grandes que el tamaño máximo. En consecuencia, algunos sistemas, al recibir paquetes de al menos un byte mayor, se colgaban o hacían *crash.* En la actualidad, esta vulnerabilidad ha sido resuelta en la mayoría de sistemas operativos, pero las versiones antiguas de algún software son vulnerables.

## 3.4 Ataque de aplicaciones

Algunas prácticas inapropiadas de los desarrolladores de códigos dejaron ciertas vulnerabilidades en los programas. A continuación se mencionarán algunos:

- El desbordamiento del *buffer* es una vulnerabilidad inherente en los códigos desarrollados, debido a que muchos programadores tienen la idea de que revisar los parámetros es una pérdida de tiempo que hace lento el programa; sin embargo, es necesario tener en cuenta, como buena práctica de seguridad en la programación, las medidas apropiadas para evitar este tipo de ataques. Como resultado de la falla en la aplicación de esta medida de seguridad, el atacante puede conseguir acceso al sistema en caso de ocasionar un desbordamiento del *buffer*.
- Las puertas trampa (*trap doors*) son una secuencia de comandos no documentados, que fueron desarrollados por los programadores al momento de la producción del sistema. Esto les permitía mejorar el tiempo de desarrollo del código, evitando la autenticación en sus pruebas de rutina. Si por un descuido o intencionalmente estas *trap doors* se dejan en el sistema, es posible tener acceso a este siguiendo esta secuencia de comandos; por ello, posteriormente pueden ser usados por el mismo desarrollador para tener acceso a información que no le es permitida.
- Los *rootkits* son paquetes de software especializado cuyo único propósito es permitir al atacante tener mayores privilegios en el sistema; normalmente utilizan como primera herramienta un ataque de diccionario para entrar al sistema como un usuario sin muchos privilegios, luego hacen uso de los *rootkits*, que se pueden encontrar en internet para ganar mayores privilegios en el sistema. Una buena medida para evitar este tipo de ataques es mantener los sistemas siempre con los últimos parches de seguridad, lo cual debe ser una práctica habitual en todo administrador de redes.

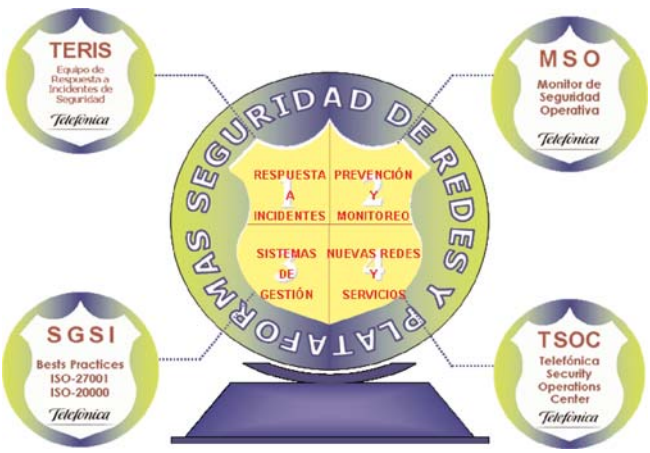
### 3.5 Ataques de reconocimiento

Como cualquier fuerza de ataque, necesita información sólida para enfocarse en los puntos donde el blanco es más vulnerable. De esta forma, los *hackers* han desarrollado diversas técnicas automatizadas que les permiten realizar un reconocimiento de la red. Entre estas técnicas se pueden mencionar tres:

- La prueba de IP, que es un simple envío de PING a diversos nodos de una red; en caso de responder al PING, esa IP específica será motivo de un análisis mayor. Debido a la existencia de este método, es recomendable la deshabilitación de la respuesta al PING, al menos a los pedidos que provengan de fuera de la red.
- Después de la prueba de IP, y teniendo la lista de direcciones IP que se encuentran activas, se realiza un escaneo de puertos para tener la relación de los servicios públicos activos que se encuentran corriendo en cada máquina.
- La tercera técnica es el escaneo de vulnerabilidades. Una vez definido el objetivo será necesario que el atacante sepa cuáles son las vulnerabilidades que en ese momento tiene la máquina. En Internet existen diversas herramientas para hacer este tipo de escaneos. Entre las más conocidas están Satan y Saint.

## 4. Seguridad de redes y plataformas en Telefónica del Perú

Actualmente, Telefónica del Perú cuenta con centros de gestión de redes fijas y móviles con infraestructura tecnológica de vanguardia, que son administrados por personal altamente especializado y certificado. Las operaciones de seguridad se organizan sobre la base de los siguientes cuatro pilares:

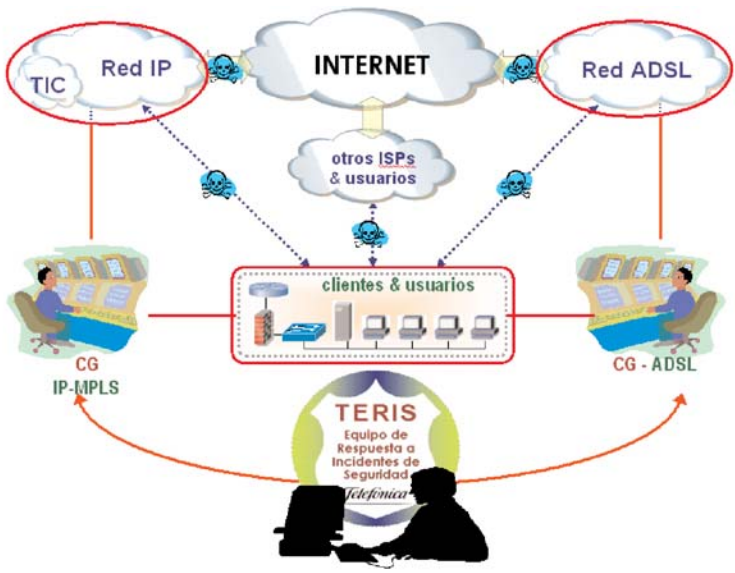


## 4.1 Telefónica Equipo de Respuesta a Incidentes de Seguridad (TERIS).

Es un equipo especializado en seguridad de redes y plataforma, que brinda a nuestros servicios, clientes, usuarios y a la comunidad de seguridad un soporte eficaz y oportuno para la atención, detección, tratamiento y resolución de incidencias de seguridad.

A su vez, este equipo realiza actividades de predicción, prevención, capacitación, implementación, fomento y difusión de la seguridad de la información en nuestra empresa, a través de las siguientes actividades:

- Detectar y resolver oportunamente las incidencias de seguridad que afecten a nuestras redes de servicio y de gestión (datos, internet y banda ancha).
- Atender y resolver eficazmente las incidencias de seguridad de nuestros clientes, usuarios y de la comunidad internacional de seguridad: fraude electrónico (*phishing*), intrusión, denegación de servicios (saturación), uso indebido de contenidos.
- Apoyar y asesorar a clientes, usuarios y a la comunidad internacional en la resolución de sus problemas de seguridad: *hackers*, virus, *spam*, escaneo de puertos, correos maliciosos, etcétera.
- Gestionar y liderar los procesos y actividades para el mejoramiento de la seguridad, así como la consolidación y ampliación del Sistema de Gestión de Seguridad de la Información (SGSI).



## 4.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Es el encargado de brindar un tratamiento a la información, basado en la confidencialidad, integridad y disponibilidad de toda la información que se utiliza en las operaciones internas, además fomenta y desarrolla las mejores prácticas en las diversas áreas operativas de la región, buscando cumplir y liderar los nuevos estándares internacionales.

En Telefónica del Perú el propósito de aplicar el SGSI es el de garantizar que los riesgos que pudiesen afectar a nuestros activos de información sean conocidos, asumidos, gestionados, controlados y minimizados por la organización de una forma documentada, sistemática, estructurada, eficiente y adaptada a los posibles cambios que se produzcan en los riesgos, en el entorno y la tecnología.

En la actualidad Telefónica del Perú maneja los procesos de información a través de un SGSI para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar los servicios de los clientes.


## 4.3 Monitor de Seguridad Operativa (MSO).

Realiza la evaluación, las auditorías y ejecuta los planes de seguridad en las redes y plataformas de la empresa. Adicionalmente, diseña e implementa rutinas, actividades y procedimientos técnico-operativos de seguridad, que son reconocidos por expertos de seguridad. Telefónica del

Perú es la única empresa peruana que cuenta con la certificación ISO 27001 en seguridad de la información para sus redes corporativas y fue la primera empresa del grupo en obtener dicha certificación a escala mundial.

### 4.4 Telefónica Security Operation Center (TSOC).

Es el área de Telefónica del Perú donde se llevan a cabo, de manera centralizada y remota, los servicios especializados de seguridad, con la disponibilidad de un conjunto de recursos informáticos (*hardware* y *software*) y profesionales altamente calificados, garantizando un adecuado y rápido tratamiento de los incidentes de seguridad.

Las principales funciones que lleva a cabo el SOC de Telefónica son:

- Configuración en la provisión: Los ingenieros especialistas que instalan los equipos en la casa del cliente coordinan con el SOC para que la habilitación de licencias y funcionalidades adicionales se hagan de manera centralizada y remota.
- Monitoreo y gestión: Monitoreo de alarmas y gestión de incidentes según el nivel de severidad, monitoreo de performance, de los equipos, de disponibilidad, de uso de interfaces, de estatus de procesamiento de *firewall* y VPN, monitoreo en tiempo real de los *logs*, monitoreo de SNMP *relay* (si se tuviera habilitada la función).
- Administración: Entre las funciones de administración están atender los requerimientos de los clientes respecto a los cambios de configuraciones, modificación o creación de políticas de seguridad de forma controlada.

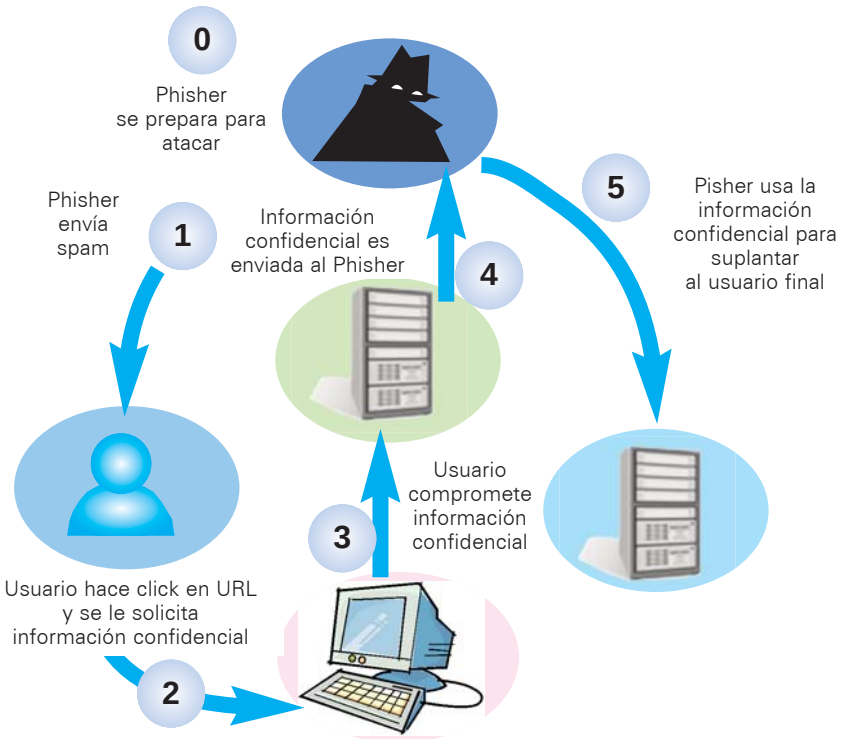
## 5. Los servicios de seguridad de Telefónica del Perú para sus clientes

Los servicios de seguridad que actualmente brinda Telefónica del Perú a sus clientes son los de *antiphishing* y seguridad gestionada.

### 5.1 *Antiphishing*

Está orientado al sector de la banca y se encarga de evitar la obtención de claves de usuarios de manera ilícita, con el fin de realizar transacciones no autorizadas. Este ataque se origina con la captura de la página web del banco, que es almacenada en un servidor cuya seguridad fue vulnerada por el atacante, que resulta siendo en muchos casos una víc-

tima más de este ataque. Una vez que la página web del banco ha sido clonada, el atacante envía un correo masivo (*spam*) a los clientes del banco con un link que los direcciona a la página clonada, donde se capturan el número de la tarjeta y la clave de la víctima. Los sistemas usados por los atacantes son cada vez más elaborados con la finalidad de confundir a la víctima.




Las entidades bancarias se preocupan por el fraude que envuelve a sus clientes, en el servicio de banca por Internet que les brindan. Recientemente, la actividad de fraude conocida como *phishing* se ha convertido en una amenaza creciente para los usuarios de internet, lo que resulta en una pérdida de confianza en el banco y el proveedor de servicios de internet. En sus inicios, este tipo de ataques estuvieron enfocados en los bancos de Estados Unidos y Europa, pero las entidades financieras de cualquier parte del mundo pueden ser víctimas de este fraude.

El volumen de estos ataques ha ido en aumento con mucha rapidez; por ello, es necesario tomar medidas drásticas para proteger a los usuarios, para lo que se requiere una adecuada combinación de los derechos de propiedad intelectual y los conocimientos técnicos, además de procedimientos claramente definidos y herramientas que permitan conseguir la evidencia apropiada.

El producto desarrollado por Telefónica del Perú se enfoca en la prevención, coordinación, desactivación y seguimiento de cada ataque de *phishing*. Este servicio es posible gracias a la asociación con empresas internacionales que tienen contacto directo con proveedores del servicio de internet (ISP, por sus siglas en inglés) en todo el mundo, con el fin de actuar de manera rápida. La prevención de estos ataques se consigue con el monitoreo de numerosas cuentas de correo trampa para tomar las acciones correspondientes antes de que alguna víctima pueda ingresar a la página clonada, así como mediante el seguimiento de la creación de nuevas páginas web que cumplen con ciertos patrones asociados a un ataque de *phishing*. Una vez desactivado el ataque se revisan los servidores donde se alojó la página clonada para evitar su reactivación o para proceder a desbloquear una vez que el servidor ya no aloje rastro de la página clonada.

## 5.2 Seguridad gestionada

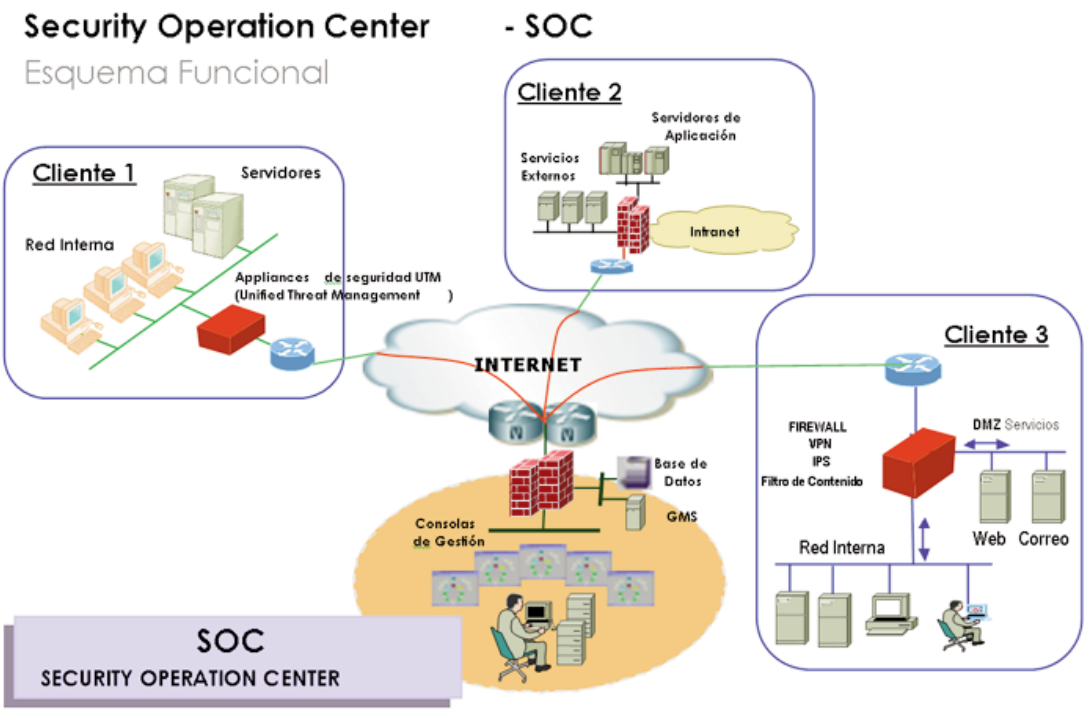
Es el servicio que brinda seguridad perimetral a las redes de nuestros clientes. De igual manera cuenta con un servicio de gestión, administración y monitoreo, permanente y centralizado, desde nuestro SOC (Security Operation Center).

En los últimos años, las compañías se han vuelto más dependientes de sus redes, pero estas son cada vez más vulnerables a los ataques e intentos de intrusión. A pesar de que se ha observado un crecimiento en la inversión de seguridad, paralelamente han crecido las amenazas por la aparición de nuevos virus, *spam* y códigos maliciosos. Es así que la seguridad enfrenta nuevos retos, que significan para las empresas no solo inversiones continuas en equipamiento y sistemas, sino también la dotación de recursos humanos especializados y permanentemente capacitados para su gestión.

Sin embargo, lo que sucede en realidad es que con frecuencia estas inversiones en equipamiento y sistemas no se complementan con una gestión permanente, sino que en la mayoría de casos se hace de mane-

ra parcial y con técnicos no especializados ni certificados en temas de seguridad. A esto se suma que, en ocasiones, también se descuida la actualización de los sistemas o el análisis sistemático de los registros.

Para enfrentar esta problemática surgen los servicios de seguridad gestionada, que son los servicios de seguridad que evitan las inversiones y gastos en infraestructura y recursos humanos especializados para una organización, dotándola de los mecanismos de seguridad perimetral como *firewalls*, concentradores VPN, detectores o preventores de intrusos, *gateways* de antivirus, antispam, antispyware y sistemas de filtrado de contenidos, asegurando una disponibilidad de estos servicios y complementándolo con una gestión, monitoreo y administración con tiempos de respuesta adecuados a los incidentes de seguridad que pudiesen surgir.




El monitoreo se llevará a cabo con una cobertura 7x24, los 365 días del año, y estará a cargo de un grupo de especialistas en tecnología de seguridad de información, quienes llevarán a cabo un correcto análisis en tiempo real y con la adecuada respuesta ante incidentes de seguridad que se pudieran suscitar en la operación del servicio.

## 6. Comunidades internacionales de seguridad

A partir del 30 de enero del 2007, Telefónica del Perú fue incorporada como miembro oficial del Forum of Incident Response and Security Teams (FIRST), organización líder creada en 1990 y la primera en ser reconocida a escala global, frente a la necesidad mundial de establecer contactos entre los equipos de respuesta ante situaciones de emergencia de las redes computacionales contra los ataques de los *hackers* y de virus, permitiendo a los miembros difundir las mejores prácticas de seguridad y generando entre ellos asistencia técnica, a través de los eventos internacionales y regionales de seguridad que se realizan cada año, así como a través de las publicaciones en las que se difunden las vulnerabilidades que acontecen en el día a día.

El FIRST trae consigo una gran variedad de equipos de respuesta a incidentes de seguridad, incluyendo equipos de productos de seguridad de áreas de gobierno, comerciales y académicas.

El Perú cuenta con el TERIS, que se integra a los más de 190 equipos que forman parte de la comunidad en cerca de 40 países, contribuyendo de esa manera a la prevención y detección temprana de los incidentes de seguridad, que son analizados por los distintos equipos que forman parte del FIRST, por lo cual su membresía le otorga los siguientes beneficios:

- Posibilidad de cooperación entre componentes de las tecnologías de la información en la prevención, detección y recuperación eficaces de los incidentes de seguridad de informática.
- Uso de los medios de comunicación de FIRST para la difusión de alertas y consejos sobre posibles situaciones emergentes que requieran el cuidado de los miembros.
- Posibilidad de generar acciones, incluyendo la investigación y actividades operacionales.
- Acceso al intercambio de información, herramientas y técnicas relacionadas con la seguridad entre sus miembros.

Es importante destacar que nuestro país fue anfitrión y auspiciador del Congreso Latinoamericano de Seguridad, que se realizó en Lima, del 13 al 18 de octubre del 2007.

En el congreso se mostraron las tendencias de la seguridad en las empresas líderes de Estados Unidos y Europa, las metodologías y mejores prácticas para una gestión eficiente de la seguridad; asimismo, se lle-

varon a cabo talleres y laboratorios con expertos y "gurús" mundiales de seguridad; se realizó una jornada completa de sesiones plenarias para las discusiones de los asuntos de interés para los miembros del FIRST, o lo que es más sensible en temas de seguridad y relacionado con el trabajo cotidiano de los participantes, seguido por un día de clases *hands-on*, donde los expertos internacionales de la seguridad se reunieron con grupos pequeños de los miembros del FIRST y trabajaron en asuntos técnicos de manera altamente interactiva.

## 7. Recomendaciones de seguridad para los usuarios finales

Actualmente, el manejo de la seguridad de la información se torna más complejo, a pesar de contar con muchas herramientas que facilitan este trabajo, por eso es muy importante orientar a los usuarios finales de los servicios para que tomen en cuenta las siguientes recomendaciones.

El *phishing* consiste en enviar correos electrónicos o cartas que aparentan ser escritos por entidades financieras (bancos, tarjetas de crédito, *paypal*, etcétera) solicitando al usuario que actualice determinados datos de su cuenta (usuario y contraseña) desde una página web que pertenece al delincuente informático. Se recomienda al usuario seguir estos consejos, que lo ayudarán a no ser una víctima de fraude:

- No acceda a la página del banco a través de enlaces ubicados en otras páginas o que reciba por correo electrónico.
- No responda a ninguna petición que le llegue por correo para actualizar sus datos o aviso de que se cerrará su cuenta bancaria.
- Nunca proporcione su usuario, número de documento de identidad ni clave en conversaciones telefónicas, electrónicas ni correos electrónicos.
- Si no está seguro de la página en la que va a ingresar sus datos para acceder a su cuenta, puede llamar a algún teléfono que ofrezca dicha entidad.

Con el fin de suplantar a otra persona, el delincuente informático puede cambiar de identidad en el correo electrónico. Si bien desde hace buen tiempo existe la firma digital, esta es usada por muy pocas personas. La cuestión pasa a ser de interés cuando comenzamos a tratar temas de mayor importancia a través del correo electrónico. En estos casos es conveniente usar la firma digital o encriptar la información.

La maniobra delictiva conocida como *ingeniería social* consiste en saber estudiar a determinado usuario para conocer sus movimientos, y

en función de eso elaborar una estrategia para invadir su computadora. Pongamos como ejemplo el siguiente caso: si un adolescente es fanático de un grupo de rock, un *hacker* podría enviarle un archivo comprimido diciéndole que contiene las fotos del último concierto de ese grupo; por lo que es muy probable que lo abra, lo cual alcanzaría para infectar la computadora. Es un ejemplo básico pero funciona con cierta regularidad. Lo que no quiere decir que no se deba abrir ningún archivo, sino que para hacerlo se debe verificar si procede de una fuente confiable, teniendo en cuenta, además, puntos de precaución importantes, que citaremos a continuación:

- Antivirus. Es una herramienta básica y primordial en todo usuario, pero no ayudará mucho si la base de datos de definiciones de virus que maneja para la prevención y detección no está actualizada. Se recomienda actualizar dicha herramienta desde la página web del proveedor y con no más de 15 días después de la última actualización.
- *Firewall.* Permite observar y establecer políticas de acceso en nuestra red, resulta fundamental para realizar detecciones tempranas de intrusos si se le da un uso adecuado. Es importante señalar que se recomienda instalarlo como una herramienta adicional, aparte de que algunos antivirus cuenten con esta opción.
- *Antispyware*. Los *spyware* son programas que espían la información que tenemos en nuestra PC y la envían a un extraño con distintos fines. Se recomienda tener un *antispyware* con el fin de que bloquee la instalación y el uso de estos programas. Su actualización debe tener la misma frecuencia que la de los antivirus.
- Puntos de restauración. Esta herramienta permite regresar a un estado anterior del sistema, en el caso de que existan errores o fallas después de ejecutado el antivirus o instalado algún programa. Se recomienda su uso para tener una fuente a la cual recurrir en caso de que se susciten fallas con el sistema. Cabe mencionar que esta herramienta solo restaura la estructura interna del sistema y de ninguna manera borra los archivos generados por el usuario.
- Actualizaciones y parches de seguridad. Para solucionar las fallas no previstas y actualizar la base de datos de los antivirus se deben descargar dichas actualizaciones y los parches de seguridad (programas adicionales de un software que lanza el proveedor) para subsanar los huecos (fallas descubiertas después de lanzado al mercado el software) del sistema. Se recomienda descargar dichas actualizaciones y parches de seguridad desde las páginas web de los proveedores de software.

- **Manejo de contraseñas.** Se recomienda emplear contraseñas diferentes para los distintos servicios que disponga el usuario; asimismo, es importante que sean complicadas de descifrar, para lo cual se utilizarán símbolos, números y mayúsculas, y no olvidar de cambiarlas cada cierto tiempo.
- **Sitios por los que navega.** Se debe tener la certeza de que los sitios desde los cuales va a descargar algún tipo de archivo sean seguros y que no puedan enviarle virus, *spyware* u otras amenazas a su PC. Muchos de los sitios que ofrecen programas u otros servicios gratuitos de distinta índole son una fuente de *spyware* y de troyanos.
- **Copias de seguridad.** Es de extrema importancia contar siempre con una copia de la información de mayor trascendencia que maneja, para lo cual se pueden utilizar herramientas informáticas que permitan realizar esta tarea periódicamente; así, en caso de pérdida pueda ser restablecida en el menor tiempo posible.
- **Encriptado de la información.** Para mantener la confidencialidad, estar libre del conocimiento de extraños o aun para ser enviada por la red, la información puede ser encriptada con técnicas que ya cuentan con muchos programas, y para desencriptarla en caso de que se necesite utilizar la información. Es recomendable tener cifrada la información que viaje en equipos portátiles como *notebooks*, *palmtops* o *pen drivers*.
- **Estar alerta ante nuevos tipos de ataques.** Para mantener nuestra PC o red seguras se debe estar lo más informado posible, ya que todos los días aparecen nuevas amenazas; con este propósito se puede suscribir a un boletín, que le enviará alertas de seguridad que ofrecen los distintos proveedores de antivirus o soluciones de seguridad.

## 8. Conclusiones

En la actualidad el tema de seguridad en las redes corporativas es fundamental en toda organización que pretende brindar a sus clientes una imagen de alta disponibilidad y respaldo a los servicios que ofrece; por ello, es necesaria la intervención de todos los actores (proveedores y clientes) con el fin de garantizar la seguridad de la información en todos los niveles, por medio de la aplicación de políticas de seguridad.

Como empresa proveedora de servicios de Internet, Telefónica del Perú es consciente de la importancia que tiene la gestión de la seguridad en sus redes, como un factor de suma relevancia pues permite brindar un servicio óptimo a sus clientes. Para ello se apoya en una infraestruc-

tura adecuada y en un personal idóneo, respaldados en los estándares internacionales y las comunidades de seguridad.

La gestión de la seguridad en las redes corporativas encuentra aún una gran limitación en muchas empresas, debido a la falta de toma de decisiones por parte de los directivos para implementar estos sistemas en sus organizaciones.

En toda organización es importante reconocer que los incidentes de seguridad que se perpetran a través de los ataques solo pueden ser mitigados, y cuanto más pronto se tomen decisiones sobre cómo organizar adecuadamente el entorno será una ventaja al momento de disminuir los riesgos de ataques a nuestra organización. Independientemente del monto invertido, si no existe un sistema de gestión de seguridad de los activos, así como el control respectivo de estos, que involucren al personal en las actividades respectivas, la empresa será vulnerable a estos ataques.

## Bibliografía

Forum of Incident Response and Secure Teams. "What's new in About FIRST", 5 de junio del 2007. [en línea] <http://www.first.org/about>. [Consulta: 5 de septiembre del 2007.]

Instituto Uruguayo de Normas Técnicas. "ISO / IEC 27000", 5. [en línea] <http://www.unit.org.uy/iso27000/iso27000.php> [Consulta: 6 de setiembre del 2007].

International Organization for Standarization. "Discover ISO", 8. [en línea] <http://www.iso.org/iso/about/discover-iso_meet-iso.htm> [Consulta: 8 de septiembre del 2007].

López Neira, Agustín. "Sistema de Gestión de la Seguridad de la Información", 14. [en línea] <http://www.iso27000.es/download/doc_sgsi_all.pdf>. [9 de septiembre del 2007].

Telefónica. Equipo de Respuesta a Incidentes de Seguridad. "Incidencias", 17 de julio del 2007. [en línea] <http://www.tp.com.pe/teris> [Consulta: 3 de septiembre del 2007].

Telefónica del Perú. "Manual del producto – Servicio de Seguridad Gestionada 2007". Lima. Versión 1.2. 2007.

Telefónica del Perú. "Manual del producto – Servicio de Antiphishing". Lima. Versión 1.4. 2007.