ANTOLOGIA

SEGURIDAD DE LA INFORMACIÓN

INGENIERÍA EN SISTEMAS COMPUTACIONALES

9°CUATRIMESTRE

Marco Estratégico de Referencia

ANTECEDENTES HISTORICOS

Nuestra Universidad tiene sus antecedentes de formación en el año de 1979 con el inicio de actividades de la normal de educadoras "Edgar Robledo Santiago", que en su momento marcó un nuevo rumbo para la educación de Comitán y del estado de Chiapas. Nuestra escuela fue fundada por el Profesor de Primaria Manuel Albores Salazar con la idea de traer Educación a Comitán, ya que esto representaba una forma de apoyar a muchas familias de la región para que siguieran estudiando.

En el año 1984 inicia actividades el CBTiS Moctezuma Ilhuicamina, que fue el primer bachillerato tecnológico particular del estado de Chiapas, manteniendo con esto la visión en grande de traer Educación a nuestro municipio, esta institución fue creada para que la gente que trabajaba por la mañana tuviera la opción de estudiar por las tarde.

La Maestra Martha Ruth Alcázar Mellanes es la madre de los tres integrantes de la familia Albores Alcázar que se fueron integrando poco a poco a la escuela formada por su padre, el Profesor Manuel Albores Salazar; Víctor Manuel Albores Alcázar en septiembre de 1996 como chofer de transporte escolar, Karla Fabiola Albores Alcázar se integró como Profesora en 1998, Martha Patricia Albores Alcázar en el departamento de finanzas en 1999.

En el año 2002, Víctor Manuel Albores Alcázar formó el Grupo Educativo Albores Alcázar S.C. para darle un nuevo rumbo y sentido empresarial al negocio familiar y en el año 2004 funda la Universidad Del Sureste.

La formación de nuestra Universidad se da principalmente porque en Comitán y en toda la región no existía una verdadera oferta Educativa, por lo que se veía urgente la creación de una institución de Educación superior, pero que estuviera a la altura de las exigencias de los jóvenes que tenían intención de seguir estudiando o de los profesionistas para seguir preparándose a través de estudios de posgrado.

Nuestra Universidad inició sus actividades el 18 de agosto del 2004 en las instalaciones de la 4ª avenida oriente sur no. 24, con la licenciatura en Puericultura, contando con dos grupos de cuarenta

alumnos cada uno. En el año 2005 nos trasladamos a nuestras propias instalaciones en la carretera Comitán – Tzimol km. 57 donde actualmente se encuentra el campus Comitán y el Corporativo UDS, este último, es el encargado de estandarizar y controlar todos los procesos operativos y Educativos de los diferentes Campus, Sedes y Centros de Enlace Educativo, así como de crear los diferentes planes estratégicos de expansión de la marca a nivel nacional e internacional.

Nuestra Universidad inició sus actividades el 18 de agosto del 2004 en las instalaciones de la 4ª avenida oriente sur no. 24, con la licenciatura en Puericultura, contando con dos grupos de cuarenta alumnos cada uno. En el año 2005 nos trasladamos a nuestras propias instalaciones en la carretera Comitán – Tzimol km. 57 donde actualmente se encuentra el campus Comitán y el corporativo UDS, este último, es el encargado de estandarizar y controlar todos los procesos operativos y educativos de los diferentes campus, así como de crear los diferentes planes estratégicos de expansión de la marca.

MISIÓN

Satisfacer la necesidad de Educación que promueva el espíritu emprendedor, aplicando altos estándares de calidad Académica, que propicien el desarrollo de nuestros alumnos, Profesores, colaboradores y la sociedad, a través de la incorporación de tecnologías en el proceso de enseñanza-aprendizaje.

VISIÓN

Ser la mejor oferta académica en cada región de influencia, y a través de nuestra Plataforma Virtual tener una cobertura Global, con un crecimiento sostenible y las ofertas académicas innovadoras con pertinencia para la sociedad.

VALORES

- Disciplina
- Honestidad
- Equidad
- Libertad

ESCUDO

El escudo de la UDS, está constituido por tres líneas curvas que nacen de izquierda a derecha formando los escalones al éxito. En la parte superior está situado un cuadro motivo de la abstracción de la forma de un libro abierto.

ESLOGAN

"Mi Universidad"

ALBORES

Es nuestra mascota, un Jaguar. Su piel es negra y se distingue por ser líder, trabaja en equipo y obtiene lo que desea. El ímpetu, extremo valor y fortaleza son los rasgos que distinguen.

SEGURIDAD DE LA INFORMACIÓN

Objetivo de la materia:

Desarrolla e Implementa Planes de Seguridad basado en normas y estándares internacionales para el aseguramiento de los activos de la organización y la continuidad del negocio, además de aporta al perfil del Ingeniero Informático las capacidades de aplicar conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario; de seleccionar y utilizar de manera óptima técnicas y herramientas computacionales actuales y emergentes; y la aplicación de normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información.

UNIDAD I INTRODUCCIÓN A LA SEGURIDAD INFORMACIÓN

1.1 El valor de la información.

1.2 Definición y tipos de seguridad información.

1.3 Objetivos de la seguridad información.

1.4 Posibles riesgos en la información.

1.5 Técnicas de aseguramiento del sistema.

1.6 Criptografía clásica: Un primer acercamiento.

1.7 Criptografía en la antigüedad.

1.8 Cifradores del siglo XIX.

1.9 Criptosistemas clásicos.

1.10 Máquinas de cifrar (siglo XX).

1.11 Estadística del lenguaje.

1.12 Ejemplos de la estadística del lenguaje.

UNIDAD II CERTIFICADOS Y FIRMAS DIGITALES

2.1 Distribución de claves.

2.2 Certificación.

2.3 Componentes de una PKI.

2.4 Arquitecturas PKI

2.5 Políticas y prácticas de certificación.

2.6 Gestión de una PKI.

2.7 Estándares y protocolos de certificación

2.8 Ejemplo de un protocolo de seguridad: HTTPS.

2.9 SSL

2.10 TSL

2.11 SSH

UNIDAD III SEGURIDAD EN REDES

3.1 Aspectos de seguridad en las comunicaciones

3.2 Debilidades de los protocolos TCP/IP.

3.3 Transmisión de paquetes y promiscuidad.

3.4 Redes locales (VLAN) y amplias (VPN)

3.5 Domicilios IP.

3.6 Vigilancia de paquetes

3.7 Estándares para la seguridad en redes.

3.8 Vulnerabilidad de los protocolos inalámbricos WEP, WPA, WPA2.

3.9 Firewall de capas inferiores.

3.10 Firewall de capa de aplicación.

3.11 Firewall personal.

3.12 Ventajas de un firewall.

3.13 Limitaciones de un firewall.

3.14 Políticas del firewall

3.15 Enlaces externos.

UNIDAD IV VIGILANCIA DE LOS SISTEMAS DE INFORMACIÓN Y HACKING

4.1 Definición de vigilancia.

4.2 Anatomía de un ataque

4.3 Escaneos.

4.4 Identificación de vulnerabilidades

4.5 Actividades de infiltración.

4.6 Consolidación.

4.7 Defensa perimetral.

4.8 Ética de hacking.

4.9 Introducción a Kali Linux.

4.10 Penetración I

4.11 Penetración II.

Índice

UNIDAD I INTRODUCCIÓN A LA SEGURIDAD INFORMACIÓN

1.1 El valor de la información.

La información tiene un gran impacto en la toma de decisiones. Aunque no tiene valor absoluto, su valor está relacionado con quién la usa y en la situación de uso.

- *El valor normativo de la información*: Se refiere al conocimiento a priori o preliminar que tenemos acerca de la ocurrencia de los eventos los cuales son relevantes para nuestras decisiones (probabilístico).
- *El valor realístico de la información*: Es el de reconocer que la información apoya las decisiones. Las acciones tomadas afectan a los logros de desempeño.
- *El valor subjetivo de la información*: Refleja la impresión comprendida de la gente para la información.
- *Beneficios tangibles:* Reducción en los niveles de inventario, en la línea de crédito, en horas-hombre, incremento de ventas y reducción en los costos de mantenimiento.
- *Beneficios intangibles:* Mejora de los procesos de toma de decisiones; amplía los horizontes de planeación; extiende las bases de información para la toma de decisiones; facilita la integración de datos.

La inversión en tecnologías de la información no lleva a ninguna parte si no va acompañada de una utilización inteligente de la información que las tecnologías nos permiten gestionar. El éxito, el retorno de la inversión, en la aplicación de las tecnologías de la información en una organización depende de que ayuden a utilizar mejor la información generada en los procesos. El valor de la tecnología es, pues, el valor que se deriva del mejor uso de la información capturada y gestionada con la tecnología.

Sistemas de información y tecnología

La tecnología en un sistema de información se refiere a aquellos dispositivos como hardware, bases de datos, software, redes y otros que se emplean para procesar la

información. Es decir, alcanzar la meta principal del sistema de información: transformar en forma económica los datos y procesos en conocimiento.

Para entender mejor este concepto se requiere el análisis de cada uno de sus componentes:

- Datos: son descripciones básicas de cosas, acontecimientos, actividades y transacciones que se registran, clasifican y almacenan. Pueden ser datos numéricos, alfanuméricos, figuras, sonidos e imágenes.
- Información: representa datos organizados que han adquirido valor y significado para el receptor.
- Conocimiento: se constituye de datos o información que se ha organizado y procesado de tal forma que sea entendible.

1.2 Definición y tipos de seguridad información.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas).

En el caso de los virus hay que subrayar que en la actualidad es amplísima la lista de ellos que existen y que pueden vulnerar de manera palpable cualquier equipo o sistema informático. Así, por ejemplo, nos encontramos con los llamados virus residentes que son aquellos que se caracterizan por el hecho de que se hallan ocultos en lo que es la memoria RAM y eso les da la oportunidad de interceptar y de controlar las distintas operaciones que se realizan en el ordenador en cuestión llevando a cabo la infección de programas o carpetas que formen parte fundamental de aquellas.

De la misma forma también están los conocidos virus de acción directa que son aquellos que lo que hacen es ejecutarse rápidamente y extenderse por todo el equipo trayendo consigo el contagio de todo lo que encuentren a su paso.

Los virus cifrados, los de arranque, los del fichero o la sobreescritura son igualmente otros de los peligros contagiosos más importantes que pueden afectar a nuestro ordenador.

Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords).

Herramientas todas ellas de gran utilidad como también lo son los conocidos sistemas de detección de intrusos, también conocidos como anti-spyware. Se trata de programas o aplicaciones gracias a los cuales se puede detectar de manera inmediata lo que son esos programas espías que se encuentran en nuestro sistema informático y que lo que realizan es una recopilación de información del mismo para luego ofrecérsela a un dispositivo externo sin contar con nuestra autorización en ningún momento. Entre este tipo de espías destaca, por ejemplo, Gator.

Un sistema seguro debe ser íntegro (con información modificable sólo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente para los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).

De todas formas, como en la mayoría de los ámbitos de la seguridad, lo esencial sigue siendo la capacitación de los usuarios. Una persona que conoce cómo protegerse de las amenazas sabrá utilizar sus recursos de la mejor manera posible para evitar ataques o accidentes.

En otras palabras, puede decirse que la seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una organización o un usuario lo ha decidido, sin intromisiones.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Tipos de Seguridad Informática

- Seguridad Física

La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención para que no le ocurra nada al ordenador, la seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático.

Por Ejemplo: Incendios, inundaciones, terremotos, instalación eléctrica, entre otros.

- Seguridad Lógica

Nuestro sistema no sólo puede verse afectado de manera física, sino también contra la Información almacenada, El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren.

Por Ejemplo: Control de acceso, autenticación, encriptación, firewalls, antivirus (en caso de Usar Windows).

1.3 Objetivos de la seguridad información.

Si estudiamos las múltiples definiciones que de seguridad informática dan las distintas entidades, deduciremos los objetivos de la seguridad informática. Según la IS027002, "La seguridad de la información se puede caracterizar por la preservación de:

- Confidencialidad: asegura que el acceso a la información está adecuadamente autorizado.
- Integridad: salvaguarda la precisión y completitud de la información y sus métodos de proceso

- Disponibilidad: Asegura que los usuarios autorizados pueden acceder a la información cuando la necesitan".

Otra de las definiciones de lo seguridad informática dada por INFOSEC Glossary 2000: "Seguridad Informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican". De estas definiciones podemos deducir que los principales objetivos de la seguridad informática son:

• **Confidencialidad**: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrentan muchas empresas; en los últimos años se ha incrementado el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio …etc.

• **Disponibilidad:** la definiremos como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

• **Integridad:** diremos que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

• **No repudio:** este objetivo garantiza la participación de las partes en una comunicación. En toda comunicación, existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio: a) No repudio en origen: garantiza que la persona que envía el mensaje

no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío. b) No repudio en destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo. Este servicio es muy importante en las transacciones comerciales por Internet, ya que incrementa la confianza entre las partes en las comunicaciones.

Para conseguir los objetivos mostrados en la figura anterior se utilizan los siguientes mecanismos:

- Autenticación, que permite identificar al emisor de un mensaje, al creador de un documento o al equipo que se conecta a una red o a un servicio.
- Autorización, que controla el acceso de los usuarios a zonas restringidas, a distintos equipos y servicios después de haber superado el proceso de autenticación.
- Auditoría, que verifica el correcto funcionamiento de las políticas o medidas de seguridad tomadas.
- Encriptación, que ayuda a ocultar la información transmitida por la red o almacenada en los equipos, para que cualquier persona ajena no autorizada, sin el algoritmo y clave de descifrado, pueda acceder a los datos que se quieren proteger.
- Realización de copias de seguridad e imágenes de respaldo, para que en caso de fallos nos permita la recuperación de la información perdida o dañada.
- Antivirus, como su nombre indica, consiste en un programa que permite estar protegido contra las amenazas de los virus.

- Cortafuegos o firewall, programa que audita y evita los intentos de conexión no deseados en ambos sentidos, desde los equipos hacia la red y viceversa.
- Servidores proxys, consiste en ordenadores con software especial, que hacen de intermediario entre la red interna de una empresa y una red externa, como pueda ser Internet.

Estos servidores, entre otras acciones, auditan y autorizan los accesos de los usuarios a distintos tipos de servicios como el de FTP (transferencia de ficheros), o el Web (acceso a páginas de Internet).

- Utilización firma electrónica o certificado digital, son mecanismos que garantizan la identidad de una persona o entidad evitando el no repudio en las comunicaciones o en la firma de documentos.
- También se utilizan mucho hoy en día para establecer comunicaciones seguras entre el PC del usuario y los servidores de Internet como las páginas web de los bancos.
- Conjunto de leyes encaminadas a la protección de datos personales que obligan a las empresas a asegurar su confidencialidad.

Seguridad de la información

El objetivo del dominio es establecer la administración de la seguridad de la información, siendo la parte fundamental de los objetivos y las actividades de la empresa.

Se debe definir de manera formal el ámbito de gestión para efectuar diferentes tareas como pueden ser la aprobación de las políticas de seguridad, la coordinación de la implantación de la seguridad y la asignación de funciones y responsabilidades.

Realizar una actualización adecuada en materia de seguridad que debe contemplar la necesidad de disponer de fuentes de conocimiento y experimentar el asesoramiento, cooperación y colaboración en materia de seguridad de la información.

Las protecciones físicas de las organizaciones son cada vez más reducidas por las actividades de la empresa que requiere por parte del personal que acceden a la información desde el exterior en situación de movilidad temporal o permanente.

En estos casos se considera que la información pude ponerse en riesgo si el acceso se produce en el marco de una inadecuada administración en la seguridad, por lo que se establecen diferentes medidas adecuadas para la protección de la información.

Organización interna

La gerencia debe establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso la seguridad de la información, publicando y manteniendo una policía de seguridad en toda la organización según la norma ISO 27001.

Se tiene que establecer una estructura de gestión con el objetivo de iniciar y controlar la implementación de la seguridad de la información dentro de la empresa.

Es necesario que el órgano de dirección debe aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar y revisar la implementación de la seguridad en toda la empresa.
Si fuera necesario, en la empresa se tiene que establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información. Deben desarrollarse contactos especializados externos de seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como facilitar los enlaces adecuados para el tratamiento de las incidencias de seguridad.

Se tiene que fomentar un enfoque multidisciplinar de seguridad de la información, que establezca la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros y la gestión de riesgos.

Actividades de control del riesgo

- Asignación de responsabilidades para la seguridad de la información: se tiene que definir y asignar claramente todas las responsabilidades para la seguridad de la información.

- Segregación de tareas: se deben segregar tareas y las áreas de responsabilidad lo antes posible para evitar conflictos de interés con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada.
- Contacto con las autoridades: se deben mantener los contactos apropiados con las autoridades pertinentes.
- Contacto con grupos de interés especial: se debe mantener el contacto con diferentes grupos o foros de seguridad que estén especializados y asociados a profesionales.
- Seguridad de la información en la gestión de proyectos: se debe contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la empresa.

Métricas asociadas

Es el porcentaje de funciones organizativas para las cuales se ha implementado una estrategia general de mantener los riesgos de seguridad de la información por debajo de los umbrales explícitamente aceptados por la dirección.

Porcentaje de los empleados que han recibido y aceptado de manera forma las responsabilidades de seguridad de la información.

Dispositivos para movilidad y teletrabajo

La protección exigible debe estar en relación con los riesgos específicos que ocasionan otras formas de trabajo. En la utilización de la informática se deben considerar todos los riesgos de trabajar en entornos desprotegidos y aplicar la protección conveniente. En el caso del teletrabajo, la empresa tiene que aplicar las medidas de protección y garantizar que las disposiciones adecuadas que se encuentren disponibles para la modalidad de trabajo.

Se tiene que establecer una estructura de gestión con objeto de iniciar y controlar la implementación de la seguridad de la información dentro de la empresa.

Tiene que disponer de políticas claramente definidas para la protección, no sólo de los propios equipos informáticos portátiles, en mayor medida, de la información almacenada en ellos.

El valor de la información supera con mucho el del hardware. El nivel de protección de los equipos informáticos se utiliza dentro de los instalaciones de la empresa tiene su correspondencia en el nivel de protección de los equipos portátiles, etc.

Actividades de control del riesgo

- Política de utilización de dispositivos para la movilidad: se tiene que establecer una política formal y se deben adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados de utilizar los recursos de informática y las telecomunicaciones.
- Teletrabajo: se tiene que desarrollar e implementar una política o medidas de seguridad de apoyo para proteger a la información accedida, procesada o almacenada en ubicaciones destinadas al teletrabajo.

Software ISO 27001

El Software ISOTools Excellence para la norma ISO 27001, se encuentra capacitado para responder a numerosos controles para el tratamiento de la información gracias a las aplicaciones que contiene y que son totalmente configurables según los requerimientos de cada organización. Además, este software permite la automatización del Sistema de Gestión de Seguridad de la Información.

1.4 Posibles riesgos en la información.

Puede que hace una década este control del empresario fuera por la mera intención de controlar que el trabajador no perdiera el tiempo en la empresa dedicado a otros quehaceres que no fueran los estrictamente laborales. Hoy en día, en cambio, el abanico de posibles peligros que puede afectar a la seguridad informática de la empresa hace que esta se vea casi forzada a establecer una serie de instrucciones u órdenes a seguir, por parte del trabajador, en lo que se refiere al uso del ordenador, internet o teléfono móvil.

Normalmente cuando un empresario de una pequeña empresa piensa en la seguridad de la información de su organización, lo primero que le viene a la cabeza es que ha de comprar antivirus para evitar que se infecten de virus sus ordenadores y, por tanto, pueda peligrar la información de su empresa. No hay bastante sólo con equipar a los ordenadores de la organización con antivirus, hay otros muchos peligros que pueden afectar a la empresa y que este no es capaz de evitar.

Triada CID

Para poder garantizar la seguridad de la información de una empresa hace falta que se cumplan los principios de Confidencialidad, Integridad y Disponibilidad de la información que almacena y gestiona (también conocidos como "triada CID"):

- **Confidencialidad**: es la propiedad que impide que la información sea divulgada a personas, entidades o sistemas no autorizados, de manera que sólo puede acceder a ella aquellas personas que cuenten con la debida autorización y de forma controlada.

- **Integridad**: es la propiedad que busca proteger la exactitud de la información, evitar que sufra modificaciones no autorizadas.

- **Disponibilidad**: el tercer y último principio de la triada CID es el que garantiza que la información sea accesible y usable bajo demanda de un usuario autorizado, que esté disponible en todo momento, evitando interrupciones del servicio por cortes de electricidad, fallos de hardware, etc.

Riesgos de la seguridad de la información

Para que el sistema de información de una organización sea fiable hay que garantizar que se mantengan los tres principios de la triada CID. Por tanto, es crucial conocer las

vulnerabilidades y amenazas que se ciñen sobre la información. A continuación, podéis encontrar algunos de los riesgos básicos que pueden llegar a afectar a algunos de los principios de la triada:

- **Permiso de administrador en el ordenador**: si los trabajadores tienen permisos de administrador en los ordenadores de la empresa se corre el riesgo que puedan instalar aplicaciones ajenas a las actividades de la empresa. Instalaciones sin supervisión que aparte de que pueden introducir códigos maliciosos, también pueden llegar a colapsar nuestra red de comunicaciones interna. También puede suceder que el trabajador ignore las actualizaciones de seguridad que precisa el ordenador, y por tanto quede expuesto al ataque de nuevos virus, con el consecuente riesgo que alguno de ellos permita acceder a información confidencial, o hasta el control del ordenador de la empresa.

- **Correos maliciosos o no deseados**: estaríamos hablando tanto de los correos que pueden contener **phishing**, **pharming**, como los de **spam**, que al igual que en el punto anterior pueden introducir malware, saturar la red de la empresa o robar información.

- **No realizar copias de seguridad**: impensable en grandes empresas, pero muy habitual en las pequeñas. Es muy sencillo realizar copias de seguridad y permitirá□ la recuperación de la información. Es fundamental para evitar sufrir pérdidas de datos, y poderse recuperar rápidamente de un posible ciberataque.

- **Buen uso de las contraseñas**: Hay que ser cuidadoso y original con las contraseñas, no dejar nunca la contraseña que ha sido asignada por defecto. Se recomiendan contraseñas que usen letras (mayúsculas y minúsculas), números, y caracteres especiales (como "!", "#"). Tampoco hay que guardar las contraseñas en el ordenador en un fichero que se llame "Contraseñas" o "Passwords", os aseguro que eso es lo primero que buscan los hackers.

- **Uso de aplicaciones de almacenamiento on-line**: el uso de Dropbox o Google Drive por parte de los trabajadores, para almacenar, compartir e intercambiar archivos con información crítica de la empresa puede provocar perdidas de los tres principios de la triada CID, tanto de confidencialidad de los datos, como de integridad y disponibilidad.

Como evitar riesgos innecesarios

Es en este punto cuando el empresario ya debe tener en mente una lista de criterios que el trabajador de su empresa tendría que seguir para minimizar los riesgos que hagan peligrar la seguridad de la información. Veamos algunos de ellos:

- Podríamos empezar por **formar a los trabajadores** en la cultura de la ciberseguridad, que sean cuidadosos y precavidos a la hora de abrir un determinado correo electrónico sospechoso, o de instalar un programa de dudosa procedencia. También insistir en el buen uso de las contraseñas.

- **Limitar el uso** de los trabajadores en los **ordenadores** de la empresa para usos particulares. Puede ser que se den simplemente instrucciones de que los recursos de la empresa sean de uso meramente laboral, y por tanto esté prohibido el uso del ordenador para fines particulares (correos personales tipo Gmail, uso de redes sociales, etc), o bien que se limite tecnológicamente el acceso vía internet a páginas relacionadas con el negocio de la empresa.

- Si no se está□ haciendo ya, aunque su empresa tan solo trabaje con la información de su cartera de clientes, haga **copias de seguridad** de está.

- No permita el intercambio de información crítica de la empresa a través de almacenamiento on-line, pendrives sin encriptar, etc.

1.5 Técnicas de aseguramiento del sistema.

Consideraciones de software

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

Existe software que es conocido por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades, pero permitiendo una seguridad extra.

Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.

Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

1.6 Criptografía clásica: Un primer acercamiento.

Básicamente, a criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

A partir de la evolución de las computadoras, la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario, así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

- autentificar la identidad de usuarios
- autentificar y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias
- proteger la integridad de transferencias electrónicas de fondos

Criptografía y Seguridad informática

Un mensaje codificado por un método de criptografía debe ser privado, o sea, solamente aquel que envió y aquel que recibe debe tener acceso al contenido del mensaje. Además de eso, un mensaje debe poder ser suscrito, o sea, la persona que la recibió debe poder verificar si el remitente es realmente la persona que dice ser y tener la capacidad de identificar si un mensaje puede haber sido modificado.

Los métodos de criptografía actuales son seguros y eficientes y basan su uso en una o más llaves. La llave es una secuencia de caracteres, que puede contener letras, dígitos y símbolos (como una contraseña), y que es convertida en un número, utilizada por los métodos de criptografía para codificar y decodificar mensajes.

Criptografía: Claves Simétricas y Asimétricas

Las claves criptográficas pueden ser básicamente de dos tipos:

Simétricas: Es la utilización de determinados algoritmos para descifrar y encriptar (ocultar) documentos. Son grupos de algoritmos distintos que se relacionan unos con otros para mantener la conexión confidencial de la información.

Asimétricas: Es una fórmula matemática que utiliza dos llaves, una pública y la otra privada. La llave pública es aquella a la que cualquier persona puede tener acceso, mientras que la llave privada es aquella que sólo la persona que la recibe es capaz de descifrar.

Actualmente, los métodos criptográficos pueden ser subdivididos en dos grandes categorías, de acuerdo con el tipo de llave utilizado: criptografía de llave única y la criptografía de llave pública y privada.

Tipos de claves criptográficas

Criptografía de llave única: La criptografía de llave única utiliza la misma llave tanto para codificar como para decodificar mensajes. A pesar de que este método es bastante eficiente en relación al tiempo de procesamiento, o sea, el tiempo que gasta para codificar y decodificar mensajes, tiene como principal desventaja la necesidad de utilización de un medio seguro para que la llave pueda ser compartida entre personas o entidades que deseen intercambiar información criptografiada.

Criptografía de llaves pública y privada: La criptografía de llaves pública y privada utiliza dos llaves distintas, una para codificar y otra para decodificar mensajes. Con este método cada persona o entidad mantiene dos llaves: una pública, que puede ser divulgada libremente, y otra privada, que debe ser mantenida en secreto por su dueño. Los mensajes codificados con la llave pública solo pueden ser decodificados con la llave privada correspondiente.

Como ejemplo, José y María quieren comunicarse de manera sigilosa. Entonces, ellos tendrán que realizar los siguientes procedimientos:

1. José codifica un mensaje utilizando la llave pública de María, que está disponible para el uso de cualquier persona.
2. Después de criptografiarlo, José envía el mensaje a María, a través de Internet.
3. María recibe y decodifica el mensaje, utilizando su llave privada, que es sólo de su conocimiento.
4. Si María quisiera responder el mensaje, deberá realizar el mismo procedimiento, pero utilizando la llave pública de José.

A pesar de que este método tiene un desempeño muy inferior en relación al tiempo de procesamiento, comparado al método de criptografía de llave única, presenta como principal ventaja la libre distribución de llaves públicas, no necesitando de un medio seguro para que llaves sean combinadas con antelación.

¿Qué es firma digital?

La firma digital consiste en la creación de un código, a través de la utilización de una llave privada, de modo que la persona o entidad que recibe un mensaje conteniendo este código pueda verificar si el remitente es quien dice ser e identificar cualquier mensaje que pueda haber sido modificado.

De esta forma, es utilizado el método de criptografía de llaves pública y privada, pero en un proceso inverso al presentado en el ejemplo anterior.

Si José quisiera enviar un mensaje suscrito a María, él codificará un mensaje con su llave privada. En este proceso será generada una firma digital, que será añadida al mensaje enviado a María. Al recibir el mensaje, María utilizará la llave pública de José para decodificar el mensaje. En este proceso será generada una segunda firma digital, que será comparada con la primera. Si las firmas fueran idénticas, María tendrá certeza de que el remitente del mensaje fue José y que el mensaje no fue modificado.

Es importante resaltar que la seguridad del método se basa en el hecho de que la llave privada es conocida sólo por su dueño. También es importante resaltar que el hecho de firmar un mensaje no significara un mensaje sigiloso. Para el ejemplo anterior, si José quisiera firmar el mensaje y tener certeza de que sólo María tendrá acceso a su contenido, sería preciso codificarla con la llave pública de María, después de firmarla.

¿Qué tamaño de llave criptográfica debe ser utilizado?

Los métodos de criptografía actualmente utilizados, y que presentan buenos niveles de seguridad, son públicamente conocidos y son seguros por la robustez de sus algoritmos y por el tamaño de las llaves que utilizan.

Para que alguien descubra una llave necesita utilizar algún método de fuerza bruta, o sea, probar combinaciones de llaves hasta que la correcta sea descubierta. Por lo tanto, cuanto mayor sea la llave criptográfica, mayor será el número de combinaciones a probar, inviabilizando así el descubrimiento de una llave en un tiempo normal. Además de eso, las llaves pueden ser cambiadas regularmente, haciendo los métodos de criptografía aún más seguros.

Actualmente, para obtenerse un buen nivel de seguridad en la utilización de un método de criptografía de llave única, es aconsejable utilizar llaves de un mínimo de 128 bits. Y para el método de criptografía de llaves pública y privada es aconsejable utilizar llaves de 2048 bits, siendo el mínimo aceptable de 1024 bits.

Dependiendo para los fines para los cuales los métodos criptográficos serán utilizados, se debe considerar la utilización de llaves mayores: 256 o 512 bits para llave única y 4096 o 8192 bits para llaves pública y privada.

1.7 Criptografía en la antigüedad.

La criptografía es una técnica muy antigua, y durante mucho tiempo se ha relacionado con los círculos militares, religiosos y comerciales. Actualmente, la necesidad de proteger la información ha hecho que la utilidad de la criptografía se haya extendido a actividades comunes. Otras aplicaciones aparte de la comunicación segura de información es la autenticación de información digital (firma digital).

Las técnicas criptográficas se remontan a la antigüedad, y ya en el año 400 a.C. aparecen las primeras prácticas. A continuación, se enumeran algunas de ellas, así como su evolución a lo largo de la historia.

La escitala espartana

El origen de esta técnica se remonta al año 400 a. C. Era utilizada en la antigua Grecia por los espartanos para enviar mensajes ocultos entre las tropas militares. La escitala era un listón de madera en el que se enrollaba una tira de cuero. Sobre esta tira se escribía el mensaje que se quería ocultar en columnas paralelas al eje del palo. Al desenrollar la tira se muestra un texto incoherente (aparentemente) con el texto inicial, pero que puede leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero.

Así, si el mensajero era interceptado, el mensaje que se encontraba era una serie de caracteres incomprensibles. Este procedimiento requiere que el emisor y el receptor del mensaje dispongan de un listón del mismo diámetro para poder descifrar el comunicado.

Tablero de Polibio

El historiador Polibio (nacido en el año 200 a. C.) ideó un código que se basaba en un tablero conocido como "Tablero de Polibio" (Ilustración 3) para transmitir mensajes a larga distancia. En este tablero de dimensiones 5x5 cada letra es equivalente a una pareja de ellas, correspondiendo a la fila y a la columna que forman sus coordenadas.

Así si se quiere cifrar un mensaje se sustituye cada una de las letras que lo forman por el par de letras que le corresponden en el tablero.

INTECO ► BDCCDDAEACCD

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I,J	K
C	L	M	N,Ñ	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Cifrado Cesar

Remontándose al 100 a.C. el "Cifrado Cesar" nació con la necesidad de ocultar información escrita en latín por parte del ejército de Julio César. La técnica utilizada para cifrar un mensaje en el "Cifrado Cesar" era sustituir cada una de las letras del mensaje por aquella que ocupaba tres posiciones más en el alfabeto.

Original	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifrado	d	e	f	g	h	i	j	k	l	m	n	o	p
Original	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifrado	q	r	s	t	u	v	w	x	y	z	a	b	c

1.8 Cifradores del siglo XIX.

En el siglo XIX comienzan a desarrollarse diversos sistemas de cifra con las características poli alfabéticas propuestas por Alberti, entre los que destacan el de discos concéntricos de Wheatstone en 1860 y el de cilindros de Bazeries en 1891.

El cifrador de Wheatstone

El criptógrafo de Wheatstone mostrado en la Figura 1.5. -según un invento de Decius Wadsworth desarrollado en 1817- sigue, básicamente, el mismo algoritmo de cifra que el de Alberti. Ahora bien, en este caso se utiliza el alfabeto inglés de 26caracteres más el espacio en blanco para el texto en claro, representado de forma ordenada en el disco exterior, en tanto que el disco interior contiene solamente los 26caracteres del lenguaje distribuidos aleatoriamente. Las agujas están engranadas de forma que cuando la externa gira 27 posiciones, la interna lo hace 26.

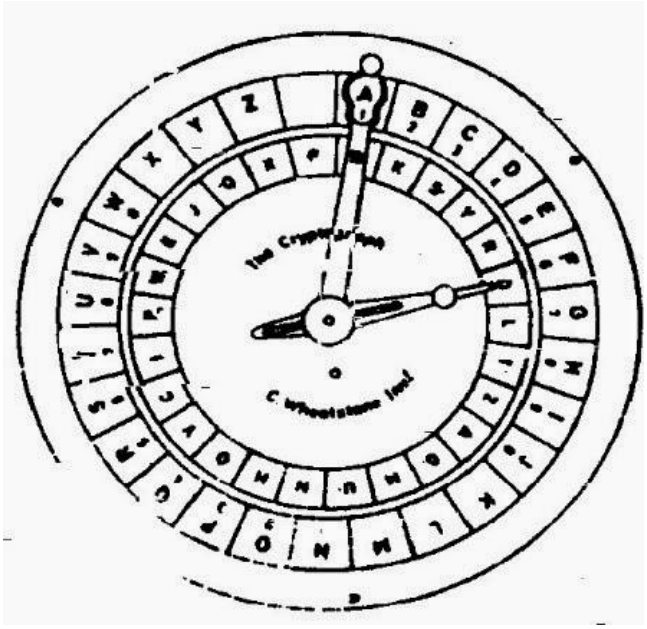


Figura 1.5. Máquina de cifrar de Wheatstone.

El método de cifra consiste en hacer girar la aguja externa en el sentido de las manecillas del reloj hasta hacer coincidir cada letra del texto en claro con la letra del disco externo y apuntar el carácter correspondiente que aparece en el círculo interior, incluso para el espacio en blanco. Observe que, por la relación de giro de las agujas, éstas se van separando una posición o letra por cada vuelta, de forma que el alfabeto de cifrado será diferente cuando se cumpla cualquiera de estas tres condiciones:

a) Que se termine una palabra del texto en claro y por tanto demos un giro completo de la aguja mayor al buscar el espacio en blanco

b) Que aparezcan letras repetidas y tengamos que dar toda una vuelta completa al buscar la segunda. No obstante, según los autores, en este caso es posible también omitir cifrar la letra repetida o bien cifrar ambas como una única letra poco usual, por ejemplo, la letra Q.

El cifrador de Bazeries

El cifrador de Étienne Bazeries, criptólogo francés nacido a finales del siglo XIX, está basado en el cifrador de ruedas de Jefferson, inventado unos 100 años antes por Thomas Jefferson reconocido como el padre de la criptografía americana. El criptógrafo mostrado en la Figura 1.6 consta de 20 discos, cada uno de ellos con 25 letras en su circunferencia, de forma que la clave se establece sobre la generatriz del cilindro, determinándose 25 alfabetos diferentes.

Su funcionamiento es el siguiente: para cifrar el mensaje, primero se divide éste en bloques de 20 letras, procediendo luego a su colocación en forma longitudinal en la línea del visor. El criptograma que se envía puede ser cualquiera de las 25 líneas, también llamadas generatrices del cilindro. Por ejemplo, si se elige la generatriz de distancia +2 en la Figura 1.6, el mensaje M = JE SUIS INDECHIFFRABLE del visor se cifraría como C = LOVS PQUUTPUKEJHHCFDA

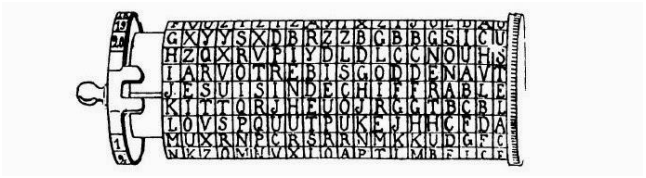


Figura 1.6. Máquina de cifrar de Bazeries

La operación de descifrado consiste en poner los caracteres del criptograma enel visor y buscar en alguna de las líneas el mensaje en claro o seguir el proceso inverso al comentado

anteriormente. Como los bloques de criptograma tienen longitud de veinte caracteres, es prácticamente imposible que exista más de una solución consentido.

1.9 Criptosistemas clásicos.

La palabra código alude a un tipo muy particular de comunicación secreta, que ha ido cayendo en desuso a lo largo de los siglos. En un código, una palabra o una frase es reemplazada por una palabra, un número o un símbolo. Por ejemplo, los agentes secretos tienen nombres codificados, palabras que se utilizan en vez de sus verdaderos nombres para enmascarar su identidad. La alternativa al código es la cifra, una técnica que funciona a un nivel más básico, reemplazando letras en vez de palabras enteras. Por ejemplo, cada letra de una frase podría reemplazarse por la siguiente letra del alfabeto.

Tipos de Cifrados Clásicos

Se puede hacer una gran división de los cifrados según el tipo de operación que se realiza en el cifrado. Dada la característica finita del alfabeto y la hipótesis de no variación de la longitud del texto, existen dos opciones para el cifrado. La primera, llamada sustitución, consiste en sustituir las unidades del texto original por otras; la segunda llamada transposición, consiste en crear el texto cifrado simplemente desordenando las unidades que forman el texto original. Los algoritmos de sustitución y los códigos, preservan el orden de los símbolos en claro, pero los disfrazan. A diferencia de éstos, los algoritmos de transposición, reordenan las letras pero no las disfrazan.

Ejemplo de transposición:

TU SECRETO ES TU PRISIONERO; SI LO SUELTAS, TÚ ERES SU PRISIONERO

T S C E O S U R S O E O I O U L A T E E S P I I N R
U E R T E T P I I N R S L S E T S U R S U R S O E O

TSCEOSURSOEOIOULATEESPIINRUERTETPIINRSLSETSURSURSOEO

Ejemplo de sustitución:

ENCONTRÉMONOS A MEDIANOCHE

A D H I K M O R S U W Y Z

V X B G J C Q L N E F P T

USMQZLUCQSQN V CUXGVSQMBU

Este es un ejemplo ilustrativo claro de una función matemática; a cada letra del alfabeto llano (elemento del dominio) le hace corresponder una letra del alfabeto cifrado (elemento del rango o conjunto imagen de la función). Por otra parte, para el proceso de descifrado es necesario contar con que la función sea biyectiva para poder ser invertible. Los sistemas criptográficos donde la clave de descifrado se puede deducir de la clave de cifrado se llaman simétricos o de clave secreta.

Los criptógrafos a menudo piensan en términos de alfabeto llano o claro, el alfabeto que se usa para el mensaje original, y alfabeto cifrado, las letras que sustituyen a las del alfabeto llano.

Cada una de las cifras puede ser considerada en términos de un método de codificación general, conocido como el algoritmo, y una clave, que especifica los detalles exactos de una codificación particular. En los casos siguientes, el algoritmo conlleva sustituir cada letra del alfabeto llano por una letra del alfabeto cifrado y el alfabeto cifrado puede consistir de cualquier combinación del alfabeto llano.

El algoritmo de transposición más común es el de tipo columnar; la clave del cifrado debe ser una palabra que no tenga ninguna letra repetida, en el ejemplo que se presenta a continuación la clave es la palabra MEGABUCK. El propósito de la clave es el de numerar las diferentes columnas que se formarán, de forma que la columna 1 es aquella que queda bajo la letra de la clave más próxima al principio del alfabeto y así sucesivamente. El texto en claro se escribe debajo de la clave en renglones horizontales; el texto cifrado se lee por columnas, comenzando por la columna cuya letra clave tiene el menor valor.

1.10 Máquinas de cifrar (siglo XX).

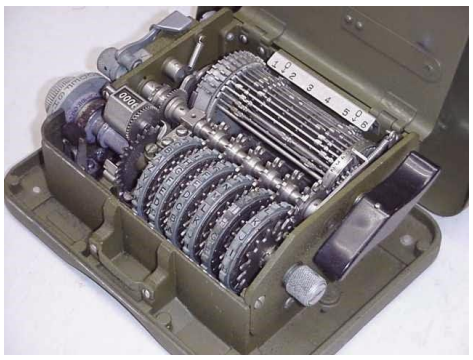
Ya entrado el siglo XX, aproximadamente unos 20 años antes de que estalle la Segunda Guerra Mundial, se desarrollan diversas máquinas de cifrar con rotores o ruedas que permiten un cifrado poli alfabético, dando lugar a un importante número de claves secretas .Este desarrollo a nivel industrial de los cripto sistemas resulta lógico pues en aquellos años previos a dicha confrontación mundial, estaba todavía muy fresco en la memoria de todos, y en especial de gobernantes y militares, los efectos de la Primera Guerra Mundial, por lo que las medidas de seguridad ante el miedo al espionaje adquirían una importancia vital. Recuerde el famoso telegrama de Zimmermann comentado al comienzo del capítulo.

La máquina Enigma

Inventada por el ingeniero alemán Arthur Scherbius en el año 1923, la máquina Enigma consiste en un banco de rotores montados sobre un eje, en cuyos perímetros había 26 contactos eléctricos, uno por cada letra del alfabeto inglés. En realidad, el precursor de este tipo de máquinas con rotores fue Edward Hugh Hebern que algunos años antes inventa y comercializa los denominados cifra dores de códigos eléctricos

Esta máquina debe su fama a la amplia utilización durante la Segunda Guerra Mundial, en especial por parte del ejército alemán. El imperio japonés también cifra sus mensajes con una máquina similar denominada Purple Estos códigos, por muy difíciles que puedan parecer, fueron rotos por los criptoanalistas de la época.

La máquina Hagelin



La máquina Hagelin fue inventada por el criptólogo sueco Boris Hagelin, quien adquirió en 1927 la fábrica de máquinas de cifrar de Arvid G. Damm, otro inventor sueco que no tuvo la suerte de sacar un producto competitivo en el mercado. Entre losamos veinte y los treinta, Hagelin diseña diversas máquinas (B-21, B-211, C-36, C-48, etc.) en las que a través de ruedas con piñones realiza una cifra similar a la utilizada por el sistema de Beaufort que veremos más adelante. La particularidad de estas máquinas que a la postre hizo millonario a Hagelin, probablemente ante la desesperación de Damm, estaba en una periodicidad muy alta puesto que el número de dientes de las diferentes ruedas eran primos entre sí. Paraseis ruedas estos valores eran 26, 25, 23, 21, 19 y 17, de forma que el período era igual a su producto, un valor que supera los 100 millones. La ecuación matemática que representa al cifrado de Hagelin es:

Eki(Mj) = (ki- M j) mod 2

1.11 Estadística del lenguaje.

En algunos criptosistemas (básicamente los de tipo clásico orientados al cifrado de caracteres) podremos aplicar esta característica para criptoanalizar textos cifrados. De hecho, lo primero que se plantea todo criptoanalista es suponer que el cifrado es de tipo básico y, por lo tanto, puede intentarse el ataque a partir de las estadísticas del lenguaje.

Aunque los sistemas clásicos estén en desuso, no por ello deben ser pasados por alto por el criptoanalista. En realidad sería bastante poco agradable perder horas de esfuerzo en la intención de romper una cifra, suponiendo de antemano que el criptosistema en cuestión empleado es de los denominados *modernos*, para luego caer en la cuenta que aquel complicado *enigma* se trataba simplemente de un cifrado elemental, que puede romperse fácilmente con herramientas básicas. No quedaríamos muy bien ante nuestros superiores.

Por lo tanto, la primera acción que realizará todo criptoanalista será la de *contabilizar* los caracteres que aparecen en el criptograma para obtener información sobre el tipo de cifra, monoalfabético o polialfabético, e intentar aplicar las técnicas que describiremos más adelante

para romper dicha cifra. Si esto no entrega los resultados esperados, buscará otros caminos, yendo como es lógico siempre desde la dificultad menor a la mayor.

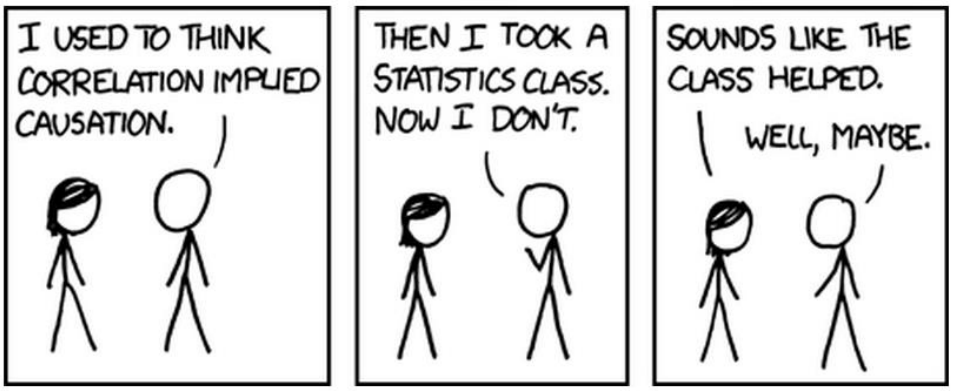
1.12 Ejemplos de la estadística del lenguaje.

Conocer los datos y la tipología de las variables: bien de tipo cuantitativo o cualitativo. Dado que en función del tipo de las variables del conjunto de datos, se aplicarán una serie de coeficientes u otros.

Conocer qué método es el más adecuado para su aplicación: de nada vale conocer el script que ejecuta una correlación, si no se puede basar matemáticamente cómo desarrollar los cálculos.

Conocer, comprender e interpretar los resultados que los indicadores ofrecen: parte fundamental del análisis, basada en la diferencia existente entre los conceptos de causalidad y correlación que subyace en el análisis, y que suelen confundirse. El mero cálculo de un coeficiente, no determinado por una causalidad, no tiene por qué ser válido. Es decir «la existencia de correlación, no implica causalidad», como se refleja en esta viñeta:

1. Lo primero, un **«conjunto de datos»**.
2. En dicho conjunto el requisito es tener mínimo dos «variables» (éste es el nombre técnico), según unas técnicas u otras se han denominado «dominios», «campos» de una base de datos y similares.
3. Conocer las bases matemáticas y estadísticas del análisis de datos, en concreto:



¿Qué no es una correlación?, ejemplos:

1. Un análisis de frecuencias:

Hacer una cuenta, lo que técnicamente se denominan «frecuencias ordinarias o acumuladas» y «absolutas o relativas». Que en su modo multidimensional se completan con las «frecuencias marginales y condicionales». Este es el caso más habitual, reflejado en la típica instrucción SQL o Python cuyo resultado es un agregado COUNT o SUM.

Un ejemplo práctico de lo que no es una correlación en seguridad: es contar el número de direcciones IP bloqueadas por un determinado filtro dentro de una base de datos o log de sistemas, cuando el número de conexiones hacia una «network destination address» concreta sobrepasa un umbral máximo establecido desde una determinada localización («source address» o geográfica). Esto no es una correlación, es un mero análisis de frecuencias, en este caso absolutas ordinarias y condicionales -por lo multidimensional-, estableciendo un límite de aparición. El límite no es más que un cuantil -de ellos los más usados son los percentiles... los mismos que usa el pediatra -, calculado sobre la frecuencia condicional.

2. **Realizar un gráfico**, como el típico «histograma de frecuencias» o gráfico de tarta con unos porcentajes o valores absolutos. Tampoco lo son lo que en la actualidad se denominan «Visual Representations». En general estas herramientas facilitan la representación de un resultado, mejorando su comprensión, pero no tienen por qué hacer referencia a un análisis

de correlación. De hecho el primer gráfico que se suele realizar para el análisis de correlación, dependiendo del número de variables, p.e. en el caso de dos variables, es un «diagrama de dispersión». Aunque realizar este diagrama no es una correlación, es el primer paso para conocer la posible existencia de relación o independencia entre las variables.

Suele ser común que el analista prefiera una tabla de datos de resultados sencilla, y en ella encuentra todo lo necesario para tomar decisiones, dado que ésta será la que alimente el gráfico, que habitualmente será el presentado a terceros.

3. La estadística nos proporciona **otras herramientas** más adecuadas. Un ejemplo de ello es contrastar la frecuencia temporal de envío de spam desde una determinada IP en un período, y analizar si su distribución -estadística, no geográfica- en función de un determinado parámetro, se ha modificado, y determinar si el establecimiento de un filtro ha funcionado o es necesario modificarlo, cambiarlo o eliminarlo. Esto no se realiza mediante una correlación, existe una técnica más apropiada denominada «Contraste de hipótesis», de la que hablaremos otro día, y de la que veremos casos reales explotando datos de un SIEM. De esta técnica surgen conceptos también ampliamente utilizados como «Falso positivo» o «Falso negativo» ... cualquier administrador de un servidor de correo electrónico da fe de lo costoso que es aplicar dicha técnica para poder parametrizar las reglas que definen unos y otros, y que dichos filtros funcionen correctamente ... que nunca perfectamente.

UNIDAD II CERTIFICADOS Y FIRMAS DIGITALES

2.1 Distribución de claves.

Lo ideal sería que pudiéramos distribuir nuestra clave entregándosela en persona a nuestros corresponsales. Sin embargo, en la práctica las claves se distribuyen a menudo por correo electrónico o algún otro medio de comunicación electrónica. La distribución por correo electrónico es una buena práctica sólo cuando tengamos unos pocos corresponsales, e incluso si tuviéramos muchos corresponsales, podríamos usar un medio alternativo como puede ser publicar nuestra clave pública en nuestra página en internet. Pero esto es inútil si las personas que necesitan nuestra clave pública no saben dónde encontrar nuestra página.

Para solventar este problema existen los servidores de claves públicas que recolectan y distribuyen las claves públicas. Cuando un servidor recibe una clave pública, bien la añade a la base de datos o bien la fusiona con una copia de la clave. Cuando alguien requiere al servidor una clave pública, éste la busca en la base de datos y, si la encuentra, la envía a quien se la haya solicitado.

Los servidores de claves también son útiles cuando hay muchas personas que firman las claves de otras con frecuencia. Sin un servidor de claves, cuando Arancha firmara la clave de Javier, debería enviar a éste una copia de la clave firmada por ella de manera que Javier pudiera añadir la clave firmada a su anillo de claves, así como distribuirla a todos sus corresponsales. Mediante este proceso Javier y Arancha sirven a la totalidad de la comunidad construyendo lazos en forma de anillos de confianza o lo que es lo mismo, mejorando la seguridad de PGP. De todos modos, esto es una molestia si se firman las claves con frecuencia.

El uso de un servidor de claves facilita este proceso. Después de firmar la clave de Javier, Arancha puede enviar la copia firmada por ella al servidor de claves. El servidor de claves añade la firma de Arancha a la copia que ya existente de la clave pública de Javier. Las personas que estén interesadas en actualizar su copia de la clave de Javier consultan al servidor por propia iniciativa para obtener la clave actualizada. Javier no necesita distribuir la clave y puede obtener las firmas en su clave requiriéndolas al servidor.

Se puede enviar una o más claves usando la opción de la línea de órdenes --send-keys. Esta opción toma uno o más especificadores de clave, y envía las claves especificadas al servidor de claves. El servidor al que se envían las claves es especificado con la opción de la línea de orden --keyserver. Paralelamente, la opción --recv-keys se usa para obtener claves desde un servidor de claves, pero la opción --recv-keys requiere el uso de un identificador de clave para poder especificar la clave deseada. En el siguiente ejemplo Javier actualiza su clave pública con nuevas firmas desde el servidor de claves *certserver.pgp.com* y acto seguido envía su copia de la clave pública de Arancha al mismo servidor de claves para que se actualice con las claves que él mismo pueda haber añadido.

Criptografía y seguridad informática son dos elementos que crean una llave perfecta que abre tus entornos digitales. Si bien cada elemento surgió y evolucionó de manera autónoma para ganar por mérito propio su correspondiente sitial de honor; criptografía y seguridad informática se combinan para garantizar el acceso exclusivo únicamente a quienes autorices.

En sí, la una retroalimenta y perfecciona a la otra para complementar y potenciar la seguridad de tus entornos digitales; y brindar a todos la oportunidad de proteger la data de todo tipo de amenazas virtuales. En pocas palabras, criptografía y seguridad informática son parte integral de la conservación de la integridad de la data manejada y compartida.

Ahora bien, ¿basta la criptografía para garantizar la protección de los datos y asegurar la privacidad de las interacciones en los entornos digitales? ¿Qué secretos se esconden detrás

de nuestras claves y contraseñas? ¿Cómo fue que se conocieron e hicieron inseparables criptografía y seguridad informática? Veamos su evolución.

Criptografía y seguridad informática: Algunos datos interesantes

Aunque la criptografía acumula miles de años de historia; comenzó con el sencillo deseo de ocultar o restringir a unos pocos los mensajes importantes.

El hombre es esclavo de sus palabras y dueño de su silencio.
La base de la criptografía echó raíces en esta premisa y gracias a ella; infinidad de técnicas vieron luz para garantizar y procurar la integridad de la información que revelamos, y segregarla de la que queremos reservarnos.

Vale el inciso para recordar el célebre caso de la máquina Enigma; la forma como los Aliados lograron romper su código; y sus repercusiones sobre el fin de la Segunda Guerra Mundial. Ahora bien, si esto fue posible en la primera mitad del siglo pasado, ¿podemos siquiera imaginar la evolución y repercusión de un evento similar en la informática actual?

En sí, la criptografía es un arte de técnica compleja empleado para la protección u ocultamiento de información. En la época moderna y específicamente durante el siglo pasado; se empleaba exclusivamente para proteger datos y documentos de origen con información militar o asuntos políticos.

Sin embargo, con la llegada y masificación del Internet, la criptografía y seguridad informática evolucionaron conjuntamente y de manera natural hacia la empresa privada. Y de ahí, a los individuos.

Por esta razón, criptografía y seguridad informática en nuestra época se traducen en diversos tipos y presentaciones que conviene conocer bien.

Criptografía y seguridad informática en la actualidad: Tipos

Criptografía simétrica

Este tipo de criptografía maneja una clave única entre Emisor y Receptor. Es decir; que ambos extremos de la comunicación conocen de antemano la clave o contraseña porque se ha compartido previamente mediante un canal sin filtros ni protocolos como, por ejemplo, una llamada telefónica; un correo; un trozo de papel; etc.

Es en este punto precisamente donde se encuentra su mayor vulnerabilidad: Como el canal transmite la clave de la misma forma como la recibe; es muy fácil interceptar el canal para interceptar la clave y dar con todos sus componentes sin necesidad de romper el código:

La principal ventaja que ofrece la criptografía simétrica, es la rapidez con la que establece y entrega los mensajes. Sin embargo, su vulnerabilidad extrema la hace poco fiable y para nada recomendable si nuestro objetivo es proteger y hacer privada la información que compartimos.

Criptografía asimétrica

Por otra parte, la criptografía asimétrica emplea dos claves para hacer más robusto e impenetrable el mensaje como tal. Una de estas claves es pública y por ello no ofrece

barreras de protección porque su único objeto es establecer un canal -o recipiente- que sirve para remitir -o entregar- el mensaje.

La otra clave es privada; y es la responsable de cifrar el mensaje para mantenerlo privado. Este par de claves son generadas al mismo momento, y es el propietario quien decide a quién va a revelarlas:

La robustez de las claves asimétricas se basa principalmente en el tamaño del código de encriptación, la cual puede alcanzar tranquilamente los 2048 bits. Y con cada bit, se hace mayor la dificultad para intentar romper el código.

Ahora bien, la principal desventaja que ofrece el cifrado asimétrico es la lentitud que ofrece para verificar los datos; y desde luego, la forma como ralentiza el proceso incluso más si queremos hacer una encriptación de llave doble para hacer bidireccional el flujo e intercambio de información.

Criptografía híbrida

Por último, encontramos la criptografía híbrida, la cual rescata lo mejor de las dos anteriores para minimizar sus desventajas a niveles aceptables. El protocolo de uso para emplear un sistema criptográfico híbrido va así:

Criptografía y seguridad informática: El Ciclo de Vida de tus Claves y Contraseñas

Partamos del principio que una imagen vale más que muchas palabras para comprender el ciclo de vida de tus claves y contraseñas:

Generación de contraseñas

Da inicio al ciclo de vida de tus claves o contraseña. Lo ideal es establecer protocolos para generar claves y contraseñas seguras y para lograrlo es necesario:

- Emplear una mezcla de símbolos y caracteres sin coherencia lógica
- Ayudarse de mnemotecnias e imágenes mentales conocidas únicamente por quien establece la contraseña segura
- Evitar utilizar información personal tal como fecha de nacimiento propia y similares

Distribución

Comprende la forma como llega y se autentica la clave o contraseña en el banco o base de datos (DB, por sus siglas en inglés) que nos autoriza el acceso a la plataforma para la que creamos tal clave o contraseña. Esta puede ser de:

Distribución manual

La clave se envía mediante canales distintos a la línea de comunicación mediante la cual se mandan mensajes cifrados, por ejemplo: Carta certificada + vía telefónica + fax; Inyección de claves.

Distribución central

Las partes interesadas en el intercambio seguro de datos establecen una conexión cifrada por un tercero. Este elemento se encarga de entregar las claves cifradas seguras de comunicación a ambos extremos.

Distribución certificada por:

- *Transferencia de clave*
  - El Emisor genera una clave asimétrica con la llave pública del Receptor (criptografía asimétrica)
- *Intercambio o acuerdo de clave*
  - El Emisor y el Receptor conocen de antemano la clave (criptografía simétrica)

Son los mecanismos que activamos cuando olvidamos la clave o contraseña que generamos. En principio se manejan dos opciones para activar este protocolo:

- Recuperación de Clave o Contraseña
- Restablecimiento de Clave o Contraseña

Ambas opciones están supeditadas a las políticas y condiciones de gestión de claves y contraseñas establecidas por el propietario de la aplicación o servicio. Las mismas se encargan de verificar la autenticidad de la data proporcionada al momento de establecer la clave o contraseña.

Políticas de Uso

Maneja todas las consideraciones para generar, emplear, recuperar, reemplazar y disponer de las claves y contraseñas. Determina los límites de uso, y esto incluye tipo de caracteres; longitud de la contraseña; políticas de almacenamiento en la DB; políticas de recuperación de clave o contraseña olvidada; y caducidad u obsolescencia ("vencimiento") de las claves.

Almacenamiento en DB

Con el propósito de autenticar usuarios y parear sus datos con sus claves o contraseñas, el propietario del sistema debe almacenar o alojar toda esta información en una Base de Datos; y restringir el acceso a ella. Tal restricción se basa en los siguientes controles de seguridad:

- Encriptación de los archivos que contienen las claves y contraseñas.
- Activación del control de acceso al sistema operativo (OS) de la DB.
- Almacenamiento de hashes criptográficos para claves y contraseñas unidireccionales en lugar de guardar las claves y contraseñas como tal.
- Verificación de los elementos del host (capacidades de seguridad del host; las amenazas en su contra del host; requerimientos de autenticación).

Obsolescencia

Es la etapa final del ciclo de vida de claves y contraseñas. Comprende las políticas de disposición final de las claves o contraseñas cuando ya caen en desuso, ya que una de las principales premisas para evitar su intercepción; robo o revelado es que las claves y contraseñas no deben usarse por tiempo indefinido.

En todo caso, existen dos tipos de disposición de las claves y contraseñas una vez se hacen obsoletas:

Disposición por Expiración

En las Políticas de Uso se establece el tiempo máximo de vida útil de claves y contraseñas. Esto da una ventana de tiempo predeterminada para que las mismas caigan en desuso, y sea necesario crear una nueva clave o contraseña para el acceso seguro.

Disposición por Revocación

Ocurre cuando el Administrador de Sistema detecta compromiso en las claves y contraseñas, y para asegurar la integridad de la data, procede a su descontinuación inmediata. También se revoca una clave o contraseña por fuerza mayor (despido, deceso o redefinición de privilegios de usuario; actualizaciones; restructuraciones, etc.)

Cuando las claves y contraseñas se hacen obsoletas, se hace redundante su almacenamiento. De la misma forma como las Políticas de Uso determinan los parámetros de generación de claves y contraseñas; se encarga de determinar los parámetros de su destrucción y disposición final. Generalmente, tales controles son los siguientes:

- Crypto-Shredding (Destrucción criptográfica)
- Borrado seguro
- Destrucción física por desmagnetización o trituración de medios magnéticos.
- Descubrimiento de contenido

El ciclo de vida de claves y contraseñas y su relación con tu seguridad informática

La criptografía y el ciclo de vida de claves y contraseñas son parte de la seguridad informática de tu empresa. Esto, porque la seguridad informática vela por la protección de la data sensible ante amenazas y vulnerabilidades de los sistemas; y su razón fundamental es blindarlos contra cualquier intromisión a lo largo del ciclo:

La seguridad informática incluye la encriptación de los datos sensibles, la tokenización de las comunicaciones y buenas prácticas de la gestión del ciclo de vida de las claves y contraseñas que proteger tus plataformas, activos, bienes y servicios.

Como comprendemos lo difícil que puede resultar la tramitación y obtención de claves y contraseñas seguras para garantizar la protección de tus datos sensibles y comunicaciones; ponemos a tu alcance herramientas de gestión que lo simplifican para ti.

Recuerda: Si tus claves de acceso caen en manos inadecuadas, pones en riesgo todos tus datos sensibles (información personal; recursos financieros; secretos profesionales). Tómate el tiempo para generar contraseñas seguras y robustecer tu seguridad informática, y si tiempo es lo que menos tienes, ¡estás en el sitio adecuado!

Como expertos en seguridad integral, la criptografía y seguridad informática son dos temas que nos preciamos de contar entre nuestros servicios. Te ayudamos a crear tus llaves perfectas para abrir tus entornos digitales únicamente a quien decidas darle ese privilegio.

2.2 Certificación.

Un recurso esencial para la gestión de las necesidades de seguridad de la información

Los sistemas de informaciones sin protección son vulnerables a fraudes, sabotajes y virus a través de computadoras.

Un sistema de gestión de seguridad de la información (SGSI) compatible con la ISO/IEC 27001:2005 puede ayudarlo a demonstrar a sus coparticipes de negocios y a clientes que usted lleva la seguridad de la información muy a serio.

La certificación ISO/IEC 27001 concedida por LRQA es una herramienta poderosa para garantizar que sus negocios tengan controles adecuados de seguridad de la información en vigor.

La ISO/IEC 27001, originalmente introducida por el DTI como BS 7799 en 1995, es una norma internacional que busca garantizar que controles adecuados estén en vigor para abordar la confidencialidad, la integridad y la disponibilidad de informaciones y proteger las informaciones de 'partes interesadas'.

Esto incluye sus clientes, colaboradores, coparticipes de negocios y las necesidades de la sociedad en general.

Su suplemento, la ISO/IEC 17799, establece las directrices y los principios generales para la iniciación, la implementación, el mantenimiento y la mejoría de la gestión de seguridad de la información en una organización identificada por el proceso de auditoría de riesgo de la ISO/IEC 27001.

La ISO/IEC 27001 se basa en el modelo PDCA (Planear, Ejecutar, Verificar y Actuar) común a la ISO 9001 y a la ISO 14001, como también utiliza la evaluación de riesgo y el análisis de impacto para identificar y administrar los riesgos en lo referente a confidencialidad, a la integridad y a la disponibilidad de informaciones.

Más de la mitad de las 200 mayores empresas del mundo eligen LRQA para la realización de servicios de certificación.

La certificación ISO/IEC 27001 concedida por LRQA puede ayudar a reducir el riesgo de amenazas a la seguridad y de pontos débiles.

La certificación ISO/IEC 27001 es una demostración poderosa del compromiso de una organización en la gestión de seguridad de la información y en la promoción de mejorías continuas. Ella brinda una ventaja competitiva para su organización por lo siguiente:

Ayuda a su organización a desarrollar un plan de continuidad de los negocios, reduciendo el impacto de las violaciones de seguridad y garantizando que los controles estén en vigor para reducir el riesgo de amenazas a la seguridad y de puntos débiles del sistema.

Posibilita que usted demuestre que sus sistemas y procesos de TI son seguros y haga una declaración pública de la capacidad sin revelar sus procesos de seguridad o abrir sus sistemas para auditorías de segunda parte.

Demuestra que su organización atiende a los requisitos de la Ley de Protección de Datos de 1998.

Permite que Usted trabaje con muchas organizaciones en las cuales esta certificación es una obligación contractual, una expectativa o requisito previo para hacer negocios.

La certificación ISO/IEC 27001 concedida por LRQA se concentra en áreas y cuestiones importantes para su gestión de seguridad de la información y su negocio.

En LRQA, somos apasionados por lo que hacemos y nuestra reputación en certificación de sistemas de gestión es reconocida mundialmente.

Nuestros auditores son especialistas calificados en el sector, que comprenden las necesidades de su negocio, lo que permite una auditoría consistente y eficaz de su sistema.

LRQA es líder en el mercado de servicios de auditoría, certificación y capacitación y más de la mitad de las 200 mayores empresas del mundo escogen a LRQA para la realización de certificación.

LRQA está entre los primeros organismos de certificación a emitir un certificado ISO/IEC 27001 en América del Norte.

Nuestro abordaje de Business Assurance garantiza que nuestras auditorías enfaticen las áreas y las cuestiones que son importantes para su empresa.

Además de la certificación, LRQA ofrece una amplia variedad de servicios para dar soporte al crecimiento y desarrollo de su negocio en el futuro, incluyendo auditoría de sistemas de gestión integrados.

2.3 Componentes de una PKI.

Una PKI (Public Key Infrastructure, infraestructura de clave pública) es un conjunto de elementos de infraestructura necesarios para la gestión de forma segura de todos los componentes de una o varias Autoridades de Certificación. Por tanto, una PKI incluye los elementos de red, servidores, aplicaciones, etc. Ahora vamos a identificar algunos de los componentes lógicos básicos de una infraestructura de clave pública.

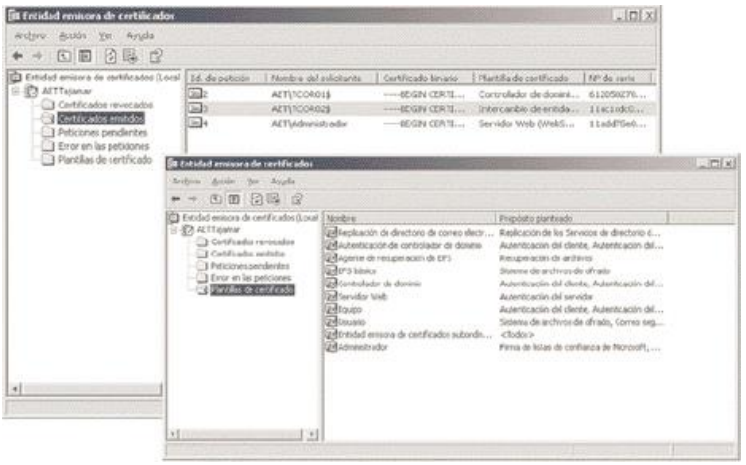
- Autoridad de certificación CA. Una autoridad de certificación es el componente responsable de establecer las identidades y de crear los certificados que forman una asociación entre la identidad y una pareja de claves pública y privada.

- Autoridad de registro RA. Una autoridad de registro es la responsable del registro y la autenticación inicial de los usuarios a quienes se les expedirá un certificado posteriormente si cumplen todos los requisitos.

- Servidor de certificados. Es el componente encargado de expedir los certificados aprobados por la autoridad de registro. La clave pública generada para el usuario se combina con otros datos de identificación y todo ello se firma digital mente con la clave privada de la autoridad de certificación.

- Repositorio de certificados. Es el componente encargado de hacer disponibles las claves públicas de las identidades registradas antes de que puedan utilizar sus certificados. Suelen ser repositorios X.500 o LDAP. Cuando el usuario necesita validar un certificado debe consultar el repositorio de certificados para verificar la firma del firmante del certificado, garantizar la vigencia del certificado comprobando su periodo de validez y que no ha sido revocado por la CA y que además cumple con los requisitos para los que se expidió el certificado; por ejemplo, que el certificado sirve para firmar correo electrónico.

Los sistemas operativos avanzados como Windows Server suelen incorporar software suficiente para construir una infraestructura de clave pública completa (Figura 1.1). En el cifrado de la información pueden emplearse muchos métodos, pero fundamentalmente se utilizan dos: sistemas de una sola clave y sistemas de dos claves, una privada y otra pública.



Consola de administración de una entidad emisora de certificados integrante de una PKI en Windows Server 2003.

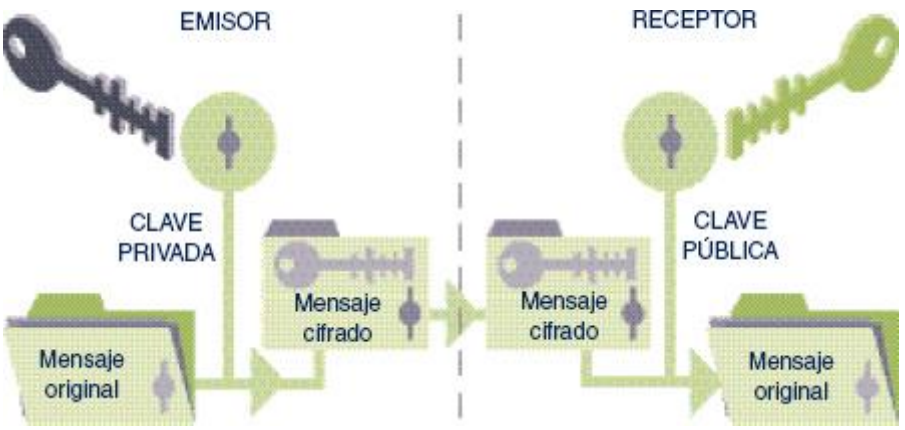
En el caso de utilizar una única clave, tanto el emisor como el receptor deben compartir esa única clave, pues es necesaria para desencriptar la información. Hasta aquí no hay ningún problema; sin embargo, el procedimiento de envío de esta clave al receptor que debe descifrar el mensaje puede ser atacado permitiendo que un intruso se apodere de esa clave.

Mucho más seguros son los procedimientos de doble clave. Consisten en confeccionar un par de claves complementarias, una de las cuales será pública, y que por tanto puede transmitirse libremente, y otra privada que sólo debe estar en posesión del propietario del certificado y que no necesitará viajar.

El algoritmo hace que un mensaje cifrado con la clave pública sólo pueda descifrarse con la clave privada que le complementa y viceversa.

Cuando el emisor quiere enviar un mensaje a un receptor, cifra la información con su clave privada que sólo él posee.

El receptor, una vez que le haya llegado el mensaje cifrado, procederá a descifrarlo con la clave pública del emisor



Cifrado y descifrado utilizando algoritmos de parejas de claves: pública y privada.

2.4 Arquitecturas PKI

En criptografía, una infraestructura de clave pública es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

Propósitos y Funcionalidad:

La tecnología PKI permite a los usuarios autenticarse frente a otros usuarios y usar la información de los certificados de identidad (por ejemplo, las claves públicas de otros usuarios) para cifrar y descifrar mensajes, firmar digital mente información, garantizar el no repudio de un envío, y otros usos.

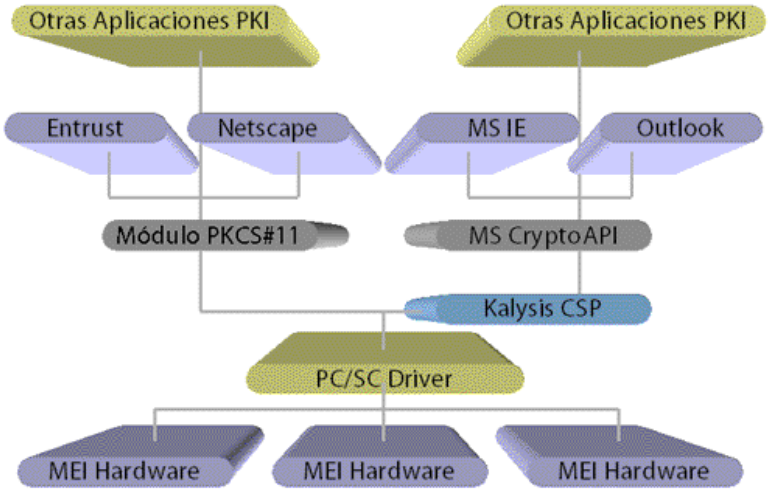
En una operación criptográfica que use PKI, intervienen conceptual mente como mínimo las siguientes partes:

- Un usuario iniciador de la operación.
- Unos sistemas servidores que dan fe de la ocurrencia de la operación y garantizan la validez de los certificados implicados en la operación (autoridad de certificación, Autoridad de registro y sistema de Sellado de tiempo).

- Un destinatario de los datos cifrados/firmados/enviados garantizados por parte del usuario iniciador de la operación (puede ser él mismo).

Las operaciones criptográficas de clave pública, son procesos en los que se utilizan unos algoritmos de cifrado que son conocidos y están accesibles para todos. Por este motivo la seguridad que puede aportar la tecnología PKI, está fuertemente ligada a la privacidad de la llamada clave privada y los procedimientos operacionales o Políticas de seguridad aplicados.

Es de destacar la importancia de las políticas de seguridad en esta tecnología, puesto que ni los dispositivos más seguros ni los algoritmos de cifrado más fuerte sirven de nada si por ejemplo una copia de la clave privada protegida por una tarjeta criptográfica se guarda en un disco duro convencional de un PC conectado a Internet.



Usos de la tecnología PKI

- Identificación del interlocutor
- Cifrado de datos digitales
- Firmado digital de datos (documentos, software, etc.)
- Asegurar las comunicaciones
- Garantía de no repudio (negar que cierta transacción tuvo lugar)

2.5 Políticas y prácticas de certificación.

La seguridad informática es una de las principales preocupaciones de las organizaciones. Es un área de las empresas que engloba tecnologías y procesos para proteger datos, redes y sistemas de ataques que pueden provocar daño y acceso no autorizado a información confidencial.

Con esto en mente, la industria de **ciberseguridad** juega un papel preponderante en los negocios digitales, ya que la integridad de los datos es clave para la operación, productividad y competitividad en los diferentes mercados en los que se desenvuelven las compañías.

Ante la velocidad con la que los delincuentes informáticos desarrollan sus estrategias de ataque y las tecnologías se desarrollan para contrarrestarlos, los profesionales con certificación en seguridad informática todavía son escasos, y eso supone un problema para las empresas que necesitan contratar a este tipo de expertos.

De acuerdo con el informe de **Estado de la Ciberseguridad de ISACA**, los encuestados señalaron que las brechas de habilidades más significativas que se observan entre los profesionales de seguridad cibernética son: la capacidad para entender el negocio (75%), habilidades de comunicación (61%)y la falta de procesos en la industria (61%).

Principales certificaciones de seguridad informática

- **SSCP (Systems Security Certified Practitioner).** Es ofrecida por el **Consorcio Internacional de Certificación de Sistemas de Información de Seguridad (ISC)** y certifica la capacidad para administrar e implementar la infraestructura de la empresa, y alinearla con las políticas de seguridad que permiten garantizar la confidencialidad de los datos.
- **CISSP (Certified Information Systems Security Professional).** En este caso, se trata de una certificación en seguridad informática ofrecida por ISC. Es ideal para quienes ya tienen conocimientos amplios, tanto técnicos como de gestión, así como experiencia. **Los expertos son capaces de diseñar, implementar y gestionar programas de seguridad propios.**

- **CRISC (Certified in Risk and Information Systems Control).** Se trata de una certificación en sistemas informáticos gestionada por Information Systems Audit and Control Association (ISACA), una asociación internacional que desarrolla metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información. Los profesionales que la obtienen pueden identificar, evaluar y preparar respuestas a diferentes riesgos de seguridad.
- **CISA (Certified Information Systems Auditor).** Está destinada a quienes realizan auditorías, controles y evaluaciones de los sistemas de **Tecnologías de Inormación (TI), también es gestionada por ISACA.** Los que la poseen tienen la capacidad de realizar evaluación de vulnerabilidades y establecer sistemas de control, entre otras mejores prácticas.
- **CISM (Certified Information Security Manager).** También es otorgada por ISACA y quienes obtienen esta certificación. Además, de ser competentes en temas de seguridad, demuestran aptitudes para comprender la relación entre los objetivos de la empresa y el programa de seguridad de la información de la organización, desarrollar y gestionar una estrategia de seguridad informática.
- **CompTIA Security+.** Se trata de una certificación en seguridad informática a nivel global que cubre los principios esenciales para la seguridad de la red y la gestión de riesgos. Quien posee esta certificación constata sus conocimientos para proteger y asegurar una red contra hackers.

Es importante recalcar que l**as certificaciones son a menudo difíciles de obtener, muchas personas pasan horas, semanas, incluso meses estudiando para los exámenes de certificación.** Sin embargo, la obtención es un referente del compromiso de los profesionales para la planificación y construcción de una ciberseguridad robusta para las empresas.

2.6 Gestión de una PKI.

Hoy en día es común oír acerca de temas como PKI, Web Services y SOA. Estos conceptos prometen facilitar y solucionar varias necesidades de las organizaciones en cuanto a

interoperabilidad, flexibilidad, re utilización, seguridad e integración de aplicaciones, pero llevar esto a la práctica no es tan trivial.

SOA, por un lado, está cambiando la forma en la que interoperan las organizaciones a nivel interno y externo. Esta tendencia conduce a sistemas de información conectados e integrados a través de la infraestructura que proporciona Internet, e introduce un nuevo entorno donde la funcionalidad de las aplicaciones se ofrece y accede como servicio. Al realizar cada servicio una tarea bien definida, se tiene una baja dependencia entre componentes de software que interactúan entre sí, lo cual permite dotar de flexibilidad la infraestructura tecnológica de un negocio, para que pueda responder a los cambios organizacionales u operacionales que traiga consigo la constante transformación del entorno en el que se desenvuelve.

Cualquier tecnología basada en servicios se puede utilizar para implementar SOA. Al ser esta una filosofía o enfoque de arquitectura, donde todas las actividades o procesos están diseñados para ofrecer un servicio**,** no especifica un protocolo específico a través del cual deban ofrecerse dichos servicios. CORBA (Common Object Request Broker Architecture), DCOM (Distributed Complement Object Model), RMI (Remote Method Invocation), ICE (Internet Communications Engine), EJB (Enterprise JavaBeans), MQSeries (hoy WebSphere) de IBM, ESB (Enterprise Service Bus), JMS (Java Messaging Service) y Web Services son algunas de las propuestas existentes para implementar SOA.

De todos estos, Web Services se postula como la tecnología más común para posibilitar arquitecturas orientadas a servicios, ya que se apoya en estándares, permite la integración de los procesos de negocio y proporciona interoperabilidad al ser independiente de plataformas, protocolos y lenguajes de implementación.

Por otro lado, la necesidad de ofrecer un entorno confiable para el intercambio de información en red, hace que PKI se convierta en una alternativa a evaluar por las organizaciones para cumplir con este propósito Comercio electrónico seguro, comunicaciones confidenciales y transacciones fiables son posibles con PKI, des afortunadamente las organizaciones enfrentan muchos problemas a la hora de adoptar este

tipo de solución pues es una tecnología costosa, tiene problemas de interoperabilidad y escalabilidad y resulta complicada para los usuarios finales.

Por lo tanto, a pesar de que en teoría son varias las utilidades y beneficios que traen consigo SOA y PKI, la implementación de esto en una organización es una tarea laboriosa: implica esfuerzo económico, operativo, administrativo y cambios en la cultura organizacional.

La realidad de las organizaciones es que, aunque quieran estar actualizadas y sacar provecho de los avances que día a día ofrece la industria tecnológica, optan por soluciones menos costosas, menos confusas y más rápidas y simples de implantar.

2.7 Estándares y protocolos de certificación

Los estándares tecnológicos son aquéllos que proporcionan un entorno de trabajo para el desarrollo de software y de aplicaciones que permiten el acceso y procesamiento de datos geográficos procedentes de diversas fuentes, a través de interfaces genéricas dentro de un entorno tecnológico abierto basado en estándares y protocolos amplia mente conocidos por la comunidad mundial de información geográfica y por la comunidad web.

Como tal, los estándares tecnológicos describen las tareas y la manera como se emplea la tecnología y la información para cumplir con metas de las diferentes entidades relacionadas con acceso y publicación de información geográfica en línea. Estos estándares también pueden llamarse estándares de servicios, los cuales describen los procedimientos y las metodologías para disponer la información geográfica en la web permitiendo diferentes niveles de publicación, tales como visualización, uso, descarga, procesamiento, acceso, etc.

Este tipo de estándares está relacionado con las especificaciones de la OGC. La especificación de implementación de OGC está detallada en el marco de trabajo del desarrollo de software para el acceso distribuido a los datos geográficos y a los recursos de procesamiento en línea de datos geográficos. Esta especificación proporciona tanto a los desarrolladores de software como a los usuarios de información geográfica, unas interfaces comunes detalladas que permiten que herramientas de software desarrolladas por

comunidades privadas y/o bajo filosofía de código abierto, puedan interoperar entre sí con información geográfica permitiendo el intercambio, uso y acceso de manera masiva a esta clase de datos.

Ejemplo de protocolo y estándares:

Protocolo de Emisión de un Sello de Tiempo

El usuario se identifica ante el sistema mediante certificado electrónico.
El servidor TSU establece comunicación con el servicio OCSP Responder y determina el estado de vigencia del certificado.
El TSU determina el estado de consumo de la cuenta cliente del usuario (servicio de pago).
El usuario envía el valor hash de un documento D; es decir, h(D), al servidor TSU.
El TSU añade al valor recibido el tiempo t, en la forma de fecha y hora de la recepción, componiendo (h(D), t).
El TSU procede a la firma digital de la asociación anterior, incluyendo los atributos, y se construye el Sello de Tiempo. El proceso de firma se realiza con un certificado que identifica al TSU emisor.
El TSU envía este Sello Digital de Tiempo al usuario. De esta forma, el usuario puede verificar el sello y probar ante otros que D existía en el tiempo t, con tan sólo verificar en cualquier momento la firma de la Autoridad de Timestamping.
El Sello de Tiempo, al incorporar el certificado del servidor TSU, permite determinar el TSU que lo emitió. El tiempo medio que un servidor TSU de ANF AC tarda en procesar un Sello de Tiempo es de 0,219 segundos.

Normas y Estándares

Todos los componentes que intervienen en el Servicio de Timestamping han sido desarrollados por el Departamento de Ingeniería de ANF AC, siguiendo y respectando las normas técnicas internacionales.

Entre ellas destaca el documento RFC 5816 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol" de la IETF (Internet Task Engineering Force), que actualiza el RFC 3161 de agosto de 2001 y es conforme con la norma ETSI TS 101 861.

Este documento determina que el Sellado Digital de Tiempo confiable se emite por un tercero de confianza, que actúa como Autoridad de Sellado de Tiempo o TSA (Time Stamping Authority). Así mismo permite el uso de la estructura ESSCertIDv2, tal como se define en el RFC 5035, para especificar el valor hash de un certificado del firmante, cuando el hash se calcula con una función distinta al algoritmo SHA-1.

Normas de referencia respetadas por ANT TSA AC

- [RFC 5816] "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)" (actualiza RFC 3161)
- RFC 3628 "Policy Requirements for Time Stamping Authorities (TSAs)"
- [TS 101 861] ETSI Technical Specification TS 101 861 V1.2.1. (2001-11). Time stamping profile
- [TS 102 023] ETSI Technical Specification TS 102 023. Policy requirements for Time stamping Authorities
- [ISO 18014] "Time-stamping services is an international standard that specifies Time stamping techniques"
- [ISO 8601] "Data elements and interchange formats — Information interchange — Representation of dates and times"
- [TF.460-5] ITU-R Recommendation TF.460-5 (1997): Standard- frequency and time-signal emissions
- [TF.536-1] ITU-R Recommendation TF.536-1 (1998): Time-scale nota

2.8 Ejemplo de un protocolo de seguridad: HTTPS.

Una conexión HTTP estándar en Internet puede ser fácilmente secuestrada por partes no autorizadas. El propósito de una conexión HTTPS es evitar esto: encriptar los datos para

asegurar una transmisión de datos segura. La transmisión está encriptada y el servidor autenticado.

Cuando un usuario hace clic en un enlace o confirma una entrada de URL en la barra de direcciones con el botón Enter, el navegador establece una conexión. El servidor presenta un certificado que lo autentica como un proveedor genuino y confiable. Una vez que el cliente ha verificado la autenticidad, envía una clave de sesión que sólo puede leer el servidor. Sobre la base de estos datos clave, ahora se puede realizar el cifrado. Normalmente, se utiliza un certificado SSL.

Antecedentes y objetivos

El propósito de una conexión HTTPS es proteger los datos que se transmiten. Una conexión HTTP puede ser fácilmente interceptada, permitiendo ataques específicos a individuos. Los datos introducidos por un usuario en la ventana de su navegador son a menudo personales (información de la cuenta, correo electrónico, información de la tarjeta de crédito, etc.) y deben protegerse de dicho acceso.

Otro problema es la suplantación de identidad (phishing), mediante la cual los datos introducidos por un usuario se envían a personas no autorizadas que utilizan sitios web falsos. El uso de HTTPS en lugar de HTTP puede evitar tanto la interceptación como el phishing. Esto último es posible con un certificado. En otras palabras, el objetivo de HTTPS es proporcionar a los usuarios de Internet privacidad, seguridad y protección de datos.

Uso y relevancia

HTTPS se utiliza para todos los sitios web en los que un usuario introduce datos. Un campo de aplicación importante es la banca online. En cualquier lugar donde se utilice una cuenta protegida por contraseña, sería sensato tener una conexión HTTPS. Esto incluye el acceso a redes sociales, o cuentas de correo electrónico y de compras, en las que de otro modo se podría causar un gran daño personal con la adquisición ilegal de datos personales. La información personal también puede ser enviada sin una cuenta. Si, por ejemplo, un vuelo

o unas vacaciones enteras se reservan en línea, entonces los datos aplicables deben ser comunicados a los proveedores de una manera segura.

En su propio interés, cualquier usuario de Internet debe prestar atención a una conexión segura en el lugar correcto y así proteger su privacidad. Si existe una conexión HTTPS se puede ver fácilmente en la barra de direcciones. Mostrará "https" al principio e incluso se resalta en muchos casos. También se muestra un pequeño icono de candado.

Desventajas

El HTTPS tiene algunas desventajas en comparación con las conexiones HTTP. Sin embargo, son muy pocas y deberían aceptarse como un compromiso por la seguridad que proporcionan.

- Hay cargos adicionales por certificados y costes crecientes con el aumento del tráfico. Estos pueden ser particularmente altos. Especialmente para sitios web nuevos y pequeños, estas tarifas pueden llegar a ser relativamente altas.
- Con conexiones HTTPS, el contenido no puede almacenarse en caché. Pero la tendencia hacia un mayor ancho de banda contrarresta esta desventaja.
- Un punto débil es también el menor rendimiento resultante del uso del cifrado SSL. El servidor debe realizar muchos más cálculos, aumentando así el tiempo de respuesta.
- Los hosts virtuales no funcionan con HTTPS.

Ventajas

Además de la ventaja obvia de la privacidad en línea, también hay otro pro. El uso de HTTPS no requiere ninguna instalación de software adicional. Esto significa que puede ser utilizado sin restricciones por cualquier persona. La autenticación con un certificado también inspira confianza en los clientes potenciales.

Diferencia con HTTP

La principal diferencia es la seguridad. La tecnología es esencialmente la misma, pero HTTPS incluye encriptación SSL. Por lo tanto, en principio es posible establecer todo Internet con conexiones HTTPS. Sin embargo, debido a las desventajas antes mencionadas y por costumbre, casi nadie utiliza una conexión segura cuando no es absolutamente necesaria.

Seguridad

Dado que la diferencia con el HTTP es el uso de cifrado, la seguridad HTTPS depende únicamente de la técnica de cifrado utilizada. Actualmente se trata de SSL, que generalmente se considera segura. Sin embargo, debe tenerse en cuenta que una transmisión de datos segura por sí sola no es suficiente para protegerlos completamente, sino que también debe ser almacenada de forma segura por el destinatario.

2.9 SSL

Aunque pueda parecernos que es ahora cuando las comunicaciones a través de medios tecnológicos deben ser más seguras que antes, contando con que ha existido una especie de "edad de la inocencia" de **Internet**, lo cierto es que en todas las épocas ha existido el peligro de que alguien lea nuestros mensajes o irrumpa, virtualmente, en nuestras computadoras.

Es por ello que, de una forma u otra, siempre se han volcado más o menos esfuerzos en conseguir que las comunicaciones sean seguras y, para ello, se han ido creando una serie de protocolos y tecnologías que nos ayudan a garantizar la integridad y confidencialidad.

El SSL y el TLS son, respectivamente, el original y el sucesor, de un protocolo criptográfico utilizado para asegurar las comunicaciones en redes telemáticas, principalmente Internet.

Lo que hacía el SSL (*Secure Sockets Layer*) y continúa haciendo TLS (*Transport Layer Security*) de forma más eficiente, es cifrar las comunicaciones mediante el uso de criptografía en diversos servicios online, como el **correo electrónico** o la web.

Constituye un estándar de Internet, elaborado, mantenido y reconocido por los **organismos** de dirección técnica de la red de redes, con la cual cosa es universal, independiente de fabricante y cuyo uso es facilitado a cualquier desarrollador de soluciones que trabaje creando software y servicios en Internet.

La historia de ambos protocolos se remonta a mediados de la década de los 90, cuando se empezó a utilizar SSL 2.0 (la versión 1.0 nunca llegó a estar disponible para el público general).

2.10 TSL

TLS 1.0 es una reimplementación mejorada de SSL 3.0, con suficientes diferencias para que ambos sean incompatibles entre ellos.

Las diferencias entre TLS y SSL es que la primera mejora al segundo corrigiendo vulnerabilidades de seguridad que se han ido encontrando en SSL, y que en TLS se autentifica al cliente, mientras que en SSL no.

Este último detalle es muy importante, ya que permite asegurar que, en una "conversación" entre programas y servicios a través de Internet, tanto el **cliente** como el servidor son quienes dicen ser, y que no hay nadie "escuchando" las comunicaciones de por medio.

En cambio, en SSL, alguien podía interceptar las comunicaciones y hacerse pasar por el cliente, ya que no existía verificación de la **identidad** de este, solamente en el caso del servidor se verificaba.

2.11 SSH

SSH (*Secure SHell*) es un programa que nos permite comunicarnos, mediante una línea de comandos, con un servidor remoto de forma segura

Y lo hace, como en el caso anterior, basándose en la criptografía para cifrar las comunicaciones intercambiadas con el servidor, de forma que nadie pueda sacar la información de los paquetes que se cruzan entre ambos.

Es una herramienta presente en la gran mayoría de los sistemas operativos de hoy en día, puesto que permite la **administración** remota y simplificada de un servidor.

Habitualmente, contamos con herramientas que funcionan sobre web, proporcionando un entorno **gráfico**, pero estas son lentas y dependen, para su ejecución, de que varios elementos estén funcionando sobre el servidor, como un servidor web.

En cambio, SSH solamente necesita de su propio servidor, muy simple y que ocupa pocos **recursos**, y no requiere siquiera de entorno gráfico, con lo cual podemos utilizarlo en los entornos más simples.

Que sea un entorno de línea de comandos significa que deberemos conocer el listado de órdenes que acepta el sistema operativo de la computadora a la cual nos conectamos.

El sistema es el mismo que el antiguo MS-DOS para las computadoras domésticas PC antes de la llegada de Windows, y sustituye al Telnet, otro programa que hacía antiguamente lo mismo, pero que no incluía la **seguridad** añadida de la criptografía para las comunicaciones.

Prueba con un generador de certificados gratuito, libre y en línea.

El OpenCA PKI Research Labs, nacida de la antigua Proyecto OpenCA, es una organización abierta dirigida a proporcionar un marco para el estudio de PKI y desarrollo de proyectos relacionados. A medida que el PKI normas, intereses y proyectos están creciendo rápidamente, se ha decidido dividir el proyecto original en otros más pequeños para acelerar y reorganizar los esfuerzos. Algunos proyectos ya han comenzado y recibidos (siempre que sea posible) los fondos, mientras que otros están encontrando su camino a la etapa de decisión final.

OCSPD v2.4.3 (BEHAPPY)

La nueva versión (v2.4.3/BeHappy) de OCSPD del OpenCA disponible. Cambios en su mayoría implican la actualización de soporte para LibPKI 0.8.1 que corrige un problema de análisis de URI con peticiones HTTP GET . Descarga la nueva versión de su sistema en las páginas de descarga OCSPD .

LIBPKI v0.8.1 (Bemore)

La nueva versión (v0.8.1/BeMore) de LibPKI disponible. Cambios en su mayoría implican la corrección de errores y análisis de URI (corrige un error en OpenCA OCSPD con peticiones HTTP GET) . Descarga la nueva versión de su sistema en las páginas de descarga LibPKI .

OCSPD v2.4.2 (Ocampa)

Una nueva versión de la OCSPD respondedor está disponible para su descarga. Las principales mejoras respecto a la última versión disponible al público son: soporte actualizado para LibPKI 0.8.0 +, inicio fija / parada guión, pérdidas de memoria fija , Corregido el error en la configuración que impide la recarga de las CRL caducadas , mejora el tiempo de respuesta , soporte fijo para la solicitud GET tipos .

OpenCA PKI V1.5.0 (SpecialK)

El OpenCA PKI v.1.5.1 (SpecialK) está fuera ! Esta versión incorpora todas las correcciones de errores de la v1.3.0 . Los cambios están disponibles en el enlace Registro de cambios desde la página de descargas OpenCA .

LIBPKI v0.8.0 (secuestrar)

La nueva versión (v0.8.0/Sequester) de LibPKI disponible. Cambios en su mayoría implican la corrección de errores . Descarga la nueva versión de su sistema en las páginas de descarga LibPKI .

LIBPKI V0.6.7 (PAPOCCHIO)

La nueva versión (v0.6.7/Papocchio) de LibPKI disponible. Los principales cambios son más v0.6.5 : inicialización respuesta OCSP fija, añade soporte para url DNS para recuperar los registros DNS a través de la simple URL_ * interfaz, añadido soporte inicial para el peso ligero Tokens revocación de Internet (LIRTs) descargar la nueva versión de su sistema en el LibPKI descargar páginas .

LIBPKI V0.6.5 (HOPE)

La nueva versión (v0.6.5/Hope) de LibPKI disponible. Los principales cambios son más v0.6.4 : Corregido un error de codificación de clave en OpenSSL , añadió nueva pki - siginfo herramienta para facilitar la información recogida de firmas para X509 objs , añadió PKI_X509_KEYPAIR_get_curve () para obtener la curva en relación con una clave de EC , añadió posibilidad de cargar cualquier tipo de X509 objetos mediante PKI_X509_get () con PKI_DATATYPE_ANY como un tipo , fija un error al configurar el algoritmo de firma en PKI_X509_CERT_new (), soporte mejorado para la gestión de claves ECDSA . Descarga la nueva versión de su sistema en las páginas de descarga LibPKI .

LIBPKI V0.6.4 (BROADWAY)

La nueva versión (v0.6.4/Broadway) de LibPKI disponible. Los principales cambios son más v0.6.3 : código HTTP fijo (error de asignación de memoria) , el aumento de la herramienta de línea de comandos para la manipulación de CRL (pki -CRL) . Descarga la nueva versión de su sistema en las páginas de descarga LibPKI .

OCSPD V2.1.0 (ELLIE)

Una nueva versión de la OCSPD respondedor está disponible para su descarga. Las principales mejoras respecto a la última versión disponible al público son: Actualizado archivos predeterminados de configuración (Passin defecto es ninguno) , soporte mejorado

para el apoyo ECDSA , gestión de hilo actualizado con soporte incorporado de LibPKI 0.6.3 , script de arranque / parada fija , fija un error de memoria en config.c causando segfault de recarga CRL , eliminan extra de dos bytes enviados después de la codificación DER de la respuesta se escribe (que estaba causando Firefox / Thunderbird no para validar la respuesta) , fija un error en la devolución de cheques código para PKI_NET_listen , fijado error en el análisis de configuración cuando se dio ninguna dirección de enlace.

LIBPKI V0.6.3 (VIPER)

La nueva versión (Viper/v0.6.3) de LibPKI disponible. Los principales cambios son más v0.6.1 : soporte ampliado para ECDSA (a través del perfil / keyparams en archivos de configuración del perfil) , vinculador fijos en Solaris , agregó pki -cert herramienta de línea de comandos, código de la biblioteca ocsp fijo. Descarga la nueva versión de su sistema en las páginas de descarga LibPKI .

DemoCA en directo por madwolf@12.12.2010

La demostración en línea CA está de vuelta en línea, debido a la gran demanda de personas interesadas en el software OpenCA PKI. Vamos a tratar de mantenerlo en línea tanto como sea posible , por favor ten cuidado, sin embargo, que es sólo un servicio de DEMO y ninguna responsabilidad está implícita .

Versión actual de la línea CA es v1.1.1 .

OCSPD FIREFOX FIX

Debido a un bug en Firefox (gestión de memoria) , es necesario tener la OCSPD ser compilado con la LibPKI v0.6.1 + . Por favor, descargue el código fuente y volver a compilar el demonio de una vez al día la biblioteca de criptografía.

OCSPD 2.0.0

Una nueva versión de la OCSPD respondedor está disponible para su descarga. Las principales mejoras respecto a la última versión disponible al público (en su mayoría

procedentes de apoyo para LibPKI v0.6.0) son: un amplio soporte para los dispositivos de hardware (PKCS # 11 y OpenSSL Motor) , par de claves múltiples y soporte certificado para firmas de respuesta , POST y GET apoyo , IPv6 apoyar .

LIBPKI v0.6.0 (TURQUÍA)

La nueva versión (Turkey/v0.6.0) de LibPKI disponible. Los cambios importantes durante v0.5.1 son: soporte para IPv6 en las llamadas de red , soluciones para análisis de la URL y PKI_SSL_ * Mejoras en la interfaz . Obtener la nueva versión de su sistema en las páginas de descarga LibPKI .

LIBPKI v0.5.1 (ZOIBERG)

La nueva versión (Zoiberg/v0.5.1) de LibPKI disponible. Los principales cambios son más v0.5.0 : . Mejor soporte para OS Gestión Thread independiente junto con las primitivas de sincronización de subprocesos (mutexes , variables de estado, y las cerraduras r / w , correcciones de interfaz LDAP Obtener la nueva versión de su sistema en las páginas de descarga LibPKI .

repositorios yum

28.08.2010 # Madwolf

Repositorios Yum para proyectos OpenCA se han creado . Si su sistema es compatible con Yum (y RPM), puede utilizar los enlaces proporcionados para instalar la configuración del repositorio en su sistema.

LIBPKI v0.5.0

La nueva versión (lulu/v0.5.0) de LibPKI está disponible para su descarga. Muchos cambios en la biblioteca y la corrección de errores sobre la versión antigua . En particular : añadido soporte para diferentes sistemas operativos (soporte inicial para el puerto Win) , añadió

PKI_SSL y apoyo para la gestión fácil SSL / TLS, añade soporte para Win API LDAP, ha añadido soporte para las arquitecturas de 64 bits , añade codificación URL seguro para el protocolo HTTP GET.

UNIDAD III SEGURIDAD EN REDES

3.1 Aspectos de seguridad en las comunicaciones

La información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad cosa que no ocurre con los equipos, la documentación o las aplicaciones, y además las medidas de seguridad no influyen en la productividad del sistema sino más bien al contrario, por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

La seguridad debe contemplar no sólo que no accedan intrusos, sino que los sistemas y las aplicaciones funcionan y son utilizados correctamente. Los niveles de seguridad no pueden, ni deben, ser iguales para todos los elementos (usuarios, aplicaciones,) que gestionan la información.

Las medidas de seguridad deben contemplar algunos de los siguientes aspectos:

- Identificación biunívoca de los usuarios (Users ID)
- Claves de acceso (password) de al menos 6 caracteres y ficheros de claves protegidos y encriptados.
- Modificación periódica de las claves de acceso (como mínimo cada tres meses)
- Registros de control del uso correcto, intentos incorrectos
- Acceso remoto seguro
- Cifrado y firma digital en las comunicaciones
- Posibilidad de desconectar si no se usa un terminal e identificación de la persona que desconecta.
- Salvaguardas y copias de seguridad.
- Planif icación de desastres.
- Formación de los usuarios en los aspectos de seguridad.

El nivel de desarrollo de estas medidas depende de la naturaleza de la organización, de la información, de las aplicaciones, de quienes las usan y acceden a las mismas.

Plan de Seguridad

La puesta en marcha de un plan de seguridad no es algo estático que se hace una vez. Una de las principales garantías de que un sistema es seguro es que se realiza un seguimiento de las medidas puestas en marcha, de los registros de auditoría. El seguimiento de las medidas de seguridad es la vía para asegurar que el plan se adapta a la organización y para detectar posibles intentos de fraude o acceso incorrecto.

El desarrollo de redes globales a las que se accede desde cualquier parte del mundo con un coste bajo y desde cualquier hogar como es INTERNET, aumenta estadísticamente la probabilidad de que alguien no autorizado intente acceder a mi red.

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

- Errores de los empleados:50%
- Empleados deshonestos 15%
- Empleados Descuidados 15%
- Intrusos ajenos a la Empresa 10%
- Integridad física de instalaciones 10%

Los planes de seguridad deben considerar la tipología de la información, de los usuarios de la misma y de los equipos y sistemas.

En un plan típico de seguridad se deben considerar los siguientes aspectos:

- Seguridad física de los locales y acceso donde se encuentran los sistemas.
- Asegurarse contra todos los riesgos posibles; esto requiere un periodo de observación y una clasificación de los recursos y sistemas que están en los edificios de la Organización, los que están fuera, los puntos de acceso remoto, las costumbres y hábitos del personal y el uso de la microinformatica estática y portátil.
- Asegúrese que es una integración por encima de los sistemas, plataformas y elementos que constituyen las redes, ..

- La gestión de la seguridad debe de ser centralizada.

Entrando ya más en el detalle, el plan debe de especificar las tareas a realizar, cómo se definen los niveles de acceso, cómo se audita el plan, cómo se realizará el seguimiento, dónde deben ponerse en marcha medidas específicas (cortafuegos, filtros, control de acceso,),.....

El sentido común debe jugar un papel de relevancia, ya que, si no es así, se pueden llegar a proponer medidas muy seguras, pero realmente impracticables, lo cual significa que hay que asumir ciertos riesgos.

Ataques o amenazas

Podemos definir un Ataque o Amenaza como la potencial violación de un sistema de seguridad. Estas tácticas o amenazas pueden producirse a partir de alguno de estos hechos:

- Modificación ilegal de los programas (virus, Caballos de Troya, borrado de información).
- Deducción de Información a partir de datos estadísticos o de uso que se utilizan para reconstruir datos sensibles
- Destrucción y modificación de datos controlada o incontrolada.
- Cambiar la secuencia de los mensajes.
- Análisis del tráfico observando los protocolos y las líneas de comunicación o los discos de los ordenares.
- Perdida del anonimato o de la confidencialidad.
- Uso de una identidad falsa para hacer transacciones o enviar operaciones.
- Impedir que a un usuario que puede usar los recursos lo haga.

- Violación de los sistemas de control de acceso.

Los "crackers", piratas o violadores informáticos con interés en atacar un sistema para obtener beneficios de forma ilegal, los "hackers", que son aquellos que lo hacen simplemente como pasatiempo y reto técnico (más respetuosos que aquellos con la información), y los "sniffers", que rastrean y observan todos los mensajes que hay en la red, constituyen nuevas tipologías de intrusos que cada vez están adquiriendo mayor relevancia en el panorama de la seguridad.

Los "crackers", una vez que acceden a un sistema, pueden entre otras cosas coleccionar las claves de acceso a los diferentes nodos y sistemas de la red para su posterior uso, o bien dejar programas que les permiten el posterior acceso al sistema.

Su objetivo es acceder al sistema operativo al más alto grado de prioridad para controlar las aplicaciones, borrar ficheros, introducir un virus, ...

Los Agentes externos no constituyen, sin embargo, el mayor peligro para una red de área global. Un estudio realizado en más de 2000 compañías encontró que el 65% de los gastos incurridos (más de 5 billones anuales de dólares en pérdidas) fueron generados por errores y mal uso de los propios usuarios de la red y no por agentes externos. El ejemplo más claro lo tenemos en los virus informáticos: el 90% de los virus los introducen en las organizaciones los propios usuarios a través de programas, juegos, disquetes, que nunca deberían haber usado y que en algún caso tenían prohibido hacerlo.

Mecanismos para garantizar la Seguridad

Los mecanismos para garantizar la seguridad no pueden ser ajenos a los sistemas informáticos que deben de ejecutarlos: de nada sirve poner en un papel que las claves de acceso tendrán 15 caracteres si luego nuestros programas sólo admiten 6. Esto que parece tan obvio indica que la gestión de las redes y la seguridad de las mismas son en ci erto modo inseparables.

Las passwords o claves de acceso suelen ser uno de los puntos más vulnerables para atacar un sistema. Cuando se teclea una clave correcta el sistema interpreta que el usuario esta autorizado a hacerlo. En general, los usuarios no toman precauciones a la hora de definir

sus claves de acceso, se están utilizando algunos programas que generan cadenas que no están en los diccionarios y que son fáciles de recordar para evitar que alguien descubra un montón de claves de una organización sin más que probar con todas las palabras que hay en un diccionario (eso sí, electrónico).

El comercio electrónico en Internet llegará a convertirse, a medio plazo, en un hecho tan habitual como el comercio convencional. Los medios de pago utilizados serán las tarjetas de débito y crédito, probablemente en una modalidad "inteligente".

Pero para que ello ocurra, es necesio que todos los actores que intervienen en el proceso adquieran la convicción de la seguridad de los diversos intercambios de información que tienen lugar, más aún si dicha información asume la representación de valores en la esfera de la circulación de las mercancías y el dinero.

Sin embargo, existe una segunda perspectiva para aquilatar debidamente el tema de la seguridad de los datos: la privacidad de las comunicaciones electrónicas es una extensión natural de los derechos individuales de libertad de expresión, intimidad, integridad, seguridad, propiedad intelectual y protección de la honra de las personas, reconocidos tanto en la Declaración Universal de los Derechos del Hombre como en las constituciones de la inmensa mayoría de los países del orbe.

Como fuere, el hecho es que, desde el punto de vista técnico, la investigación y desarrollo, particularmente en las áreas de encriptación y cifrado de mensajes, ha proveído soluciones consistentes, sin perjuicio de que en materia de seguridad la prudencia aconseja considerar todo avance como un paso esencialmente trasitorio.

Objetivos para proteger la seguridad

En términos genéricos, el objetivo de proteger la información apunta a obtener:

- Confidencialidad, esto es, que los mensajes transferidos o recibidos, sean secretos y nadie más que su legítimo destinatario tenga acceso a ellos.
- Disponibilidad, es decir, que los recursos estén disponibles cuando se necesiten, y que no se usen indebidamente o sin autorización de su autor.
- Integridad y confiabilidad, que consiste en la certeza que el mensaje transferido no ha sido modificado en ninguna parte del circuito o proceso de transferencia.

Niveles de los mecanismos de seguridad

Por definición, el tema de la seguridad de los datos distingue tres niveles:

A. Seguridad a nivel de los sistemas.
B. Seguridad en recursos y servicios.
C. Se guridad de la información.

A Seguridad a Nivel de los Sistemas

En el nivel de los sistemas, el administrador tiene la opción de arbitrar las siguientes medidas de seguridad:

- Control de password, o claves secretas de usuarios. Esto pasa por identificar passwords triviales o fáciles de detectar; manejar un sistema de passwords con tiempo de expiración; y detectar cuentas sin passwords, que generen alarmas ante fallas reiteradas de acceso.
- Control de usuarios, es decir, revisión periódica de las características del usuario en cuanto a los privilegios otorgados, al acceso a información que disponen, horario de conexión asignado, etc.

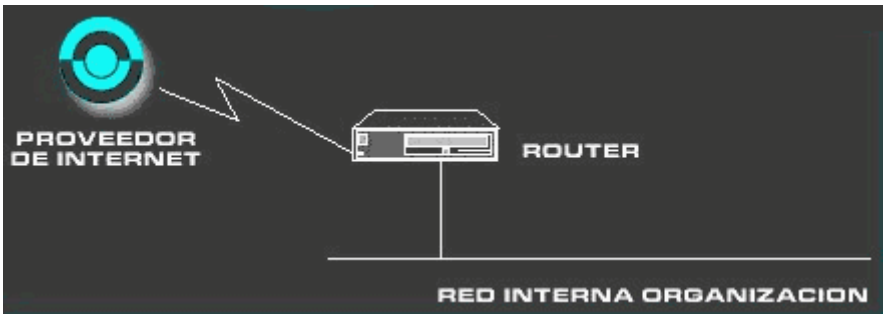
- Control de acceso, esto es, revisar periódicamentel cómo, el cuándo y desde dónde se puede acceder al sistema.

- Generación de reportes, que den cuenta de anomalías o problemas encontrados en cualquiera de los controles indicados anteriormente.

B Seguridad a Nivel de Recursos y Servicios

Las medidas de seguridad orientadas a proteger la red misma y los recursos y servicios involucrados tales como ancho de banda, tiempo de respuesta, acceso a servidores de la red, etc, consisten en la instalación de mecanismos o dispositivos denominados firewalls o cortafuegos, cuya función principal es mantener un control del acceso a la red y los recursos.

Existen tres tipos de firewalls:



Esquema básico de un firewall

1. Filtro de Paquetes: que filtra sobre la base de la información contenida en un paquete, como por ejemplo port del servicio (FTP, SMTP, etc), tipo de protocolo (TCP, UDP, ICMP) o direcciones de origen y/o destino del paquete. Se puede realizar el filtro en la entrada, salida o en ambas partes. Se configura de acuerdo a un host, un conjunto de host o redes que pueden o no hacer uso de recursos o servicios en la red, también se puede restringir el conjunto de routers con los que se puede intercambiar información de ruteo. Normalmente este tipo de firewall se implementa en el router que hace de puerta de entrada a Internet. La filosofía de los firewalls de filtro de paquete es "todo lo que expresamente no sea permitido será prohibido", lo que lo hace ser muy restrictivo.

2. Gateway a Nivel de Circuito: que controla el acceso a la red según quién lo esté solicitando y el servicio de red que se provee, y retransmite conexiones TCP. El origen conecta un port TCP de la gateway, el cual conecta a su vez al destino solicitado, al otro lado de la gateway. El problema de este firewall es que sólo traspasa bytes desde el origen al destino y viceversa, por lo cual el usuario inadvertidamente puede subvertir el sistema de seguridad corriendo servicios de red en port no-standard.
3. Gateway a nivel de aplicación: que es un mecanismo específico para una aplicación de red. Para cada servicio entre la red interna y externa se debe desarrollar una aplicación por lo que se restringe bastante el uso de servicios especiales o nuevos.

C) Seguridad de la Información:

El nivel de seguridad de la información es probablemente el más importante, toda vez que es aquel en que mayor participación le cabe al usuario, y al igual que en los casos anteriores, distingue varias clases y niveles.

A nivel de protocolos, el protocolo IP provee dos header o encabezamientos de datagramas, destinados a la seguridad: el AH (Authentication Header) y el ESP (Encapsulating Security Payload), cuyos detalles pueden encontrarse en el RFC 1825, Security Architecture for IP.

A nivel de transporte, Netscape propuso el estándar SSL (Secure Socket Layer), que genera un "túnel" virtual entre el cliente y el servidor, a través del cual circulan los datos, encriptados con el sistema DES, en condiciones de seguridad.

NETSCAPE_(Un ejemplo de seguridad en buscadores)

- Netscape SSLREF

Es una implementación de la recomendación del protocolo 'Secure Sockets Layer' cuya finalidad es ayudar y acelerar los esfuerzos de los desarrolladores en proveer seguridad avanzada en las aplicaciones TCP/IP que utilicen SSL. SSLRef se compone de una librería, cuyo fuente se distribuye en ANSI C, que puede compilarse en una amplia variedad de plataformas y sistemas operativos y linkados con programas de aplicación. En la actualidad es de libre distribución para fines no comerciales.

- OPEN STANDARDS

La tecnología de seguridad en Internet desarrollada por Netscape para asegurar comunicaciones privadas y autentificadas (SSL, Secure Sockets Layer protocol) es una plataforma abierta de dominio público para la comunidad de Internet.

- ASPECTOS DE SEGURIDAD DE NETSCAPE

a. Tecnología de seguridad de Netscape

Las facilidades de seguridad integradas en 'Netscape Navigator' y 'Netscape Commerce Server' protege las comunicaciones por Internet con:

- Autentificación de Servidores
- Privacidad mediante encriptación.
- Integridad de los datos.

Sin una seguridad completa, la información transmitida en Internet es susceptible de intervención por intermediarios. La información que viaja entre nuestro computador y cualquier servidor utiliza un proceso de enrutamiento que la hace pasar por otros sistemas computadores de la red. Cualquiera de estos sistemas de computadoras representa intermediarios con el potencial de acceder al flujo de información entre nuestro computador y el servidor destino. Es necesario por ello métodos de seguridad que asegure que estos intermediarios no intervienen de alguna forma sobre nosotros. Internet por sí mismo no facilita esta seguridad.

El protocolo 'SSL' proporciona autentificación de servidores, encriptación de los datos e integridad de los mensajes. SSL se sitúa por debajo de los protocolos de aplicación, tales

como HTTP, Telnet, FTP, Gopher, y N NTP, y por encima del protocolo de conexión TCP/IP. Esta estrategia permite a SSL operar de forma independiente a los protocolos de aplicación de Internet. Con SSL implementado en el cliente y en el servidor, las comunicaciones Internet son transmitidas de una forma encriptada, asegurando de esta forma la privacidad.

Con la tecnología de seguridad de Netscape, se puede confiar en que la información enviada llega de una forma privada y sin alterar al servidor especificado y no a ningún otro.

SSL utiliza la tecnología de autentificación y encriptación desarrollada por 'RSA Data Security Inc'. La encriptación establecida entre nosotros y un servidor remoto permanece válida a través de las múltiples conexiones, aún más, el esfuerzo utilizado en vencer la encriptación de un mensaje no afecta en el siguiente mensaje.

'Netscape Navigato y 'Netscape Commerce Server' incorporan autentificación de servidor utilizando firmas digitales certificadas facilitadas por terceras partes conocidas como 'autoridades certificadoras'. Un certificado digital verifica la conexión entre una clave pública de un servidor y la identificación del servidor. La criptografia comprueba, por medio de las firmas digitales, asegurando que la información dentro de un certificado puede ser autentificada.

b. Transmisión segura de Información Personal tal como tarjetas de crédito

   Se puede introducir el número de la tarjeta de crédito en un formulario de 'Netscape' seguro (https) y transmitir el formulario en Internet a algún Servidor Netscape Comercial Seguro sin riesgo de que en algún punto intermedio se obtenga el número de la tarjeta de crédito.

   Las facilidades de seguridad ofrecidas por la tecnología de comunicaciones Netscape protege las transacciones comerciales, además de otras comunicaciones.

   Las comunicaciones seguras no eliminan todo lo concerniente a los usuarios de Internet. Los administradores de los servidores deben tomar precauciones adicionales para prevenir agujeros en la seguridad. Para proteger nuestra

información en dichos servidores, ellos deben mantener la seguridad física de sus servidores y controlar el acceso mediante claves privadas.

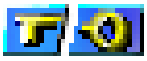
c. Información facilitada por Netscape sobre seguridad.

Netscape identifica a los documentos seguros de diferentes formas. Se puede conocer cuando un documento procede de un servidor seguro observando el campo de localización (URL). Si la URL comienza con "https://" en lugar de "http://", sabemos que el documento procede de un servidor "seguro".

Se necesita utilizar https:// para las URLs HTTP con SSL y http:// para las URLs HTTP sin SSL.

Además se puede verificar la seguridad de un documento examinando el icono de seguridad de la esquina inferior-izquierda de la pantalla principal de Netscape y la barra de color situada por encima del área de contenido.

El icono consiste en una llave con un fondo azul para los documentos seguros y una llave rota con fondo gris para los documentos no seguros



Un documento que contenga ambas, información segura y no segura, se muestra como seguro, con la información no segura reemplazada por una icono de seguridad mixta. Algunos servidores pueden permitirnos acceder a los documentos no seguros (utilizando "http://") permitiéndonos visualizar documentos mixtos sin sustitución por icono.

Podemos obtener información más detallada sobre la seguridad seleccionando la opción de menú File/Document Information. Varias cajas de diálogo de notificación nos informaran cuando entremos o abandonemos un espacio seguro. Siempre seremos avisados si un URL seguro es redireccionado a una localización no segura, o si submitimos un formulario seguro utilizando un proceso de submisión no seguro.

d. Información facilitada por la opción 'Document Information'

&sp;

Seleccionando el ítem de menú File/Document Information visualiza una caja de diálogo que muestra la siguiente información sobre el documento en uso:

- Título del documento.
- Localización (URL).
- Fecha de la última modificación.
- Juego de caracteres.
- Estatus de seguridad.

Los documentos seguros especifican el tipo de encriptación que protege al documento y la versión, número de serie, distribuidor y el servidor sujeto del certificado devuelto por el documento.

Encryption Key

Tipo de clave pública soportada.

Subject (server id)

El proceso de solicitud de certificación requiere del administrador de cada servidor que facilite la dirección e-mail y cierta información de identificación. Esta información de identificación puede incluir:

- Country (C): Código del país.
- State or Province (ST): Nombre del Estado o Provincia.
- Organization (O): Nombre de la organización.
- Organizational Unit (OU): Nombre del departamento (opcional).
- Locality (L): Localidad
- .Common Name (CN): Nombre del servidor.

Issuer (certifier id)

Identifica la autoridad que entrega el certificado. La información de identificación se presenta utilizando las mismas abreviaciones que las utilizadas para identificar al servidor. (C, para el país, etc.).

b. Firma Digital

Para operar utilizando las facilidades de seguridad, 'Netscape Commerce Server' necesita de un certificado de firma digital. Sin el certificado, el servidor puede únicamente operar en forma no segura.

'Netscape Communications' ha contratado los servicios de 'RSA Certificate Services', una división de la empresa 'RSA Data Security, Inc.', para distribuir certificados a los clientes del producto 'Netscape Server'. Durante el proceso de solicitud, el software de nuestro servidor genera una pareja de claves pública/privada y se elige un nombre. El formulario en línea nos guía a través del proceso de submitir el proceso a RSA.

RSA verifica la autenticidad de cada solicitud de certificado. Una vez autentificado, RSA nos devuelve vía e-mail un certificado firmado digitalmente único. Una vez recibido se puede instalar la firma y activar la seguridad. Los certificados estás protegidos por una pareja de claves públicas y privadas ligadas a un potente algoritmo criptográfico. Se deberá establecer precauciones adecuadas para mantener la integridad de la firma y nuestra clave privada.

Técnicamente, un certificado puede utilizarse en múltiples servidores, aunque en muchas circunstancias pueden aparecer riesgos que nos hagan abandonar esta elección. Si se utiliza el mismo certificado en múltiples servidores, algún problema con la pareja de claves pública y privada, puede poner en peligro al resto servidores.

De forma similar ocurre si deseamos utilizar la misma llave de seguridad para la casa, la oficina, el coche, etc. Sólo utilizamos una llave, pero no tenemos la flexibilidad de proveer el acceso a uno de estos elementos sin proveer de acceso a todos los demás. Si se compromete la seguridad de un elemento, comprometerá la seguridad del resto.

c. Limitaciones impuestas por la seguridad

El protocolo de seguridad trabaja como un añadido a los otros protocolos sin limitar las capacidades de acceso. Se puede utilizar Netscape para traer documentos seguros y no seguros. La seguridad no limita las capacidades de noticias Usenet o correo electrónico.

Si un documento que es seguro contiene información que no es segura, la información insegura es reemplazada por un icono de seguridad mixta. Aunque, un servidor puede permitirnos saltarnos esta facilidad de seguridad accediento al documento de seguridad mixta a través del protocolo no seguro http en lugar de con el protocolo https. Los aspectos de seguridad de SSL nos protegen de transmisiones inseguras, pero no limita la capacidad de recibir transmisiones inseguras.

Los formularios en línea pueden 'asegurarse' si la acción de submitirlos es un URL https:// hacia un servidor seguro. Netscape utiliza las cajas de dialogo para informarnos acerca del status de seguridad del proceso de submision al submitir un formulario.

Se puede salvar un documento seguro (los documentos seguros no son cacheados a disco durante la sesión). También puede verse el HTML fuente de un documento seguro. La seguridad afecta a la transmisión de un documento sin afectar la capacidad de manipularlo.

Seguridad en los servidores

Los sistemas seguros de correo electrónico y servidores web emplean protocolos especiales que hacen uso de algoritmos de cifrado de clave pública, lo que da lugar a la firma electrónica y a que se satisfagan las funciones de seguridad de Confidencialidad, Integridad, Autenticación de Origen, Irrefutabilidad de Origen, Autenticación de Destino, Irrefutabilidad de Recepción, Temporalidad, Acreditación y otras.

De forma sencilla, la Entidad de Certificación es un servidor de credenciales, que garantiza que cada usuario es quien dice ser, y que pueden utilizarse sin restricciones elementos criptográficos que garantizan la confidencialidad.

Algunos de los protocolos utilizados son SSL (Secure Sockets Layer), PEM (Private Enhanced Mail) y S/MIME (Secure/Multipurpose Internet Mail Extensión), ya soportados por

un buen número de programas visualizadores y de programas de correo. Para el buen funcionamiento de estos sistemas, es necesario contar con un procedimiento que permita verificar fehacientemente la identidad de los usuarios y de otorgar un certificado electrónico que vincula los datos de los usuarios con su clave pública.

En el caso de FESTE, son los Corredores de Comercio y los Notarios los encargados de verificar la identidad de las Entidades en las que se instalan los equipos (en el caso de los servidores), o de las personas que intercambian correo seguro (en el so de browsers , o programas de correo)

Cuando un participante comunica a otro su certificado, indica la Entidad de Certificación utilizada. La llave pública de la Entidad de Certificación debe ser conocida por todos y es la única que necesita ser conocida previamente. Habitualmente está incorporada al software de realización y verificación de firmas electrónicas, o es posible obtenerla a partir de sistemas de difusión públicos, tales como servidores Web. En el caso de FESTE, la clave pública de la Entidad de Certificación para certificados "Nivel 2" de "Entidades Cualificadas" se puede obtener en la dirección www.FESTE.com/cacert/certwebcualif.nivel2/FESTE-qicl2.der.cacert

La Entidad de Certificación debe ser una Entidad de Confianza (Trusted Third Party), Conocida ampliamente, cuya Política de Certificación incluya cláusulas aceptables por los diferentes interlocutores, que permita, entre otras cosas, la Verificación de identidad, que dé información sobre Uso y validez de los certificados y que realice Gestión de certificados revocados (para impedir que claves privadas expuestas puedan tener vigencia) y ofrezca la Lista de certificados expedidos

Dado que en una red existe más de una Entidad de Certificación, la selección de las autoridades de certificación adecuadas para cada uso vendrá dada por las características de su Política de Certificación, o por el reconocimiento de alguna de ellas por parte de entidades que aceptan sus certificados. Se están desarrollando sistemas jerárquicos en los cuales todas las autoridades de certificación que pertenezcan a una jerarquía dada puedan realizar certificaciones mutuas.

Los parámetros que definen a una Entidad de Certificación son su dirección de red (nombre distinguido, por ejemplo www.FESTE.com) y su clave pública. Además, es necesario especificar en su identificación: Entidad Emisora del Certificado, Departamento u Organización responsable de la custodia de la clave privada y Ubicación (Ciudad, País).

Entidad de Registro

Puesto que al realizar la comprobación de la identidad del usuario en la primera certificación es necesario realizar unas actividades especiales, la Entidad de Certificaci&oa cute;n lleva asociada una Entidad de Registro.

Esta Entidad de Registro mantiene información sobre los aspectos relevantes del registro y sobre los procedimientos de identificación utilizados, así como la vinculación del registro con la identidad que garantiza la Entidad de Certificación.

Además de este tipo de Entidades de Registro, existen otras, que demuestran la realización en el tiempo de determinados Actos Electrónicos: Certificaciones en presencia de un fedatario (como en el caso de contratos firmados ante notario), Certificaciones de Acreditación respecto a la capacidad suficiente para obrar o para representar a terceros, Registro de contratos o transmisiones patrimoniales.

Algunas de estas entidades tienen actividades independientes y adicionales a las de las autoridades de certificación, que se centran en la Autenticación de los Intervinientes y las funciones derivadas.

FESTE distingue dos tipos de Entidades de Registro: Entidades con capacidad contrastada de verificación de identidad de sus propios clientes o empleados (entidades financieras, proveedores de Internet, …), con capacidad de activar la emisión de certificados de Nivel 1 (Certificados Registrados), o Fedatarios, con la misión de verificar de forma incuestionable la identidad y capacidad de actuar de cualquier solicitante, y con capacidad de activar la emisión de certificados de Nivel 2 (Certificados Autenticados). Existen también los certificados de Nivel 0, destinados a pruebas.

Instalación de los Certificados

Una vez que se ha decidido activar el modo seguro de los servidores web, es preciso generar la pareja de claves que constituye el componente criptográfico básico del protocolo SSL, basado en criptografía de clave pública.

El procedimiento consiste básicamente en tres pasos:

•Generación de la solicitud,

•Acreditación ante la Entidad de Registro

•Obtención del Certificado e instalación

Para generar la solicitud, debe ejecutarse la opción correspondiente del software servidor (algunos de los que disponen modo seguro son FasTrack de Netscape, Internet Information Server de Microsoft, Secure Server de Oracle, o el popular Apache el más instalado sobre plataformas Linux), el cual influirá en los pasos concretos a seguir.

Estos pasos deben permitir generar las claves criptográficas, rellenar un formulario con los datos que formarán parte del certificado, obtener la solicitud en un formato compatible (DER o PEM) y enviarlo por correo electrónico a la Entidad de Certificación.

En algunos casos, como por ejemplo, con Microsoft Internet Information Server, es preciso obtener previamente el certificado de la Entidad de Certificación (en formato DER), lo que debe llevarse a cabo mediante Microsoft Internet Explorer, puesto que comparten la estructura de datos de almacenamiento de certificados. Existe una pequeña diferencia en caso de utilizar IIS 4.0, ya que para activar los Certificados del Explorer en el Server, existe una utilidad denominada IISCA en el directorio win\System32\InetSrv.

Tras enviar la solicitud de certificado a la Entidad de Certificación, debe procederse al registro. El Registro consiste en verificar la identidad del solicitante, comprobando la a decuada cumplimentación de los datos del formulario. En el caso de FESTE, la Entidad de Registro puede ser cualquiera de los Notarios o Corredores de Comercio españoles, lo que proporciona un elevado nivel de reconocimiento.

Cuando la Entidad de Registro comprueba los datos, permite que la Entidad de Certificación genere el certificado y lo envíe por correo electrónico. En ocasiones, la Entidad de Certificación proporciona un enlace al URL en el que se ha depositado, permitiendo la comunicación de información complementaria. Una vez en posesión del certificado, puede instalarse en el servidor, con lo queda listo para establecer comunicaciones seguras.

Certificados de Cliente

Si los requerimientos de seguridad exigen la autenticación del usuario (a través del Explorer o el Navigator), es preciso instalar certificados personales para cada uno de l usuarios que sea preciso autenticar.

Los pasos a seguir son, en esencia, los mismos que en el caso de servidores, aunque se activan de forma un poco diferente a la de aquellos. Habitualmente los servidores web de la Entidad de Certificación describen el proceso e incluyen las explicaciones y el software necesario para activar la generación de claves en el browser. En el caso de Explorer, se encargan de cargar las DLL correspondientes (CERTENR3.DLL en la versión 3.0 de MSIE y XENROLL.DLL en el IE 4.0) que hacen un poco más complicado el proceso de solicitud de certificado.

Una vez generada, sobre el web, la solicitud de certificado, hay que acudir a la Entidad de Registro (Corredor de Comercio o Notario) para que compruebe la veracidad de los datos y autorice la generación de certificado.

La Entidad de Certificación enviará un correo electrónico indicando la disponibilidad del certificado que podrá obtenerse a través del propio servidor web.

La ventaja de los certificados de cliente es que pueden ser utilizados tanto para autenticación de usuarios, cuando están accediendo a un servidor web, como para cifrar y firmar correo electrónico, apoyados en la codificación S/MIME (extensiones de seguridad de Correo Elecrón

Por último, para que las comunicaciones viajen protegidas por algoritmos criptográficos, es preciso instalar software servidor equipado con SSL, y preparar los Certificados que lo habilitan con una Entidad de Certificación adecuada.

3.2 Debilidades de los protocolos TCP/IP.

El modelo TCP/IP es un modelo de descripción de protocolos de red desarrollado en los años 70

El modelo TCP/IP, describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

VENTAJAS

- El conjunto TCP/IP está diseñado para enrutar
- Tiene un grado muy elevado de fiabilidad.
- Es adecuado para redes grandes y medianas, así como redes empresariales.
- Es compatible con las herramientas estándar para analizar el funcionamiento de la red.
- proporciona abstracción de capas.
- Puede funcionar en máquinas de todo tamaño (multiplataforma)
- Soporta múltiples tecnologías
- Imprescindible para Internet

DESVENTAJAS

- El modelo no distingue bien entre servicios, interfaces y protocolos, lo cual afecta al diseño de nuevas tecnologías en base a TCP/IP.
- Es más difícil de configurar y mantener a pesar de tener menos capas.
- Es algo más lento en redes con un volumen de tráfico medio bajo, puede ser más rápido en redes con un volumen de tráfico grande donde haya que enrutar un gran número de tramas.
- Peor rendimiento para uso en servidores de fichero e impresión

3.3 Transmisión de paquetes y promiscuidad.

En las redes de ordenadores, la información se transmite en una serie de paquetes con la dirección física (o dirección MAC) de quien lo envía y quien lo tiene que recibir, de manera que cuando transmitimos un fichero, éste se divide en varios paquetes con un tamaño predeterminado y el receptor es el único que captura los paquetes evaluando si llevan su dirección.

En el modo promiscuo, una máquina intermedia captura todos los paquetes, que normalmente desecharía, incluyendo los paquetes destinados a él mismo y al resto de las máquinas. Resulta a destacar que las topologías y hardware que se usen para comunicar las redes, influye en su funcionamiento, ya que las redes en bus, redes en anillo, así como todas las redes que obliguen a que un paquete circule por un medio compartido, al cual todos tienen acceso, los modos promiscuos capturarán muchos más paquetes que si están en una red con topología en árbol. Para completar el modo, las máquinas en modo promiscuo

suelen simplemente copiar el paquete y luego volverlo a poner en la red para que llegue a su destinatario real (en el caso de topologías que requieran de retransmisión).

Paquete

Se le llama paquete de red o paquete de datos a cada uno de los bloques en que se divide, en el nivel de Red, la información a enviar. Por debajo del nivel de red se habla de trama de red, aunque el concepto es análogo.

En todo sistema de comunicaciones resulta interesante dividir la información a enviar en bloques de un tamaño máximo conocido. Esto simplifica el control de la comunicación, las comprobaciones de errores, la gestión de los equipos de encaminamiento (routers), etc.

Datagrama

Un datagrama es un fragmento de paquete (análogo a un telegrama) que es enviado con la suficiente información para que la red pueda simplemente encaminar el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ETD destino.

Los datagramas también son la agrupación lógica de información que se envía como una unidad de capa de red a través de un medio de transmisión sin establecer con anterioridad un circuito virtual.

Tiempo de bit

Para cada velocidad de medios diferente se requiere un período de tiempo determinado para que un bit pueda colocarse y detectarse en el medio. Dicho período de tiempo se denomina tiempo de bit.

Mac Addres

La dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo.

Tipos de IP

Clase A

En esta clase se reserva el primer grupo a la identificación de la red, quedando los tres siguientes para identificar los diferentes hosts. Los rangos de esta clase están comprendidos entre 1.0.0.0 y 127.255.255.255. Actualmente la ICANN asigna redes de este grupo a gobiernos de todo el mundo, aunque hay algunas grandes empresas que tienen asignadas IP's de esta clase.

Clase B

En esta clase se reservan los dos primeros grupos a la identificación de la red, quedando los dos siguientes para identificar los diferentes host. Los rangos de esta clase están comprendidos entre 128.0.0.0 y 191.255.255.255. Actualmente la ICANN asigna redes de este grupo a grandes y medianas empresas.

Clase C

En esta clase se reservan los tres primeros grupos a la identificación de la red, quedando el último para identificar los diferentes hosts. Los rangos de esta clase están comprendidos entre 192.0.0.0 y 223.255.255.255. Actualmente la ICANN asigna redes de este grupo a aquellos que lo solicitan

3.4 Redes locales (VLAN) y amplias (VPN)

Una VLAN (acrónimo de Virtual LAN) es una subred IP separada de manera lógica, las VLAN permiten que redes IP y subredes múltiples existan en la misma red conmutada, son útiles para reducir el tamaño del broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos para una empresa, oficina, universidades, etc.) que no deberían intercambiar datos usando la red local.

CARACTERISTICAS DE UNA VLAN:

La característica principal de una red de área local es que los dispositivos que la conforman

comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo.

Cuando utilizamos un concentrador o hub dentro de una red, ésta se puede ver como una red de distribución hidráulica, donde las estaciones de trabajo conectadas a la misma toman cierta

cantidad de agua, y mientras más máquinas existan en esa LAN, menor será la cantidad de líquido que podrán utilizar. A este segmento de "tubería" se le puede llamar también "dominio de colisiones".

¿COMO SE CONFIGURA UNA VLAN?

Ciscoredes# configure terminal
Ciscoredes(config)# vlan vlan-id
Ciscoredes(config-vlan)# name nombre-de-vlan
Ciscoredes(config-vlan)# exit

- Vlan .- comando para asignar las VLAN
- Valn-id.- Numero de vlan que se creará que va de un rango normal de 1-1005 (los ID 1002-1005 se reservan para Token Ring y FDDI).

· Name.- comando para especificar el nombre de la VLAN

· Nombre-de-vlan.- Nombre asignado a la VLAN, sino se asigna ningún nombre, dicho nombre será rellenado con ceros, por ejemplo para la VLAN 20 sería VLAN0020.

Asignar puertos a la VLAN

Ciscoredes# configure terminal
Ciscoredes(config)# interface interface-id
Ciscoredes(config-vlan)# switchport mode access
Ciscoredes(config-vlan)# switchport access vlan vlan-id
Ciscoredes(config-vlan)# end

Donde:

- interface .- Comando para entrar al modo de configuración de interfaz.
- Interface-id.- Tipo de puerto a configurar por ejemplo fastethernet 0/0
- Switchport mode access .- Define el modo de asociación de la VLAN para el puerto
- Switchport access vlan .- Comandos para asignar un puerto a la vlan.
- Vlan-id.- Numero de vlan a la cual se asignará el puerto.

VPN

¿QUE SON LAS VPN?

VPN o "Virtual Private Network" es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

El ejemplo más común es la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet; también permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputos, o que un usuario pueda acceder a su equipo hogareño desde un sitio remoto, como por ejemplo un hotel. Todo esto utilizando la infraestructura de Internet.

Para hacerlo posible de manera segura es necesario proveer los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación.

- Autenticación y Autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: La garantía de que los datos enviados no han sido alterados.
- Confidencialidad: Dado que los datos viajan a través de un medio hostil como Internet, los mismos son susceptibles de interceptación: por eso es fundamental el cifrado de los datos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma.

CARACTERISTICAS DE LA VPN:

Una VPN proporciona conectividad en distancias potencialmente grandes. En este aspecto, VPN es una forma de red WAN. Las VPN permiten compartir archivos, video conferencias y servicios de red similares. Las VPN generalmente no proporcionan ninguna funcionalidad que no sea ya ofrecida por otras alternativas, pero una VPN implementa esos servicios con mayor eficiencia y economía en la mayoría de los casos...

Una característica importante de una VPN es su capacidad de trabajar tanto sobre redes privadas como en públicas como la Internet. Utilizando un método llamado "tunneling", una VPN puede usar la misma infraestructura de hardware de las conexiones de Internet o Intranets existentes. Las tecnologías VPN incluyen varios mecanismos de seguridad para proteger las conexiones virtuales privadas.

¿COMO SE CONFIGURA UNA VPN?

Explicaremos el procedimiento para configurar una VPN en Windows (R) XP, tanto en modo cliente como en modo servidor.

VPN (Virtual Private Network) significa literalmente Red Privada Virtual. Básicamente consiste en realizar una conexión a una red externa creando un túnel a través de internet, permitiendo la creación de una red privada dentro de una red pública.

A continuación, reproducimos parte de la explicación contenida en la ayuda de windows xp sobre VPN, por ser bastante ilustrativa:

La VPN utiliza el Protocolo de túnel punto a punto (PPTP, *Point-to-Point Tunneling Protocol*) o el Protocolo de túnel de nivel dos (L2TP,*Layer Two Tunneling Protocol*), mediante los cuales se puede tener acceso de forma segura a los recursos de una red al conectar con un servidor de acceso remoto a través de Internet u otra red. El uso de redes privadas y públicas para crear una conexión de red se denomina red privada virtual, *Virtual Private Network*).

Un usuario que ya está conectado a Internet utiliza una conexión VPN para marcar el número del servidor de acceso remoto. Entre los ejemplos de este tipo de usuarios se incluyen las personas cuyos equipos están conectados a una red de área local, los usuarios de cables de conexión directa o los suscriptores de servicios como ADSL, en los que la conectividad IP se establece inmediatamente después de que el usuario inicie el equipo. El controlador PPTP o L2TP establece un túnel a través de Internet y conecta con el servidor de acceso remoto habilitado para PPTP o L2TP. Después de la autenticación, el usuario puede tener acceso a la red corporativa con total funcionalidad.

3.5 Domicilios IP.

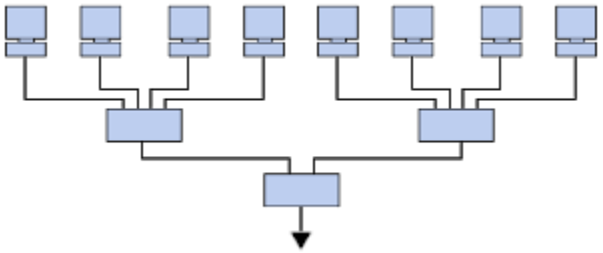
Los equipos comunican a través de Internet mediante el protocolo IP (Protocolo de Internet). Este protocolo utiliza direcciones numéricas denominadas direcciones IP compuestas por cuatro números enteros (4 bytes) entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo, 194.153.205.26es una dirección IP en formato técnico.

Los equipos de una red utilizan estas direcciones para comunicarse, de manera que cada equipo de la red tiene una dirección IP exclusiva.
El organismo a cargo de asignar direcciones públicas de IP, es decir, direcciones IP para los equipos conectados directamente a la red pública de Internet, es el ICANN (Internet Corporation for Assigned Names and Numbers) que remplaza el IANA desde 1998 (Internet Assigned Numbers Agency).

Cómo descifrar una dirección IP

Una dirección IP es una dirección de 32 bits, escrita generalmente con el formato de 4 números enteros separados por puntos. Una dirección IP tiene dos partes diferenciadas:
los números de la izquierda indican la red y se les denomina netID (identificador de red).
los números de la derecha indican los equipos dentro de esta red y se les denomina host ID(identificador de host).

Veamos el siguiente ejemplo:



Observe la red, a la izquierda 194.28.12.0. Contiene los siguientes equipos:

· 194.28.12.1 a 194.28.12.4

Observe la red de la derecha 178.12.0.0. Incluye los siguientes equipos:

· 178.12.77.1 a 178.12.77.6

En el caso anterior, las redes se escriben 194.28.12 y 178.12.77, y cada equipo dentro de la red se numera de forma incremental.

Tomemos una red escrita 58.0.0.0. Los equipos de esta red podrían tener direcciones IP que van desde58.0.0.1 a 58.255.255.254. Por lo tanto, se trata de asignar los números de forma que haya una estructura en la jerarquía de los equipos y los servidores.

Cuanto menor sea el número de bits reservados en la red, mayor será el número de equipos que puede contener.

De hecho, una red escrita 102.0.0.0 puede contener equipos cuyas direcciones IP varían entre 102.0.0.1 y 102.255.255.254 (256*256*256-2=16.777.214 posibilidades), mientras que una red escrita 194.24 puede contener solamente equipos con direcciones IP entre 194.26.0.1 y 194.26.255.254 (256*256-2=65.534 posibilidades); ésta es el concepto de clases de direcciones IP.

Direcciones especiales

Cuando se cancela el identificador de host, es decir, cuando los bits reservados para los equipos de la red se reemplazan por ceros (por ejemplo, 194.28.12.0), se obtiene lo que se llama dirección de red. Esta dirección no se puede asignar a ninguno de los equipos de la red.

Cuando se cancela el identificador de red, es decir, cuando los bits reservados para la red se reemplazan por ceros, se obtiene una dirección del equipo. Esta dirección representa el equipo especificado por el identificador de host y que se encuentra en la red actual.

Cuando todos los bits del identificador de host están en 1, la dirección que se obtiene es la denominada dirección de difusión. Es una dirección específica que permite enviar un mensaje a todos los equipos de la red especificados por el netID.

A la inversa, cuando todos los bits del identificador de red están en 1, la dirección que se obtiene se denomina dirección de multidifusión.

Por último, la dirección 127.0.0.1 se denomina dirección de bucle de retorno porque indica el host local.

Direcciones IP reservadas

Es habitual que en una empresa u organización un solo equipo tenga conexión a Internet y los otros equipos de la red acceden a Internet a través de aquél (por lo general, nos referimos a un proxy o pasarela).

En ese caso, solo el equipo conectado a la red necesita reservar una dirección de IP con el ICANN. Sin embargo, los otros equipos necesitarán una dirección IP para comunicarse entre ellos.

Por lo tanto, el ICANN ha reservado una cantidad de direcciones de cada clase para habilitar la asignación de direcciones IP a los equipos de una red local conectada a Internet, sin riesgo de crear conflictos de direcciones IP en la red de redes. Estas direcciones son las siguientes:

· Direcciones IP privadas de clase A: 10.0.0.1 a 10.255.255.254; hacen posible la creación de grandes redes privadas que incluyen miles de equipos.

· Direcciones IP privadas de clase B: 172.16.0.1 a 172.31.255.254; hacen posible la creación de redes privadas de tamaño medio.

· Direcciones IP privadas de clase C: 192.168.0.1 a 192.168.0.254; para establecer pequeñas redes privadas.

3.6 Vigilancia de paquetes

Ya hemos visto que la vigilancia en el trabajo por medio de nuestro ordenador es posible, y hay varias formas de hacerlo. De las varias maneras que se puede hacer, puede que una de las más populares sea con un sniffer de red. Los administradores de red han estado usando sniffer de red durante años para monitorizar sus redes y realizar diagnósticos y pruebas para detectar problemas en la red. Básicamente, un sniffer de red es un programa que puede ver toda la información pasando por una red a la cual está conectado. Según los flujos de datos van y vienen por la red, el programa hace una vigilancia de ello, o "captura" los paquetes que atraviesan los dispositivos de red. Como ya hemos comentado en otros artículos, un paquete es una parte de un mensaje que ha sido partido para poder ir de un sitio a otro. Normalmente, un ordenador solo hace caso de paquetes con direcciones destinadas a él, e ignora el resto del tráfico de la red.

Sin embargo, cuando un sniffer de red es configurado en un equipo u ordenador, el interfaz de red es puesto en modo promiscuo para el sniffer. Esto significa que está vigilando todo lo que atraviesa ese interfaz. La cantidad de tráfico depende mucho en la localización delordenador en la red. Un sistema cliente en una parte aislada de la red, solo ver un pequeño segmento del tráfico de red, mientras que el servidor de dominio principal ve prácticamente todo. Un sniffer de red puede ser configurado en dos modos: Filtrado (captura todos los paquetes) y no filtrado (captura solo aquellos paquetes contendiendo elementos de datos específicos). Los paquetes que contienen datos que se filtran, son copiados al disco duro según pasan. Estas copias pueden ser analizadas con tranquilidad después para encontrar una información específica.

Cuando te conectas a Internet, te estás uniendo a una red mantenida por un proveedor de servicios de Internet o ISP. La red de este proveedor comunica con redes mantenidas por otras ISPs para formar la estructura de la red. Un sniffer de red localizado en uno de los servidores de tu ISP podría potencialmente ser capaz de monitorizar todas las actividades online, que podrían ser las páginas Web que se visitan, que es lo que se busca en un sitio concreto, a quién se envían email, que contienen el email, lo que nos descargamos, con servicios se utilizan, y muchas cosas más. De esta información, una compañía puede determinar cuánto tiempo un empleado está online haciendo cosas que no tienen nada que

ver con el trabajo que desarrolla. Los sniffer de red son solo una de las herramientas utilizadas para monitorizar la actividad de los ordenadores de empresa.

El software de monitorización de ordenador trabaja de forma diferente que un sniffer de red. Lo que hacen realmente es seguir cada acción que se hace en un ordenador. Cada vez que se realiza una actividad por pequeña que sea en el ordenador, ya sea teclear una palabra en el teclado o abrir una nueva aplicación, se transmite una señal. Estas señales pueden ser interceptadas por el programa de monitorización, el cual puede ser instalado en el ordenador a un nivel de sistema operativo. La persona que recibe las señales interceptadas puede ver cada uno de los caracteres interceptados y puede replicar lo que el usuario está viendo en su monitor. Estos programas pueden ser instalados de dos maneras:

Físicamente – Alguien se siente en el ordenador e instala el software.
Remotamente – Un usuario abre un archivo añadido a un correo o enviado de otro modo.

El archivo, el cual contiene un programa que el usuario quiere instalar, puede contener también el programa de monitorización. Esto es llamado troyano – un programa deseado y contiene un programa no deseado.

Los programas de monitorización tienen la habilidad de registrar cada tecla que pulsamos. Cuando estás tecleando, una señal es enviada del teclado a la aplicación con la que estás trabajando. Esta señal puede ser interceptada y reenviada a la persona que instaló el programa de monitorización o registrarlo en un fichero de texto y enviarlo después. Esta información puede ser enviada a un administrador de red, pero también es un método popular entre piratas informáticos. Normalmente los hackers usan este tipo de programas para obtener contraseñas, y al registrar todo lo que se teclea, puede ser peligroso para el usuario ya que intercepta números de tarjeta y otra información privada.

Los programas de monitorización pueden leer correos y ver cualquier programa que esté abierto en la pantalla. Captura la imagen en la pantalla del ordenador al interceptar señales que están siendo transmitidas a la tarjeta de video del ordenador. Estas imágenes son luego enviadas por la red al administrador de red. Algunos de estos programas tienen incluso

sistemas de alerta – cuando un usuario visita un sitio Web específico o escribe un correo con texto inapropiado, el administrador es avisado de estas acciones. Sin embargo, no es necesario tampoco instalar un software como este para hacer un seguimiento del usuario. Hay un sistema ya instalado en el ordenador que dice lo que ha estado haciendo el usuario.

Tu ordenador está lleno de registros o logs que proveen de evidencias de lo que has estado haciendo. A través de estos registros, un administrado de red puede determinar que sitios Web se han visitado., a quién se han enviado emails o de quién se ha recibido. Por lo tanto, si te descargas archivos de música MP3, hay muchas probabilidades de que haya un registro que muestre esta actividad. En muchos casos, esta información puede ser localizada incluso después de haber borrado lo que crees que son las evidencias – borrar un correo o un archivo no borra las pruebas. Hay algunos sitios donde se puede encontrar estos registros:

En el propio sistema operativo.
En los navegadores de Internet.
En las propias aplicaciones que usamos.
En los registros de los programas de correos.

Si el disco duro de un empleado de una compañía y el ordenador de un administrado r de red están conectados, este último puede ver los logs remotamente. Lo único que tiene que hacer es acceder al disco duro remotamente y verificar los registros. Si el ordenador no se apaga, lo puede hacer antes de que el empleado llegue por la mañana y se vaya por la tarde.

3.7 Estándares para la seguridad en redes.

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad.

Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

Dentro de este conjunto están:

Norma	Descripción
ISO/IEC 27000	Vocabulario estándar para el SGSI para todas las normas de la familia.. Se encuentra en desarrollo actualmente.
ISO/IEC 27001	Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.

ISO/IEC 27002	*Information technology - Security techniques - Code of practice for information security management.* Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un **código de buenas prácticas** para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.
ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standar BS 7799 parte 3. Publicada en junio de 2008.
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC 27007	Guía para auditar al SGSI. Se encuentra en preparación.
ISO/IEC 27799:2008	Guía para implementar ISO/IEC 27002 en la industria de la salud.

3.8 Vulnerabilidad de los protocolos inalámbricos WEP, WPA, WPA2.

Los algoritmos de seguridad WiFi han pasado por muchos cambios y mejoras desde los años 90 para hacerse más seguros y eficaces. Se desarrollaron diferentes tipos de protocolos de seguridad inalámbricos para la protección de redes inalámbricas domésticas. Los protocolos de seguridad inalámbrica son WEP, WPA y WPA2, que cumplen el mismo propósito pero que son diferentes al mismo tiempo. No sólo los protocolos evitan que las partes no deseadas se conecten a su red inalámbrica, sino que también los protocolos de seguridad inalámbrica cifran sus datos privados enviados a través de las ondas.

No importa lo protegido y cifrado, las redes inalámbricas no pueden mantenerse en seguridad con redes cableadas. Estos últimos, en su nivel más básico, transmiten datos entre dos puntos, A y B, conectados por un cable de red. Para enviar datos de A a B, las redes inalámbricas lo transmiten dentro de su alcance en todas las direcciones a cada dispositivo conectado que esté escuchando.

Privacidad Equivalente al Cableado (WEP)

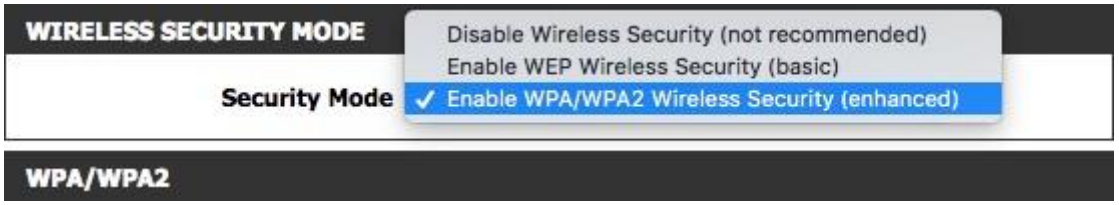
WEP fue desarrollado para redes inalámbricas y aprobado como estándar de seguridad Wi-Fi en septiembre de 1999. WEP tenía como objetivo ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo, hay un montón de problemas de seguridad bien conocidos en WEP, que también es fácil de romper y difícil de configurar.

A pesar de todo el trabajo que se ha hecho para mejorar el sistema, WEP sigue siendo una solución altamente vulnerable. Los sistemas que dependen de este protocolo deben ser

actualizados o reemplazados en caso de que la actualización de seguridad no sea posible. WEP fue oficialmente abandonada por la Alianza Wi-Fi en 2004.

Acceso protegido Wi-Fi (WPA)

Durante el tiempo en que el estándar de seguridad inalámbrica 802.11i estaba en desarrollo, WPA se utilizó como una mejora de seguridad temporal para WEP. Un año antes de que WEP fuera oficialmente abandonado, WPA fue formalmente adoptado. La mayoría de las aplicaciones WPA modernas usan una clave previamente compartida (PSK), más a menudo conocida como WPA Personal, y el Protocolo de Integridad de Clave Temporal o TKIP (/ tiːkɪp /) para encriptación. WPA Enterprise utiliza un servidor de autenticación para la generación de claves y certificados.



WPA era una mejora significativa sobre WEP, pero como los componentes principales se hicieron para que pudieran ser lanzados a través de actualizaciones de firmware en dispositivos con WEP, todavía dependían de elementos explotados.

WPA, al igual que WEP, después de ser puesto a prueba de concepto y las demostraciones públicas aplicadas resultó ser bastante vulnerable a la intrusión. Sin embargo, los ataques que representaron la mayor amenaza para el protocolo no fueron los directos, sino los que se hicieron en Configuración de Wi-Fi Segura (WPS) - Sistema auxiliar desarrollado para simplificar la vinculación de dispositivos a puntos de acceso modernos.

Wi-Fi Protected Access versión 2 (WPA2)

El protocolo basado en estándares de seguridad inalámbrica 802.11i fue introducido en 2004. La mejoría más importante de WPA2 sobre WPA fue el uso del Estándar de cifrado avanzado (AES) para el cifrado. AES es aprobado por el gobierno de EE.UU. para cifrar la información clasificada como de alto secreto, por lo que debe ser lo suficientemente bueno para proteger las redes domésticas.

En este momento, la principal vulnerabilidad a un sistema WPA2 es cuando el atacante ya tiene acceso a una red WiFi segura y puede acceder a ciertas teclas para realizar un ataque a otros dispositivos de la red. Dicho esto, las sugerencias de seguridad para las vulnerabilidades WPA2 conocidas son principalmente importantes para las redes de niveles de empresa, y no es realmente relevante para las pequeñas redes domésticas.

Lamentablemente, la posibilidad de ataques a través de Configuración de Wi-Fi Segura(WPS), sigue siendo alta en los actuales puntos de acceso capaces de WPA2, que es el problema con WPA también. Y aunque forzar el acceso en una red asegurada WPA / WPA2 a través de este agujero tomará alrededor de 2 a 14 horas sigue siendo un problema de seguridad real y WPS se debe inhabilitar y sería bueno si el firmware del punto de acceso pudo ser reajustado a una distribución para no apoyar WPS, para excluir por completo este tipo de ataque.

Qué método de seguridad funcionará para su red

Aquí está la calificación básica de mejor a peor de los modernos métodos de seguridad WiFi disponibles en modernos (después de 2006) routers:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP Existe como un método alternativo)

4. WPA + TKIP
5. WEP
6. Red abierta (sin seguridad en absoluto)

La mejor manera de hacerlo es desactivar Configuración de Wi-Fi Segura (WPS) y configurar el router a WPA2 + AES. Y a medida que avanza por la lista, lo menos seguro será su red.

Propósito

Si deja su router sin seguridad, cualquiera puede robar el ancho de banda, realizar acciones ilegales en su conexión y nombre, supervisar su actividad web e instalar fácilmente aplicaciones malintencionadas en su red. Se supone que tanto WPA como WPA2 protegen las redes inalámbricas de acceso no autorizado.

WPA contra WPA2

Los router Wi-Fi admiten una variedad de protocolos de seguridad para asegurar redes inalámbricas: WEP, WPA y WPA2. Sin embargo, WPA2 se recomienda sobre su predecesor WPA (Acceso protegido Wi-Fi).

Probablemente el único inconveniente de WPA2 es cuánta potencia de procesamiento se necesita para proteger su red. Esto significa que se necesita hardware más potente para no experimentar un menor rendimiento de la red. Este problema se refiere a los puntos de acceso más antiguos que se implementaron antes de WPA2 y sólo admiten WPA2 a través de una actualización de firmware. La mayoría de los puntos de acceso actuales se han suministrado con hardware más capaz.

Definitivamente use WPA2 si puede y sólo use WPA si no hay manera de que su punto de acceso soporte WPA2. El uso de WPA también es una posibilidad cuando su punto de acceso experimenta regularmente altas cargas y la velocidad de la red sufre del uso de WPA2. Cuando la seguridad es la principal prioridad, entonces el retroceso no es una opción, sino que uno debería considerar seriamente la posibilidad de obtener mejores puntos de acceso. WEP tiene que ser usado si no hay posibilidad de usar cualquiera de los estándares WPA.

Velocidad de cifrado

Dependiendo de qué protocolos de seguridad utilice, la velocidad de datos puede verse afectada. WPA2 es el más rápido de los protocolos de cifrado, mientras que WEP es el más lento.

Proteja su red WiFi

Aunque WPA2 es mucho más seguro que WPA y por lo tanto mucho más seguro que WEP, la seguridad de su router depende en gran medida de la contraseña que haya establecido. WPA y WPA2 le permiten usar contraseñas de hasta 63 caracteres.

Utilice tantos varios caracteres en su contraseña de la red WiFi como sea posible. Los hackers están interesados en objetivos más fáciles, si no pueden romper su contraseña en varios minutos, lo más probable es que pasen a buscar redes más vulnerables. Resumen:

1. WPA2 es la versión mejorada de WPA;
2. WPA sólo admite cifrado TKIP mientras WPA2 admite AES;
3. TTeóricamente, WPA2 no es hackable mientras WPA sí lo es;
4. WPA2 necesita más potencia de procesamiento que WPA;

5. ¡Use NetSpot para comprobar su cifrado!

3.9 Firewall de capas inferiores.

Estos niveles se encargan de gestionar el apartado físico de la conexión, como el establecimiento de la comunicación, el enrutamiento de ésta y el envío

- **Capa 1: Física**

  Este nivel se encarga directamente de los elementos físicos de la conexión. Gestiona los procedimientos a nivel electrónico para que la cadena de bits de información viaje desde el transmisor al receptor sin alteración alguna. Define el medio físico de transmisión: cables de pares trenzados, cable coaxial, ondas y fibra óptica

- **Capa 2: Enlace de datos**

  Este nivel se encarga de proporcionar los medios funcionales para establecer la comunicación de los elementos físicos. Los elementos típicos que todos conocemos para servir de ejemplo a esta capa son el switch o también el router de red.

- **Capa 3: Red**

  Esta capa se encarga de la identificación del enrutamiento entre dos o más redes conectadas. Este nivel hará que los datos puedan llegar desde el transmisor al receptor siendo capaz de hacer las conmutaciones y encaminamientos necesarios para que el mensaje llegue. El protocolo más conocido que se encarga de esto es el IP.

- **Capa 4: Transporte**

  Este nivel se encarga de realizar el transporte de los datos que se encuentran dentro

del paquete de transmisión desde el origen al destino. Esto se realiza de forma independiente al tipo de red que haya detectado el nivel inferior. Los protocolos más conocidos son UDP y TCP.

3.10 Firewall de capa de aplicación.

En el segundo grupo están los niveles que trabajan directamente de cara a aplicaciones que solicitan servicios de los niveles inferiores. Adecuan la información modelándola para que sea entendible desde el punto de vista del usuario.

- **Capa 5: Sesión**

  Mediante este nivel se podrá controlar y mantener activo el enlace entre las máquinas que están transmitiendo información. De esta forma se asegurará que una vez establecida la conexión, esta e mantengas hasta que finalice la transmisión.

- **Capa 6: Presentación**

  Como su propio nombre intuye, esta capa se encarga de la representación de la información transmitida. Asegurará que los datos que nos llegan a los usuarios sean entendibles a pesar de los distintos protocolos utilizados tanto en un receptor como en un transmisor. Traducen una cadena de caracteres en algo entendible, por así decirlo.

- **Capa 7: Aplicación**

  Este es el último nivel, y en encargado de permitir a los usuarios ejecutar acciones y comandos en sus propias aplicaciones como por ejemplo un botón para enviar un email o un programa para enviar archivos mediante FTP. Permite también la

comunicación entre el resto de capas inferiores. Ejemplos de la capa de aplicación pueden ser el protocolo SMTP, FTP, etc.

3.11 Firewall personal.

Los firewalls son programas de software especiales diseñados para mantener a los intrusos fuera de la red. Estos programas se ejecutan en hardware de computadora y pueden diseñarse para evitar los hackers informáticos. Un firewall personal es uno que se administra y controla a nivel de escritorio de la computadora. Normalmente se incluye en la mayoría de los paquetes de software antivirus.

Es fácil configurar un firewall personal. Este software permite el filtrado de mensajes entrantes y salientes en una red informática. El firewall puede deshabilitar puertos específicos en el sistema informático, que los piratas informáticos suelen utilizar como método de infiltración en una red.

El sistema operativo Windows® generalmente se vende con software de firewall personal incluido. Si se desea otro software de firewall, el software de Windows® debe deshabilitarse. No se recomienda ejecutar dos programas de software de firewall simultáneamente porque la protección puede volverse poco confiable.

Hay muchos tipos de software de firewall personal disponibles. Estos incluyen productos comerciales y productos de código abierto de descarga gratuita. Al seleccionar el software de firewall, es importante elegir un producto de un proveedor de seguridad confiable. Esto ayudará a garantizar que la red informática no se vea comprometida.

El software de firewall personal debe ser fácil de configurar, instalar y administrar. Una vez que el software está configurado, debe permanecer en modo de monitoreo en todo momento. El software debe establecerse en el estado de inicio predeterminado para garantizar que la seguridad esté habilitada cada vez que se enciende el sistema. Esto permitirá una protección de 24 horas en la red informática de la casa o empresa.

La mayoría de los paquetes de software de firewall rastrearán las transferencias de datos entrantes o salientes. Estos datos se almacenarán en archivos de registro y los administradores del sistema podrán revisarlos periódicamente. El registro habilitado garantiza que se supervisen todas las transferencias de datos, lo que debería limitar a los usuarios la descarga de archivos sospechosos.

3.12 Ventajas de un firewall.

Seguridad en tu red

Un Firewall protege la red al monitorear el tráfico que ingresa a tu ordenador. Además, se puede obtener seguridad de doble función mediante el uso de un Firewall bidireccional, que rastrea el tráfico entrante y saliente.

Este software también se encarga de inspeccionar cada paquete, y si detecta uno potencialmente dañino, lo bloquea inmediatamente.

También protege contra troyanos

Los troyanos, también conocidos como caballos de Troya, **son una pieza de malware que puede dañar tus dispositivos**. Se introducen pasivamente en tu sistema, espiando todos los archivos que contiene. Lo más preocupante es que recopila datos y los envían a un servidor web predeterminado.

Sin embargo, no te darás cuenta de nada de lo que está sucediendo con tu PC hasta que comience a causar problemas. La buena noticia es que si tienes un Firewall integrado en tus dispositivos, no tienes que preocuparte porque evitará que los troyanos entren y los afecten.

Reduce el riesgo de ataques cibernéticos

Los piratas informáticos están constantemente buscando fallas en la red. No hay vuelta atrás una vez que las encuentran. Ellos irán tras esos sistemas y causarán muchos estragos incluyendo propagar el virus a través de un botnet, instalar programas para registrar pulsaciones de teclas, y mucho más.

3.13 Limitaciones de un firewall.

- Un cortafuegos o firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
- El cortafuegos no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes.
- El cortafuegos no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.
- El cortafuegos no puede proteger contra los ataques de la "Ingeniería Social"
- El cortafuegos no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real esta en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.
- El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico. Hay que configurar correctamente y cuidar la seguridad de los servicios que se publiquen a internet.

3.14 Políticas del firewall

Nombre de la política	Nivel de seguridad	Configuración del cliente	Excepciones	Uso recomendado
Acceso total	Bajo	Activar cortafuegos	Ninguna	Utilícela para permitir a los clientes un acceso a la red sin restricciones
Cisco Trust Agent for Cisco NAC	Bajo	Activar cortafuegos	Permitir el tráfico UDP entrante y saliente a través del	Utilícela cuando los clientes tienen una instalación del agente

			puerto 21862	Cisco Trust Agent (CTA)
Puertos de comunicación para Trend Micro Control Manager	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP/UDP entrante y saliente a través de los puertos 80 y 10319	Utilícela cuando los clientes tienen una instalación del agente MCP
Consola de ScanMail for Microsoft Exchange	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP entrante y saliente a través del puerto 16372	Utilice esta opción cuando los clientes necesiten acceder a la consola de ScanMail
Consola de InterScan Messaging Security Suite (IMSS)	Bajo	Activar cortafuegos	Permitir todo el tráfico TCP entrante y saliente a través del puerto 80	Utilícela cuando los clientes necesitan acceder a la consola de IMSS

3.15 Enlaces externos.

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todos las computadoras de la red estarían expuestos a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales

salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

Limitaciones de un Firewall

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

UNIDAD IV VIGILANCIA DE LOS SISTEMAS DE INFORMACIÓN Y HACKING

4.1 Definición de vigilancia.

El **Sistema de Gestión de Seguridad de la Información ISO 27001** persigue la protección de la información y de los sistemas de información del acceso, de utilización, divulgación o destrucción no autorizada.

Los términos seguridad de la información, seguridad informática y garantía de la información son utilizados con bastante frecuencia. El significado de dichas palabras es diferente, pero todos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización.

Entre dichos términos existen **pequeñas diferencias**, dichas diferencias proceden del enfoque que le dé, las metodologías usadas y las zonas de concentración.

La Seguridad de la Información, según **ISO27001**, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser:

- Electrónicos
- En papel
- Audio y vídeo, etc.

Los gobiernos, las instituciones financieras, los hospitales y las organizaciones privadas tienen enormes cantidades de información confidencial sobre sus empleados, productos, investigación, clientes, etc. La mayor parte de esta información es reunida, tratada, almacenada y puesta a disposición de las personas que deseen revisarla.

Si se da el caso de que información confidencial de la organización, de sus clientes, de sus decisiones, de sus cuentas, etc. caen en manos de la competencia, esta se hará pública de una forma **no autorizada** y esto puede suponer **graves consecuencias**, ya que se

perderá credibilidad de los clientes, se perderán posibles negocios, se puede enfrentar a demandas e incluso puede causar la quiebra de la organización.

Es por todo esto que se convierte en una necesidad proteger la **información confidencial**, ya que es un requisito del negocio, y en muchos casos se convierte en algo ético y una obligación legal.

Para una persona normal, la **Seguridad de la Información** puede provocar un efecto muy significativo ya que puede tener diferentes consecuencias la violación de su privacidad dependiendo de la cultura del mismo.

La **Seguridad de la Información** ha crecido mucho en estos últimos tiempos, además ha evolucionado considerablemente. Se ha convertido en una carrera acreditada mundialmente. Dentro del éste área se ofrecen muchas especializaciones que se pueden incluir al realizar la auditoría del **Sistema de Gestión de Seguridad de la Información ISO-27001**, como pueden ser:

- Planificación de la continuidad de negocio
- Ciencia forense digital
- Administración de Sistemas de Gestión de Seguridad

Realizar correctamente la **Gestión de la Seguridad de la Información** quiere establecer y mantener los programas, los controles y las políticas de seguridad que tienen la obligación de conservar la confidencialidad, la integridad y la disponibilidad de la información de la empresa.

- **Confidencialidad**: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.
- **Integridad**: es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
- **Disponibilidad**: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones.

Seguridad Informática

La **Seguridad de la Información** consiste en asegurar que los recursos del Sistema de Información de una empresa se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización.

Los objetivos de la seguridad informática:

Los activos de información son los elementos que la **Seguridad de la Información** debe proteger. Por lo que son tres elementos lo que forman los activos:

- Información: es el objeto de mayor valor para la empresa.
- Equipos: suelen ser software, hardware y la propia organización.
- Usuarios: son las personas que usan la tecnología de la organización.

Análisis de riesgos

El activo más importante que tiene la organización la propia información, por lo que tienen que existir técnicas que las mantengan seguras, mucho más allá de la seguridad física que se puede estableces gracias a los equipos con los que cuenta la organización para almacenar dicha información.

La **información se blinda** con seguridad lógica, es decir, aplicar barreras y procedimientos que resguardan el acceso a todos los datos y restringe el acceso a las personas autorizadas.

Los medios necesarios para conseguirlo son:

- **Restricción del acceso**: de las personas que forman parte de la organización a los programas y a los archivos más importantes.
- Se debe asegurar de que los operados pueden realizar su trabajo pero que no puedan realizar modificaciones en los programas ni en los archivos que no sea necesario.
- Hay que asegurar la utilización de los datos, archivos y los programas correctos en los procedimientos elegidos.
- Se tiene que asegurar la información transmitida, es decir, que la información transmitida sea la misma que se reciba por el destinatario.
- Asegurarse de que existen diferentes sistemas en caso de **emergencia** y estos están distribuidos por toda la organización.
- Hay que organizar a todos los trabajadores y otórgales distintas claves, que sean intransferibles.
- Se debe actualizar de forma constante todas las **contraseñas** de acceso a los sistemas de cómputo.

Para poner en marcha la **política de seguridad**, lo primero que se debe hacer es asegurar los derechos de acceso a los datos y los recursos con los que cuenta la organización, establecer las herramientas de control con las que se contará y lo mecanismos de identificación. Todos los mecanismos facilitan que los operadores tengan los permisos que se les ofrecieron.

Software para ISO 27001

El **Software ISOTools Excellence ISO 27001** para Riesgos y Seguridad de la Información, está capacitado para responder a numerosos controles para el tratamiento de

la información gracias a las aplicaciones que contiene y que son totalmente configurables según los requerimientos de cada organización. Además, este software permite la automatización del **Sistema de Gestión de Seguridad de la Información**.

4.2 Anatomía de un ataque

Fase 1 – Reconocimiento (Reconnaissance)

El reconocimiento se refiere a la fase preparatoria donde el atacante obtiene toda la información necesaria de su objetivo o victima antes de lanzar el ataque. Esta fase también puede incluir el escaneo de la red que el Hacker quiere atacar no importa si el ataque va a ser interno o externo. Esta fase le permite al atacante crear una estrategia para su ataque.

Esta fase puede incluir la Ingeniería Social, buscar en la basura (Dumpster diving), buscar que tipo de sistema operativo y aplicaciones usa el objetivo o víctima, cuáles son los puertos que están abiertos, donde están localizados los routers (enrutadores), cuáles son los host (terminales, computadoras) más accesibles, buscar en las bases de datos del Internet (Whois) información como direcciones de Internet (IP), nombres de dominios, información de contacto, servidores de email y toda la información que se pueda extraer de los DNS (Domain Name Server).

Esta fase le puede tomar bastante tiempo al Hacker ya que tiene que analizar toda la información que ha obtenido para lanzar el ataque con mayor precisión.

Fase 2 – Escaneo (Scanning)

Esta es la fase que el atacante realiza antes de la lanzar un ataque a la red (network). En el escaneo el atacante utiliza toda la información que obtuvo en la Fase del Reconocimiento (Fase 1) para identificar vulnerabilidades específicas. Por ejemplo, si en la Fase 1 el atacante descubrió que su objetivo o su víctima usa el sistema operativo Windows XP entonces el buscara vulnerabilidades específicas que tenga ese sistema operativo para saber por dónde atacarlo.

También hace un escaneo de puertos para ver cuáles son los puertos abiertos para saber por cual puerto va entrar y usa herramientas automatizadas para escanear la red y los host en busca de más vulnerabilidades que le permitan el acceso al sistema.

Fase 3 – Ganar Acceso (Gaining Access)

Esta es una de las fases más importantes para el Hacker porque es la fase de penetración al sistema, en esta fase el Hacker explota las vulnerabilidades que encontró en la fase 2. La explotación puede ocurrir localmente, offline (sin estar conectado), sobre el LAN (Local Area Network), o sobre el Internet y puede incluir técnicas como buffer overflows (desbordamiento del buffer), denial-of-service (negación de servicios), sesión hijacking (secuestro de sesión), y password cracking (romper o adivinar claves usando varios métodos como: diccionary atack y brute forcé atack).

Los factores que ayudan al Hacker en esta fase a tener una penetración exitosa al sistema dependen de cómo es la arquitectura del sistema y de cómo está configurado el sistema objetivo o víctima, una configuración de seguridad simple significa un acceso más fácil al sistema, otro factor a tener en cuenta es el nivel de destrezas, habilidades y conocimientos sobre seguridad informática y redes que tenga el Hacker y el nivel de acceso que obtuvo al principio de la penetración (Fase 3).

Fase 4 – Mantener el Acceso (Maintaining Access)

Una vez el Hacker gana acceso al sistema objetivo (Fase3) su prioridad es mantener el acceso que gano en el sistema. En esta fase el Hacker usa sus recursos y recursos del sistema y usa el sistema objetivo como plataforma de lanzamiento de ataques para escanear y explotar a otros sistemas que quiere atacar, también usa programas llamados sniffers para capturar todo el tráfico de la red, incluyendo sesiones de telnet y FTP (File Transfer Protocol).

En esta fase el Hacker puede tener la habilidad de subir, bajar y alterar programas y data.

En esta fase el hacker quiere permanecer indetectable y para eso remueve evidencia de su penetración al sistema y hace uso de Backdoor (puertas traseras) y Troyanos para ganar

acceso en otra ocasión y tratar de tener acceso a cuentas de altos privilegios como cuentas de Administrador. También usan los caballos de Troya (Trojans) para transferir nombres de usuarios, passwords e incluso información de tarjetas de crédito almacenada en el sistema.

Fase 5 – Cubrir las huellas (Covering Tracks)

En esta fase es donde el Hacker trata de destruir toda la evidencia de sus actividades ilícitas y lo hace por varias razones entre ellas seguir manteniendo el acceso al sistema comprometido ya que si borra sus huellas los administradores de redes no tendrán pistas claras del atacante y el Hacker podrá seguir penetrando el sistema cuando quiera, además borrando sus huellas evita ser detectado y ser atrapado por la policía o los Federales.

Las herramientas y técnicas que usa para esto son caballos de Troya, Steganography, Tunneling, Rootkits y la alteración de los "log files" (Archivos donde se almacenan todos los eventos ocurridos en un sistema informático y permite obtener información detallada sobre los hábitos de los usuarios), una vez que el Hacker logra plantar caballos de Troya en el sistema este asume que tiene control total del sistema.

4.3 Escaneos.

Es un análisis, identificación y reporte muy sistemático de las vulnerabilidades en cuestión de seguridad que se tienen en una infraestructura de cómputo. La intención es proteger en el mejor porcentaje posible la seguridad de la información ante el ataque de un ente externo.

¿En que ayuda a una empresa?

Permite remediar las vulnerabilidades dentro del ambiente TI antes de que un hacker o agresor cibernético logre detectarlas, es cierto, nadie puede proteger una empresa al 100% pues cada segundo nace nuevos virus y es imposible seguirles el paso.

¿Importa el tamaño de la empresa?

Alrededor del mundo no se ha detectado un patrón de comportamiento para los ataques y es que la información puede tener un valor diferente entre las personas, no importa si eres una PyME o una empresa de talla mundial, siempre habrá alguien que valore tu información de una forma u otra.

¿Cuáles son los entregables en un Escaneo de Vulnerabilidades?

- Contrato de confidencialidad
- Detección y evaluación de las vulnerabilidades a través del uso de hardware y software
- Análisis del muestreo
- Reporte cuantitativo y cualitativo de los datos obtenidos
- Sugerencias
- Propuesta de Soluciones para robustecer la estrategia de ciberseguridad

¿Cada cuándo se debe hacer?

Los expertos de Cero Uno Software recomiendan hacer esta actividad cada 6 meses, de esta forma se da un seguimiento equilibrado y estructurado a la estrategia de Seguridad Informática.

Detalles importantes para contratar un escaneo de vulnerabilidades con una empresa:

- Identifica la trayectoria en el tema de Ciberseguridad de la empresa que contratarás
- Revisa si están debidamente certificadas
- Pide referencias del personal que te atenderá
- Investiga en internet la reputación que tiene la empresa
- Exige el contrato de confidencialidad que te blindará en caso de que la información se filtre

- Pide costos y alcances previo a firmar un contrato

4.4 Identificación de vulnerabilidades

La diferencia entre vulnerabilidad y amenaza es muy interesante, aunque son términos que se confunden a menudo. Veamos cómo se definen:

- Una **vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.
- Por su parte, una **amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas.

Por tanto, las vulnerabilidades son las condiciones y características propias de los sistemas de una organización que la hacen susceptible a las amenazas. El problema es que en el mundo real, si existe una vulnerabilidad, siempre existirá alguien que intentará explotarla, es decir, sacar provecho de su existencia.

Una vez que tenemos clara la diferencia entre amenaza y vulnerabilidad, es interesante introducir el concepto de **riesgo**. El riesgo es la probabilidad de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como puede ser un hacker, un ataque de denegación de servicios, un virus… El riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice

aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo.

Algunas de las fuentes de amenazas más comunes en el ámbito de sistemas de información son:

- Malware o código malicioso: permite realizar diferentes acciones a un atacante. Desde ataques genéricos mediante la utilización de troyanos, a ataques de precisión dirigidos, con objetivos específicos y diseñados para atacar a un dispositivos, configuración o componente específico de la red.
- Ingeniería social: Utilizan técnicas de persuasión que aprovechan la buena voluntad y falta de precaución de la víctima para obtener información sensible o confidencial. Los datos así obtenidos son utilizados posteriormente para realizar otro tipo de ataques, o para su venta.
- APT o Amenazas Persistentes Avanzadas (*Advanced Persistent Threats*): son ataques coordinados dirigidos contra una empresa u organización, que tratan de robar o filtrar información sin ser identificados. Se suelen ayudar de técnicas de ingeniería social y son difíciles de detectar.
- Botnets: conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS.
- Redes sociales: el uso no controlado de este tipo de redes puede poner en riesgo la reputación de la empresa.

- Servicios en la nube: una empresa que contrate este tipo de servicios tiene que tener en cuenta que ha de exigir los mismos criterios de seguridad que tiene en sus sistemas a su proveedor de servicios. Se ha de asegurar de contratarlos con empresas cuya seguridad este demostrada, y firmar SLA o ANS (Acuerdos de Nivel de Servicio) en los que quede definida la seguridad que necesita la empresa.

Algunos incidentes pueden implicar problemas legales que pueden suponer sanciones económicas y daños a la reputación e imagen de la empresa. Por eso, es importante conocer los riesgos, medirlos y evaluarlos para evitar en la medida de lo posible los incidentes, implantando las medidas de seguridad adecuadas.

Podemos identificar los activos críticos de los sistemas de información que pueden suponer un riesgo para la empresa, realizando un análisis de riesgos. Análisis que nos llevará a obtener una imagen rigurosa de los riesgos a los que se encuentra expuesta nuestra empresa. Estas fases son las siguientes:

Este análisis nos servirá para averiguar la magnitud y la gravedad de las consecuencias del riesgo a la que está expuesta nuestra empresa y, de esta forma, gestionarlos adecuadamente. Para ello tendremos que definir un umbral que determine los riesgos asumibles de los que no lo son. En función de la relevancia de los riegos podremos optar por:

- **Evitar el riesgo** eliminando su causa, por ejemplo, cuando sea viable optar por no implementar una actividad o proceso que pudiera implicar un riesgo.
- **Adoptar medidas que mitiguen el impacto o la probabilidad del riesgo** a través de la implementación y monitorización de controles.

- **Compartir o transferir el riesgo** con terceros a través de seguros, contratos etc.
- **Aceptar la existencia del riesgo** y monitorizarlo.

4.5 Actividades de infiltración.

Un empleado recoge del suelo una llave maya y apenas llega a la empresa la instala en su computadora personal (PC) para revisar qué tiene, descarga una foto en su red social o abre un archivo anexo que le llegó en un correo a su dirección electrónica empresarial.

En todos los casos es probable que un ciberdelincuente haya colocado un software maligno (malware). En ese momento, pese a todos los antivirus, murallas de fuego (firewall), antispam y otros programas informáticos de seguridad usuales, ya el hacker –como popularmente se les conoce– habrá infiltrado a su compañía.

El segundo paso será pasar a otras PC hasta obtener los accesos a algún servidor. Esperará pacientemente para obtener las credenciales y permisos que le permitan llegar a equipos y sistemas donde se guarda la información clave, aquella de la que dependen las operaciones de la firma.

A partir de ahí podría robar información de los clientes, realizar fraudes financieros, provocar un ataque de denegación de servicios o simplemente, como si tuviera un switch, apagar los sistemas con los que se atiende a proveedores y clientes.

“Los antivirus o firewall son necesarios, pero no son suficientes”, recalcó Roberto Arbeláez, jefe regional de asesoría en seguridad de Microsoft. “Los atacantes buscan el eslabón más débil, que son los usuarios”.

Los hackers recurren a la llamada “ingeniería social”, que consiste en aprovechar la confianza e inocencia de los usuarios para infiltrar las compañías e instituciones públicas.

El problema es que, pese a que todas reciben ataques día a día, la mayoría de las organizaciones no se dan cuenta de que han sido infiltradas. Cuando lo hacen, ya es muy tarde, casi un año tarde.

Múltiples mecanismos

Los peligros aumentarán con las nuevas tendencias como las tecnologías del vestir (wearables) y hasta Internet de las cosas (IoT), donde hay múltiples equipos, dispositivos y sensores conectados.

"El perímetro de seguridad se extiende", advirtió Pablo Ruiz, subgerente de desarrollo de negocios de seguridad integral de Telefónica en España, durante el evento Tech Day organizado por la revista IT Now la semana pasada en el hotel Herradura.

El primer paso que deben dar las empresas es, precisamente, identificar las amenazas que hay más allá de ese perímetro, los riesgos que enfrenta y las vulnerabilidades que tiene. El objetivo es resolver estas debilidades en lo inmediato y diseñar estrategias de largo plazo basadas en las mejores prácticas de la industria.

Los softwares de seguridad usuales son herramientas de protección necesarias. El problema es que se basan en patrones y listas de malware ya detectados. Ante los nuevos programas malignos –que aprovechan los descuidos y la confianza de los usuarios para infectar los sistemas corporativos– se necesitará un esfuerzo tecnológico adicional.

Detectarlos implica recurrir a la "seguridad inteligente", que se basa en big data, analítica, telemetría e inteligencia artificial. Así se puede identificar –entre las miles o millones de transacciones– cuáles presentan un comportamiento alterado debido a fallas o pulgas normales de los sistemas y cuáles se deben a un malware.

4.6 Consolidación.

- Mejoras en la Administración, la Gestión y el Soporte
- Ahorro de inversión (licencias de software, espacio físico, contratos de mantenimiento.)
- Reducción en la complejidad de las Infraestructuras de la Información
- Optimización en anchos de banda
- Facilidad y Seguridad en el acceso a las aplicaciones
- Calidad en los niveles de Servicio a los usuarios a través de una infraestructura de información optimizada

4.7 Defensa perimetral.

La seguridad perimetral informática no deja de tener el mismo significado que la general. De hecho, también son todos los sistemas destinados a proteger de intrusos tu perímetro. La única diferencia es que, en lugar de un espacio físico, **se protegen las redes privadas de tu sistema informático**.

Se trata de una **primera línea de defensa**, igual que las alarmas de una oficina. La seguridad total no existe ni en el mundo físico ni en el informático, pero reduce muchísimo el riesgo a que nos roben nuestros datos o, incluso, que puedan desaparecer.

Funciones de una buena seguridad perimetral informática

La seguridad perimetral que protege tus redes debe cumplir **cuatro funciones básicas**:
– **Resistir** a los ataques externos.

– **Identificar** los ataques sufridos y alertar de ellos.

– **Aislar** y **segmentar** los distintos servicios y sistemas en función de su exposición a ataques.

– **Filtrar** y **bloquear** el tráfico, permitiendo únicamente aquel que sea absolutamente necesario.

Herramientas de seguridad perimetral informática

Igual que para proteger tu casa, en informática tienes varias formas de establecer una seguridad perimetral.

Cortafuegos

Los cortafuegos definen, mediante una **política de accesos**, qué tipo de tráfico se permite o se deniega en la red.

Existen varios tipos de cortafuegos:

– A nivel de pasarela: para aplicaciones específicas.

– De capa de red: filtra por IP origen/destino.

– De capa de aplicación: según el protocolo a filtrar.

– Personal: para sistemas personales como PC o móviles.

Sistemas de Detección y Prevención de Intrusos

Son dispositivos que **monitorizan y generan alarmas cuando hay alertas de seguridad**.
Su actuación sigue estos pasos:

1. Identificación de un posible ataque.
2. 2. Registro de los eventos.
3. Bloqueo del ataque.
4. Reporte a los administradores y sistemas de seguridad.

Honeypots

Se trata de una **trampa para atraer y analizar ataques de bots y hackers**. De esta forma se pueden detectar a tiempo y recoger información que servirá para evitar ataques en un futuro hacia sistemas más importantes. Evidentemente, deben estar muy controlados y permanecer desconectados de cualquier red propia.

Pasarelas antivirus y antispam

Se trata de sistemas intermedios que **filtran el contenido malicioso que quiere entrar a nuestras redes**. Sobre todo, se detectan los malware en pasarelas web y servidores de correo, evitando que lleguen a afectar los sistemas privados.

Seguridad perimetral: ¿Cómo proteger a tu empresa?

La mejor manera de dotar de seguridad perimetral informática a tu empresa es contratando los servicios de una empresa con experiencia como Accensit. Ayudamos a establecer y gestionar los sistemas de tu empresa mediante:

– Un diseño de una **topología red adecuada**.

– Recomendaciones de **soluciones eficientes**.

– Instalación y configuración de **elementos red que sean necesarios**.

– Proporción de soporte y equipos para **el seguimiento y la administración de la red**.

Para cualquier duda, contacta con Accensit. Escucharemos tu caso y te daremos las mejores soluciones en relación calidad-precio.

4.8 Ética de hacking.

Qué es un hacking ético se define a través de lo que hacen los profesionales que se dedican a ello, es decir, los piratas informáticos éticos. Estas personas son contratadas para hackear un sistema e identificar y reparar posibles vulnerabilidades, lo que previene eficazmente la explotación por hackers maliciosos. Son expertos que se especializan en las pruebas de penetración de sistemas informáticos y de software con el fin de evaluar, fortalecer y mejorar la seguridad.

Este tipo de pirata informático a menudo se denomina como **hacker de 'sombrero blanco'** (White hat), con el fin de diferenciarlos de los piratas informáticos criminales, que se conocen como hackers de 'sombrero negro'.

Una de las armas más poderosas en la lucha contra los **ciberdelincuentes** ha sido la de los piratas informáticos. Los profesionales con un profundo conocimiento de cómo penetrar en la seguridad de una infraestructura en línea se implementan comúnmente para encontrar vulnerabilidades que aquellos del otro lado del espectro de piratería moral buscarían explotar.

TIPOS DE HACKERS

Si hay que explicar **qué es el hacking ético** es porque hay otro tipo de piratería que ha provocado su aparición.

Dentro de la comunidad de **seguridad cibernética**, los piratas informáticos se dividen en tres campos: piratas informáticos 'sombrero negro', 'sombrero gris' y 'sombrero blanco'.

Los **sombreros negros** piratean sus objetivos por razones egoístas, como ganancias financieras, para vengarse o simplemente para causar estragos.

Fuente: El Comercio

Los **piratas informáticos de sombrero blanco**, en cambio, apuntan a mejorar la seguridad, encontrar agujeros en ella y notificar a la víctima para que tenga la oportunidad de arreglarlos antes de que un hacker menos escrupuloso los explote.

Los **sombreros grises** se ubican en algún lugar entre los dos campos, a menudo llevando a cabo operaciones ligeramente más cuestionables desde el punto de vista moral, como piratear grupos a los que se oponen ideológicamente, o lanzar protestas hacktivistas.

La forma que utilizan estos profesionales para ganar dinero también explica **qué es el hacking ético**. Los que lo practican, con bastante frecuencia son empleados por las compañías de seguridad cibernética, o dentro de los departamentos de seguridad de las organizaciones más grandes. El hecho de que ellos sepan cómo operan los atacantes, a menudo les da una valiosa perspectiva sobre cómo prevenir los ataques.

Otra forma con la que los **hackers éticos** pueden ganarse la vida es mediante la recopilación de "recompensas de errores". Las grandes empresas, en particular las de tecnología como Facebook, Microsoft y Google, ofrecen una recompensa a los

investigadores o hackers que descubren agujeros de seguridad dentro de sus redes o servicios.

4.9 Introducción a Kali Linux.

Kali Linux es la nueva generación de la distribución Linux BackTrack para realizar Auditorías de Seguridad y Pruebas de Penetración. Kali Linux es una plataforma basada en GNU/Linux Debian y es una reconstrucción completa de BackTrack, la cual contiene una gran cantidad de herramientas para capturar información, identificar vulnerabilidades, explotarlas, escalar privilegios y cubrir las huellas.

Este Curso proporciona una excelente guía práctica para utilizar las herramientas más populares que abarcan las bases de las Pruebas de Penetración incluidas en Kali Linux. Así mismo, este curso es una excelente fuente de conocimiento tanto para los profesionales como para los novatos.

Características de Kali Linux

Kali Linux es una completa reconstrucción de BackTrack Linux, y se adhiere completamente a los estándares de desarrollo de Debian. Se ha puesto en funcionamiento toda una nueva infraestructura, todas las herramientas han sido revisadas y empaquetadas, y se utiliza ahora Git para el CVS.

- Más de 300 herramientas de Pruebas de Penetración
- Es Libre y siempre lo será
- Árbol Git Open Source
- Cumple con FHS (Filesystem Hierarchy Standart)
- Amplio soporte para dispositivos inalámbricos
- Parches al Kernel para inyección.
- Entorno de desarrollo seguro
- Paquetes y repositorios firmados con GPG
- Varios lenguajes
- Completamente personalizable
- Soporte ARMEL y ARMHF

Obtener Kali Linux

Kali Linux puede ser descargado para diferentes arquitecturas, como i386, amd64 y armel, armhf. Únicamente para la arquitectura i386 puede ser descargado ya sea en una imagen ISO o en una máquina virtual para VMWare. Además puede ser descargado mediante descarga directa o mediante Torrent.

Kali Linux puede ser descargado desde la siguiente página:

http://www.kali.org/downloads/

Instalación de Kali Linux

Kali Linux puede ser instalado en un disco duro, para realizar un arranque dual con un Sistema Operativo Windows, instalado en una unidad USB e instalado en un disco cifrado.

Se puede encontrar la información detallada sobre la instalación de Kali Linux en la siguiente página: http://docs.kali.org/category/installation

1.4 Cambiar la Contraseña del root

Por una buena práctica de seguridad se recomienda cambiar la contraseña por defecto del usuario root. Esto dificultará que usuarios maliciosos pueden obtener acceso al sistema, con esta clave por defecto.

```
# passwd root
Enter new UNIX password:
Retype new UNIX password:
```

[*] La contraseña no será mostrada mientras sea escrita y está deberá ser ingresada dos veces.

Iniciando Servicios de Red

Kali Linux viene con algunos servicios de red, lo cuales pueden ser de utilidad en varias situaciones y que está deshabilitadas por defecto. Estos servicios son, HTTP, Mestaploit,

MySQL y SSH. Por ejemplo, para iniciar el servicio HTTP se debe ejecutar el siguiente comando

/etc/init.d/apache2 start

Los cuatro servicios, detallados en el párrafo anterior, también pueden iniciados y detenidos desde: Applications -> Kali Linux -> System Services.

Kali Linux tiene documentación oficial sobre varios de sus aspectos y características. La documentación está en constante trabajo y progreso. Esta documentación puede ser ubicada en la siguiente página:

http://docs.kali.org/

4.10 Penetración I

Pruebas de caja negra

Las pruebas de caja negra implican la realización de una evaluación de la seguridad y pruebas sin conocimiento previo de la infraestructura o de la infraestructura de red a probar. La prueba simula un ataque de un hacker malicioso fuera del perímetro de seguridad de la organización.

Pruebas de caja blanca

Las pruebas de caja blanca implican la evaluación de la seguridad y las pruebas son con conocimiento completo de la infraestructura de red, como un administrador de red podría hacer.

Pruebas de caja gris

Las pruebas de caja gris implican la realización de la evaluación de la seguridad y pruebas internas. Las pruebas examinan el grado de acceso a información privilegiada dentro de la red. El propósito de esta prueba es para simular las formas más comunes de ataque, los que se inician desde dentro de la red.

Triángulo de la Seguridad, funcionalidad y facilidad de uso

Como profesional de la seguridad, es difícil encontrar un equilibrio entre la instauración de barreras de seguridad para evitar un ataque y permitir que el sistema permanezca funcional para los usuarios. El triángulo de la seguridad, funcionalidad y facilidad es una representación del equilibrio entre la seguridad, la funcionalidad y la facilidad de uso para los usuarios del sistema (ver Figura 1.3). En general, cuando la seguridad aumenta, la funcionalidad y facilidad de uso para los usuarios del sistema disminuye.

Figura 1.3 – Triángulo de la Seguridad

En un mundo ideal, los profesionales de la seguridad les gustaría tener el más alto nivel de seguridad en todos los sistemas; Sin embargo, a veces esto no es posible. Demasiadas barreras de seguridad dificultan el uso de los sistemas a los usuarios e impiden la funcionalidad del sistema.

Investigación de Vulnerabilidades y Herramientas

El estudio de vulnerabilidades es el proceso de descubrimiento de vulnerabilidades y debilidades de diseño que podría conducir a un ataque a un sistema. Existen varios sitios web y herramientas para ayudar a los hackers éticos en el mantenimiento de una lista actualizada de vulnerabilidades y posibles agujeros de seguridad de los sistemas o redes.

Es esencial que los administradores de sistemas se mantengan actualizados sobre los últimos virus, Troyanos y otros ataques comunes a fin de proteger adecuadamente sus sistemas y

redes. Además, al familiarizarse con las nuevas amenazas, un administrador puede aprender a detectar, prevenir y recuperarse de un ataque.

Informe de Hacking Ético

El resultado de una prueba de penetración en una red o una auditoría de seguridad es un informe de hacking ético, o de pen test. Cualquier nombre es aceptable, y se puede utilizar indistintamente. Este informe detalla los resultados de la actividad de hackeo, los tipos de pruebas realizadas y los métodos de hacking usados. Los resultados se comparan con las expectativas inicialmente acordadas con el cliente.

Cómo ser ético

El hacking ético se suele llevar a cabo de una manera estructurada y organizada, por lo general como parte de una prueba de penetración o de auditoría de seguridad. La profundidad y amplitud de los sistemas y aplicaciones a verificar se fija normalmente a partir de las necesidades y preocupaciones del cliente. Muchos hackers éticos son miembros de un equipo tigre. Un equipo tigre trabaja en conjunto para realizar una prueba a gran escala que cubre todos los aspectos de la red, físico e intrusión en los sistemas.

Los pasos siguientes son un marco para la realización de una auditoría de seguridad en una organización y ayudará a asegurar que la prueba se lleva a cabo de una manera organizada, eficiente y de manera ética:

- Hablar con el cliente, y discutir las necesidades a ser consideradas durante la prueba.
- Preparar y firmar documentos NDA con el cliente.
- Organizar un equipo de hacking ético, y preparar un calendario para la prueba.
- Llevar a cabo la prueba.
- Analizar los resultados de las pruebas, y preparar un informe.
- Presentar los resultados del informe al cliente.

Realización de una prueba de penetración

Muchos hackers éticos que desempeñan el papel de profesionales de seguridad utilizan sus habilidades para llevar a cabo evaluaciones de seguridad o pruebas de penetración. Estas pruebas y evaluaciones tienen tres fases, generalmente ordenadas de la siguiente manera:

Preparación.

Esta fase consiste en un acuerdo formal entre el hacker ético y la organización. Este acuerdo debe incluir el alcance completo de la prueba, los tipos de ataques (Internos o externos) a utilizar, y los tipos de pruebas: caja blanca, negra o gris

Realizar evaluación de la seguridad

Durante esta fase, las pruebas se llevan a cabo, después de lo cual el pentester prepara un informe formal de vulnerabilidades y otros hallazgos.

4.11 Penetración II.

Pruebas orientadas a un objetivo

Estas pruebas selectivas se llevan a cabo en conjunto por el equipo de TI de la organización y el equipo de pruebas de penetración. A veces se le llama un enfoque de "luces encendidas" porque cualquiera puede ver el examen que se lleva a cabo.

Comprobación externa

Este tipo de prueba de penetración se dirige a los servidores o dispositivos de la compañía que son visibles externamente, incluyendo servidores de nombres de dominio (DNS), servidores de correo electrónico, servidores web o *firewalls*. El objetivo es averiguar si un atacante externo puede entrar y hasta dónde puede llegar una vez que ha obtenido acceso.

Pruebas internas

Esta prueba simula un ataque interno detrás del *firewall* por un usuario autorizado, con privilegios de acceso estándar. Este tipo de prueba es útil para estimar la cantidad de daño que un empleado descontento podría causar.

Pruebas a ciegas

Una estrategia de prueba a ciegas simula las acciones y procedimientos de un atacante real, limitando severamente la información dada de antemano a la persona o equipo que está realizando la prueba. Por lo general, solo se les puede dar el nombre de la empresa. Debido a que este tipo de prueba puede requerir una cantidad considerable de tiempo para el reconocimiento, puede ser costosa.

Pruebas de doble ciego

Las pruebas de doble ciego toman la prueba a ciegas y la llevan un paso más allá. En este tipo de prueba de penetración, solo una o dos personas de la organización pueden ser conscientes de que se está realizando una prueba. Las pruebas de doble ciego pueden ser útiles para probar el monitoreo de seguridad y la identificación de incidentes de la organización, así como sus procedimientos de respuesta.

Bibliografía

”Seguridad Informática”	Garcia-Cerevignon A. Alegre Ramos M. (2010)	PARANINFO
“Firewalls and Internet Security: Repelling the Wily Hacker.”	Cheswick, William R.; Bellovin, Steven M.	Addison-Wesley Pub Co.
“Libro Electrónico de Seguridad Informática y Criptografía”.	Aguirre, Jorge R	Legal M-10039-2003. Disponible en Internet en http://www.criptored.upm.es/guiateoria/gt_m001a.htm

TITULO	LINK	AUTOR
Seguridad informática vs Seguridad de la información	https://youtu.be/Z2aF4UqHKkA	Instituto de Ciberseguridad
Cultura Hacker. Conociendo al enemigo	https://youtu.be/MYBZpeq-h_M	Instituto de Ciberseguridad
Cultura Hacker. Conociendo al enemigo	https://youtu.be/_PsB2e0U5FU	Chema Alonso