imperiasti

Liderar es Cumplir

PRINCIPIOS Y EVENTOS SOBRE SEGURIDAD DE LA INFORMACIÓN

Introducción

Como todos sabemos, la Previsibilidad, Disponibilidad, Continuidad y Protección de los Activos de Información son objetivos de especial atención.
En nuestro medio no hay una clara noción de su importancia, dado que sólo es tenida en cuenta en aquellos casos en que hay Entes Rectores, como el BCRA que regulan estos temas en las Instituciones Financieras o en empresas que se ven perjudicados ante hechos accidentales o intencionales, y luego de producida la pérdida consecuente.

El crecimiento y la expansión de los sistemas Informáticos, el acceso a la información que estos permiten, hacen que debamos concientizarnos de la importancia que tiene la seguridad en el manejo de los mismos y de la información en ellos contenida; muchos de los datos son de naturaleza confidencial y crítica para la Organización.
De allí el énfasis en el término "Protección de Activos de la Información" para lograr una adecuada protección de los recursos informáticos y de la información con que se cuenta.

De allí que todas las operaciones del negocio dependen de la disponibilidad y continuidad de las Operaciones.
Hoy más que nunca, cada uno de nosotros, debe entender que con la colaboración adecuada, se puede lograr la protección necesaria y el planeamiento de recuperación de desastres que aseguren la continuidad del negocio.
Para que sea posible, lo invitamos a considerarnos cuando decida evaluar los servicios ofrecidos, accediendo a herramientas adecuadas para el logro de los objetivos propuestos.

Objetivo

El objetivo de este documento es presentar un panorama de diferentes instancias propias de la Protección de Activos de Información, con el fin de colaborar en la concientización sobre la dependencia de los Servicios de Información, por lo cual las organizaciones son cada vez más vulnerables a las amenazas concernientes a la Seguridad de la Información.

El programa de concientización en la gestión de Protección de Activos de Información buscará una visión holística global de los servicios operativos y estratégicos de la seguridad, buscando la toma de conocimientos sobre la evolución en dicha materia, que facilite la comprensión del desempeño humano dentro del contexto tecnológico en el cual ocurre.

Estrategia de Protección de Activos de Información

La Estrategia de Protección de Activos de Información debe sentar las bases para concluir en Normas y Procedimientos que incluyan una estrategia **"Proactiva"** y otra **"Reactiva"**.

La estrategia **"proactiva"** o de previsión serán un conjunto de Procedimientos que coadyuven a reducir al mínimo la cantidad de puntos vulnerables existentes en el uso de los Sistemas Aplicativos, su tecnología asociada y los recursos humanos intervinientes y además desarrollar planes de Contingencia y Continuidad del Negocio.

La estrategia **"reactiva"**, también denominada **"Forense"** o posterior a una situación de ataque o crisis ayudará al personal de Protección de Activos de Información a evaluar el daño que se ha causado, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva a fin de normalizar la operatividad lo antes posible, a documentar y aprender de la experiencia, modificando y/o creando nuevos procedimientos que sos la y en los puntos vulnerables detectados, retroalimentando la estrategia **"Proactiva"**.

imperiasti

Liderar es Cumplir

Peligros en la web y en el correo electrónico

Internet es una herramienta de mucha utilidad y el uso descuidado, como por ejemplo el acceso a páginas de dudosa procedencia, puede provocar daños en su PC y a su privacidad.

Esto se realiza por medio de programas maliciosos que se introducen al sistema. Estos programas se dedican al robo de datos personales, a cuentas de crédito o pedidos de rescates, mientras que otros son utilizados con fines publicitarios. Estos ingresan por diferentes medios y los antivirus tradicionales no suelen detectarlos. Para eliminarlos se requieren programas especiales.

La capacitación y difusión a Directivos, Gerentes y personal para identificar este tipo de amenazas y denunciarlas, mejora en forma substancial la problemática. Es el mejor método de prevención.
Software malicioso: son programas también conocidos como malware (Programa maligno). Puede ser un virus que parece inocente, con alguna imagen en la pantalla que aparece y desaparece, hasta un virus que destruya toda la información. Este software es muy peligroso para las empresas, porque algunos programas fueron creados con propósitos criminales, tales como las transferencias de dinero, espionaje industrial, etc.

Software espía o spyware: registra todo lo que el usuario hace con el propósito de conocer sus preferencias y enviarle publicidad relacionada con su perfil.

Ransomware: o secuestro de Datos es un software malicioso que cifra los datos en un ordenador, impidiendo el acceso del legítimo propietario de la información, hasta que se pague una cantidad exigida de dinero. Es una de las amenazas más comunes a las que están expuestas hoy las organizaciones en todo el mundo. La mejor manera de defenderse contra ella es impidiendo que suceda. Y para ello, es necesario que este tema esté en la agenda de capacitaciones sobre seguridad de la información y protección de datos.

Scareware: Esto persuade a un usuario a comprar y descargar software no deseado y potencialmente peligroso al asustarlo. Scareware engaña a un usuario para que piense que su computadora tiene un virus, luego recomienda que descargue y pague por un software antivirus falso para eliminar el virus. Sin embargo, si el usuario descarga el software y permite que el programa se ejecute, sus sistemas se infectarán con malware.

Spearphishing: es el resultado de la evolución de esta práctica criminal. Mediante ella, los ciber-delincuentes pretenden legitimar un correo electrónico, para un grupo definido de destinatarios. En este correo, aparentemente dirigido desde un supuesto alto cargo u organismo validado, se esconde un archivo de malware.

Spam: consiste en todo lo que el usuario recibe en su casilla de correo electrónico sin haberlo solicitado.

Hay diferentes tipos de spam que pueden llegar a nuestra Bandeja de Entrada. Entre estos se destacan los más perjudiciales como el Hoaxes, los Fraudes y los Scams.

- ***Hoaxes o bromas de mal gusto:*** Un mail que invita a hacer algo que resulta perjudicial. Hace creer al usuario que debe hacerlo para evitarse problemas. Una broma que circuló hace un tiempo invitaba a buscar en la máquina un archivo determinado, diciendo que si estaba implicaba que la máquina se encontraba infectada y que la única forma para solucionarlo era borrarlo inmediatamente. Se trataba en realidad de un archivo esencial del sistema operativo, por lo que nuestra máquina dejaba de arrancar a partir de entonces (por ejemplo, archivos tales como jdbmgr.exe, sulfbnk.exe, esenciales para el sistema operativo).

imperiasti

Liderar es Cumplir

- ***Frauds o fraudes:*** Un mail que implica un comportamiento deshonesto, cuyo objetivo es hacer dinero, donde alguien se hace pasar por quien no es, o nos hace creer algo que no es cierto, sugiriendo que sigamos un procedimiento por el cual seremos perjudicados económicamente.

- ***Scams:*** Los Scams son una forma de Fraude. Se trata de un mail que atrae el interés del usuario y que esconde una maniobra deshonesta. En algunos casos ofrece ganar dinero fácilmente, para lo cual hace una propuesta que, al seguirla, pondrá en grave riesgo el patrimonio del usuario e incluso su buen nombre y honor. A modo de ejemplo, podemos citar un mail que da la noticia de que se ha ganado un importante premio de lotería o que un señor africano (Nigerian Scam) tiene que cobrar mucho dinero y tiene un impedimento para hacerlo en su país y necesita que el usuario se lo cobre. O que un software malicioso se ha instalado en el equipo y tiene fotos comprometidas de la persona por la cual pide un rescate.

- ***Phishing:*** o Suplantación de identidad; se recibe un mail proveniente, en apariencia, de una entidad de reconocida trayectoria y que invita a visitar el Web Site de la empresa para actualizar datos. El vínculo en realidad lo remite a una página falsa con la intención de robar datos personales, que puede incluir incluso número de cuenta bancaria y palabra clave. Aun cuando en esa página no complete ningún dato el sólo hecho de haber ingresado lo expone a un ataque. Existe una organización que lucha contra el Phishing, Scam y otros fraudes, cuya dirección es: www.antiphishing.org. Para evitar este tipo de engaño siempre es necesario ver el dominio (identidad) de la página web que se visita. Como por ejemplo estar atento a la extensión y nos daremos cuenta que es falso.

- ***Smishing:*** Es otra forma de phishing que usa mensajes de texto SMS para engañar a los usuarios, se suele emplear en paralelo con llamadas de voz dependiendo de los métodos del atacante.

- ***Pharming:*** Es más difícil de detectar, ya que a diferencia del Phishing, la persona que sufre el Pharming visita un Web Site malicioso en forma totalmente inadvertida. Se debe a que el proveedor del servicio de Internet sufrió un ataque en su DNS , el cual quedó "envenenado". A raíz de que el DNS quedó envenenado, ponemos correctamente el lugar que queremos visitar, pero el DNS nos manda a un lugar incorrecto: un Web site malicioso donde sufriremos un ataque a nuestra privacidad. Es responsabilidad del Proveedor de Servicios de Internet proteger el DNS para que esto no ocurra.

- ***Vishing:*** La mayoría de las personas han oído hablar del phishing; sin embargo, aunque el vishing es un ataque diferente, está dentro de la misma clasificación que el phishing y tiene objetivos en común. Los vishers, como se conoce a los perpetradores de estas técnicas usan números telefónicos fraudulentos, software de modificación de voz, mensajes de texto e ingeniería social para convencer a los usuarios de que divulguen información delicada. En el vishing generalmente se usa la voz para engañar a los usuarios.

¿CUÁL ES LA DIFERENCIA ENTRE VISHING Y PHISHING?

El phishing y el vishing persiguen el mismo objetivo: obtener información confidencial de las personas que podría usarse para robo de identidad, obtener beneficios financieros o apoderarse de cuentas. La diferencia principal entre el phishing y el vishing es el medio que se emplea para identificar a las potenciales víctimas. Si bien el phishing es un ataque basado principalmente en correo electrónico, el vishing emplea la voz, típicamente mediante llamadas al móvil de un usuario.

En todos los casos los delincuentes y estafadores emplean tácticas de intimidación para convencer a los usuarios de que hagan una llamada telefónica o que respondan ante a la consulta de un IVR dando opciones para aceptar, por ejemplo un beneficio de ANSES, deudas con la AFIP, o el mensaje intimidante que “se instaló un agente en su computadora” y desde hace tiempo viene recogiendo información, tienen fotos comprometedoras, y que si no pagan un rescate en Bitcoins será publicadas en las redes y todos los contactos de la víctima.

imperiasti

Liderar es Cumplir

Estos tipos de mensajes sean por correo electrónicos, mensajes de texto (SMS), de WhatsApp o telefónicos, el atacante simula tener datos precisos de la víctima y trata de convencer al damnificado que pague con Bitcoins, su tarjeta de crédito o que transfiera dinero directamente desde la cuenta del usuario a cuentas "Mula" desde las cuales luego los ciberdelincuentes las transfieren varias veces hasta que llegan a su poder.

Estafas Bancarias

Con el avance de la bancarización en todos los estratos sociales y la digitalización del dinero también creció el robo de datos y las estafas virtuales.

Los fraudes y las estafas virtuales siguen aumentando y sofisticándose en la medida que continúa creciendo la digitalización y la bancarización mediante el uso de medios de pagos digitales y de billeteras virtuales. Los ciberdelincuentes aplican nuevas formas de fraudes y estafas y muchas veces resulta difícil prevenirlas. Una de las más comunes es la que está **directamente vinculada** con Correos electrónicos y/o llamadas telefónicas que tiene como objetivo robar las claves personales de home banking para hacerse del dinero de las cuentas. Mientras que otro de los métodos delictivos más identificados es el del pedido de descarga e instalación de aplicaciones en celulares y computadoras. Se trata de programas que permiten a los estafadores acceder a la visualización de lo que se está realizando en la pantalla de los dispositivos para robar datos personales.

En sí el método que venimos definiendo conocido como ***"phishing"*** o la suplantación de identidad es un mecanismo que se utiliza para conseguir información confidencial de forma fraudulenta y así apropiarse de la identidad digital de las personas. Estar alerta e informado/a, así como custodiar celosamente la información confidencial, da la posibilidad de prevenir cualquier vulneración que ponga en riesgo el bienestar financiero de las personas.

Por esto mismo nunca se deben dar a conocer datos personales como respuesta a una llamada telefónica, ya que el Banco jamás se contactará con sus clientes para pedir información sensible y confidencial como usuarios y contraseñas de home banking.

En caso de recibir un mensaje de WhatsApp, SMS o un llamado telefónico de un número privado o desconocido es importante tener en cuenta que pueden provenir de destinatarios falsos que buscan concretar algún tipo de delito virtual, por lo que no se deben dar a conocer claves, usuarios ni códigos como el Token, además de información personal relevante.

¿Sabés cómo reconocer un mail o mensaje falso?

Considera estos tips que te pueden servir para cuidarte y estar prevenido:

- Ninguna Entidad Financiera nunca te va a solicitar que reveles tus claves o información personal a través de correos electrónicos, ni SMS, ni por páginas de Internet a las que se ingrese desde un correo o mensaje. Tampoco van a solicitarte la contraseña (Clave) de tu correo electrónico, es personal y no la necesitan. Ninguna persona o sector de un banco necesita tus claves.
- Si recibís un mail raro y el dominio no es oficial del Banco, sospechá. Podés revisarlo apretando la foto de perfil, al lado del nombre de usuario (App de Gmail, Android), o apretando dos veces en el nombre de usuario (App de Mail, IOS).
- No te dejes apurar.
- Los mails falsos suelen decir cosas como "Home Banking bloqueado" o "en 48 hs se bloqueará tu cuenta". Nunca van a comunicarte esa forma. Los correos importantes van a venir de nuestros dominios oficiales o de las páginas oficiales.

imperiasti

Liderar es Cumplir

- Si alguien te pide tus claves, no se las des. Son las llaves de tu cuenta. Solamente las tienes que usar para ingresar a los diferentes canales que te ofrecen las Entidades Bancarias (Home Banking, App Banco para celulares o Banca Telefónica).
- Todas las entidades financieras tienen correos para hace denuncias sobre Ciberseguridad, pueden allí efectuar la consulta o redireccionar lo recibido.
- Utiliza doble factor de autenticación para ingresar desde los celulares y cierra la sesión al finalizar.
- Si accedes desde una computadora, utiliza un antivirus actualizado antes de abrir los archivos.
- Nunca entres desde computadoras de uso público o que desconozcas su mantenimiento.
- No abras ni ejecutes archivos terminados en ".exe".
- Nunca instales programas desconocidos.
- Utilizá programas con licencias oficiales.
- En accesos las cuentas de Redes oficiales siempre chequeá que tengan **"el tilde azul"**.
- Nunca pagues rescates, recurre a especialistas de confianza que te guiarán o te ayudarán a superar el inconveniente.

Suplantación de Identidad.

Existe una nueva modalidad de estafa a través de la usurpación de tu identidad en la aplicación "Whatsapp". En este caso los usurpadores o estafadores se contactan con vos, y mediante una excusa solicitan que confirmes tu identidad. Los motivos que suelen dar se relacionan con una nueva actualización de Whatsapp, la habilitación de un turno para la vacuna de Covid-19, o cualquier otra excusa por la que necesiten **"confirmar que sos vos".**

Para comprobar que la persona a la que se están dirigiendo es la propietaria de la cuenta, los estafadores te solicitan que compartas un código de seguridad de seis dígitos que vas a recibir vía SMS.
Al compartir este código, los estafadores toman control de tu cuenta y pueden iniciar sesión en otro dispositivo, accediendo al detalle de tus contactos y el historial de tus conversaciones.
Con toda esta información, los estafadores hacen ingeniería social con tus contactos en base a tus últimas conversaciones, y se contactan en tu nombre para:
Solicitar que transfieran dinero a un tercero por una urgencia.

Ofrecer dólares de un supuesto amigo tuyo que necesita venderlos urgente y pasar los datos de una cuenta para realizar una transferencia.
Cualquier otro motivo que incluya el envío de fondos a terceros.
De la misma manera, si alguno de tus contactos sufrió una usurpación de identidad a través de esta modalidad, podrías recibir mensajes por parte de los estafadores pensando que se trata de tu contacto genuino.
Para prevenir que seas estafado por esta modalidad, las recomendaciones son:

- Nunca respondas mensajes de Whatsapp o SMS desconocidos.
- No compartas con terceras personas códigos de seguridad que recibas a través de SMS o mensajes de Whatsapp.
- Para una mayor seguridad al utilizar Whatsapp, activá la verificación en dos pasos con PIN y/o E-mail como una barrera más de seguridad para el ingreso a tu cuenta y la recuperación. Podés hacerlo a través de Ajustes > Cuenta > Verificación en dos pasos.

- Si confirmas que tu cuenta ha sido hackeada, tendrás que inmediatamente contactar al soporte técnico de tu compañía de celular. La empresa inmediatamente te enviará un código de verificación al cual solamente vos tendrás el acceso. Inmediatamente publica en el “Estado de Whatsapp” alertando a tus contactos que te encuentras bien y no respondan ningún pedido de transferencias de dinero.

- En la actualidad, Whatsapp permite que te puedas conectar en varios dispositivos al mismo tiempo. Teniendo en cuenta esta situación, si en algún momento identificas alguna conexión sospechosa inmediatamente podrás deshabilitar su ingreso. Si consideras que tu actividad es inusual o que espían tu cuenta, podrás percatarte a través de mensajes extraños que hayan sido enviados a otros contactos. Para evitar mayores inconvenientes te recomendamos seguir los siguientes pasos:

    - Deberás acceder a los ajustes de WhatsApp.

    - Posteriormente, presionar sobre “dispositivos vinculados” y verificar los inicios de sesión de tu cuenta. En la aplicación se detalla el horario y lugar de cada acceso.

    - El último paso es bastante sencillo. En esta instancia deberás identificar si alguna de las cuentas vinculadas es de tu total desconocimiento, y si esto es correcto, tendrás que cerrarlo de inmediato. Presiona sobre el acceso que sospechas y presionar la opción marcada en Rojo “Cerrar sesión”.

Gestión de Evaluación de Riesgos

El Riesgo es todo evento contingente que, de materializarse, puede impedir o comprometer el logro de los objetivos.

La Gestión de Evaluación de Riesgos es un proceso estructurado, consistente y continúo implementado a través de toda la organización para: identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos.

Todos en la organización juegan un rol en el aseguramiento de éxito de la Gestión de Riesgos, pero la responsabilidad principal de la identificación y manejo de éstos recae sobre la dirección.
Los Riesgos requieren ser identificados (amenazas) y administrados (vulnerabilidades), para lo cual el Servicio utilizará la gestión de riesgos como herramienta fundamental para el logro de sus objetivos.

Amenazas

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema o los elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso.

Desde el punto de vista de la organización que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos y también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos.

Generalmente se distingue y divide tres grupos

- **Criminalidad:** son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.

- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.

- **Negligencia y decisiones institucionales:** son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

Las amenazas más preocupantes

- Ataques de virus (>50%)
- Robo de celulares, portátiles y otros equipos (>40%)
- Falta de respaldo de datos
- Perdida de información por rotación, salida de personal
- Abuso de conocimientos internos (no consultado en encuesta de organizaciones sociales)
- Mal manejo de equipos y programas
- Acceso non-autorizado, etc.

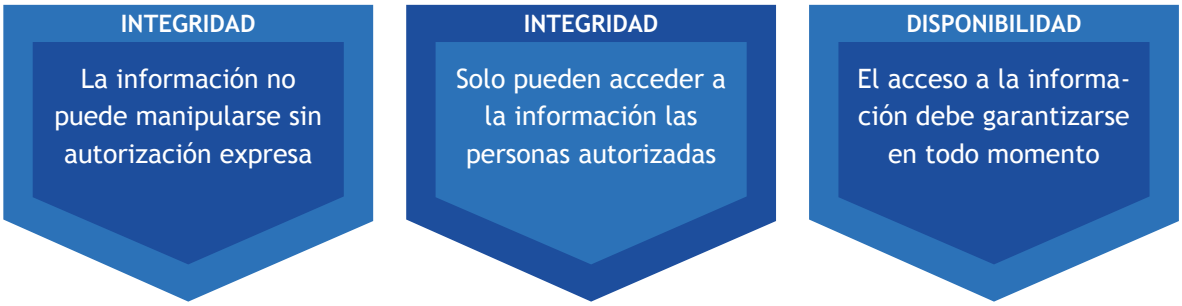
Vulnerabilidades

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño].

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Aspectos de la Política de Seguridad de la Información

OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN



imperiasti

Liderar es Cumplir

Algunos aspectos principales son establecer controles de seguridad para las aplicaciones que procesen datos, entre ellas:

- ✓ Segmentación de roles y perfiles (Administradores, Usuarios, etc.)
- ✓ Autenticación segura de Usuarios
- ✓ Implementar reglas y controles de seguridad en los servidores que estén conectados a una red externa y almacenen o gestionen datos, programando alertas ante posibles ataques.
- ✓ Segmentar en forma física o lógica la red de la Organización, separando las áreas públicas de las privadas.
- ✓ Separar los ambientes de Producción, QA, Prueba y Desarrollo.
- ✓ Implementar controles para la prevención de virus informáticos en los servidores que almacenen o gestionen datos.
- ✓ Implementar controles para la prevención de ataques en las estaciones de trabajo que gestionen datos.
- ✓ Implementar controles para la prevención de virus informáticos en las estaciones de trabajo que gestionen datos.
- ✓ Establecer y ejecutar un procedimiento de actualización periódica de software/hardware de todo el equipamiento.
- ✓ Establecer procedimientos de Gestión de Incidentes de Seguridad de la Información.
- ✓ Gestionar Riesgos y Vulnerabilidades.
- ✓ Definir a una persona responsable del cumplimiento de las medidas de seguridad.
- ✓ Perímetro de Seguridad Física. (Áreas protegidas, control de accesos físicos, Seguridad del Cableado).
- ✓ Continuidad: Copias de Seguridad, suministros de energía, pruebas, etc.
- ✓ Mecanismos de distribución de Información.
- ✓ Desafectación y/o reubicación de equipos, etc.

Recomendaciones

Mantenga actualizado el software. Es muy importante contar con un buen antivirus y un antispyware. También actualice cada 15 días su antivirus y su Sistema Operativo. Esto será programado en su equipo y no debe ser modificado.
Utilice exploradores que no tengan muchas fallas de seguridad, como Google, Microsoft Edge o Explorer, Firefox.

Sea cuidadoso con los lugares que visita y mucho más cuando esos lugares le hacen instalar programas especiales, por ejemplo "dialers" o marcadores telefónicos que, en algunos casos, pueden marcar números que van a tomar el control de tu teléfono o Whatsapp. Como resultado de su visita puede tener instalado un espía en su máquina que va a informar al dueño de la página todo lo que usted hace minuto a minuto.

Sea cuidadoso con los correos que abre. No basta conocer el emisor para abrir el correo con confianza, ya que no existe ningún mecanismo para autenticar el nombre del remitente. La persona que envía puede colocar en el campo "De" o "From" el nombre o la frase que desee, y este nombre es el que se muestra en el mensaje al recibirse.

Cualquier correo, cualquiera sea el asunto que un mensaje tenga, puede ser contaminante (es sencillo para un programador emitir mensajes con el mismo contenido malicioso y cientos de asuntos distintos).

Si la redacción del mail no concuerda con lo que habitualmente suele recibir del remitente, no lo abra. Mucho menos si tiene un Link o vínculo a sitios que le propongan.

imperiasti

Liderar es Cumplir

- Verifique por e-mail o teléfono si realmente esa persona amiga/conocida le mandó ese mail y, sólo una vez verificado que no existen problemas, proceda a abrirlo.

- O en caso contrario elimínelo rápidamente para evitar cualquier contratiempo.

Salvo circunstancias muy especiales no se haga partícipe de cadenas de mails o mensajes de Whatsapp, ni creas en frases que le incentivan a participar en las mismas diciendo algo así como: "Atención: no es una broma, funciona. Entonces, date gusto, regálate…", etc.

Utilice la opción "copia oculta" para enviar mails masivos. Les evitarás problemas a los destinatarios ya que el mail, en camino a su destinatario pasa por equipos intermedios que tienen acceso al contenido del mensaje, y pueden utilizarse para recopilar direcciones para después utilizarlas para enviar correo SPAM.
S
i tienes contratada banda ancha, la cual no paga por tiempo de conexión, no la dejes "conectada" en forma permanente las 24 horas del día, ya que el tiempo prolongado de conexión aumenta la probabilidad de éxito de un eventual atacante que encuentre su máquina al barrer, al azar, direcciones de Internet. Si el atacante tiene éxito, debido a vulnerabilidades no protegidas del sistema, puede instalar en la máquina programas maliciosos o incluso utilizarla como iníciate de otros ataques dirigidos a terceras máquinas.

Solamente llene formularios en la WEB en los que se esté utilizando el protocolo https:// (utiliza un Servidor Seguro con encriptación -ilegible para alguien que lo "atrapa" en el medio e intenta leer- de datos entre el Servidor y su máquina), en lugares que le merezcan confianza, y solamente en los casos en los que el llenarlo le proporcione un real beneficio (por ejemplo, acceso a información que usted necesita consultar).

Recomiende a sus allegados que no den ninguna clase de dato respecto a su propia persona ni de ningún familiar directo y que el uso que le den al Chat sea el mismo tanto en presencia de los padres como en ausencia de estos.

Considere seriamente, también, la ubicación de la PC en un área "pública" de la casa (un lugar donde la pantalla esté siempre a la vista de los padres). Instale programas para evitar que sus hijos accedan a páginas prohibidas.

No confíe ciegamente en lo que está publicado en INTERNET. Cualquiera puede publicar lo que quiera y no existe un órgano fiscalizador que controla que lo que está publicado en la WEB no sea malicioso ni que sea verdadero. Procure seleccionar lo que consulta tratando de quedarse con aquello que sea realmente confiable. Sea crítico al analizar el contenido, y deseche páginas o "sites" completos donde observe errores, inexactitudes, superficialidad u otro atributo que le hagan perder confianza en lo allí publicado.

NIC (Network Information Center), es el organismo que administra y registra los dominios en argentina y el mundo. Usted puede visitar www.nic.ar y ver quiénes son los responsables de los sitios que usted visita, en Argentina.

¿Sospecho que mi máquina está infectada?

Existen algunos indicios que pueden despertar sospechas en el usuario sobre si su equipo se encuentra infectado. Si bien esto no funciona a ciencia exacta, se pueden tener en cuenta algunos aspectos a la hora de prestar atención al funcionamiento cotidiano del equipo. Algunos síntomas para sospechar son:

imperiasti

Liderar es Cumplir

Se muestran ventanas (pop-ups) o imágenes repentinamente.

En caso de contar con un firewall, este informa de ciertas aplicaciones que intentan conectarse a diferentes direcciones de internet sin que el usuario haya ejecutado ninguna de las mismas.

Los contactos del usuario mencionan que han recibido correos o mensajes por alguna red social sin que el usuario los enviara.

El sistema operativo demora más de lo habitual para iniciarse.

Además de estos síntomas, existen muchos otros que permiten sospechar si se está frente a un equipo infectado.

¿Qué debo hacer?

Si se cree que el equipo se encuentra infectado con algún tipo de malware, se pueden seguir ciertos consejos para no comprometer la información disponible en dicho sistema, así como tampoco sufrir del robo de datos de origen crítico.

Desconectar el equipo de Internet: Esto impedirá que el malware que infectó el equipo continúe propagándose por la red así como también una posible reinfección online luego de la limpieza.

Si no se posee un programa antivirus, instalar alguno en esta instancia: Siempre es recomendable algún software con capacidad de detección proactiva de amenazas. Descargar y actualizar la base de firmas del antivirus instalado previamente para contar con la última actualización y así poder realizar un análisis del equipo más eficiente.

Realizar un análisis completo del sistema, con la opción ante del inicio de Windows que la mayoría de los Antivirus poseen. Efectuar un análisis completo de los discos del equipo en busca de amenazas.

Modificar las contraseñas de los correos, cuentas de redes sociales y cualquier servicio que requiera autenticación: Este procedimiento debe efectuarse para eliminar toda posibilidad de robo de credenciales por parte del cibercriminal detrás del malware.

En caso de ser necesario, realizar una limpieza manual: Muchas veces luego de una infección no es suficiente escanear el sistema y realizar una limpieza automatizada. Es por esto que en ciertas ocasiones se debe efectuar una limpieza manual. Para poder llevar a cabo esta tarea, es recomendable identificar de qué tipo de malware se trata para luego buscar el método correcto de desinfección.

Estos pasos son un buen punto de partida en el caso que se sospeche que el equipo ha sido infectado por malware. Además, esto debe complementarse con la serenidad por parte del usuario, es decir, no entrar en pánico, ya que muchas veces esto puede derivar en acciones que comprometan aún más el sistema.

Finalmente, en el caso de que se confirme la infección, se le recomienda al usuario contactar con personal especializado que efectúe la desinfección y recupero del sistema.