Nombre del alumno: Johanne Joaquín Arriaga Díaz

Nombre del profesor: Icel Bernardo Lepe Arriaga.

Nombre del trabajo: Mapa conceptual de unidad II.

Materia: Seguridad en la información.

Grado: Noveno cuatrimestre.

Grupo: ISC13SDC0119-F

Frontera Comalapa, Chiapas a 11 de junio de 2022

CERTIFICADOS Y FIRMAS DIGITALES

Distribución de

Las claves se distribuyen por correo electrónico u otro medio electrónico. Por correo electrónico es una buena práctica sólo cuando tengamos unos pocos corresponsales, e incluso si tuviéramos muchos corresponsales.

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 al servidor de claves.

Criptografía

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

Criptografía simétrica

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.

Criptografía asimétrica

Emplea dos claves para hacer más robusto e impenetrable el mensaje. Una clave es pública y no ofrece protección porque su único objeto es establecer un canal -o recipiente- que sirve para remitir -o entregar- el mensaje.

Certificación.

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

La certificación ISO/IEC 27001 es una demostración del compromiso de una organización en la gestión de seguridad de la información.

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.

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 los componentes de una o varias Autoridades de Certificación. Incluye los elementos de red, servidores, aplicaciones, etc.

Componentes lógicos básicos de una infraestructura de clave pública.

Autoridad de certificación CA. Establece identidades y crea los certificados que forman una asociación entre la identidad y una pareja de claves pública y privada.

Autoridad de registro RA. Responsable del registro y autenticación inicial de los usuarios a quienes se les expedirá un certificado si cumplen todos los requisitos.

Servidor de certificados. Expide certificados aprobados por RA. La clave pública generada para el usuario se combina con otros datos de identificación y se firma digitalmente con la clave privada de la CA.

Repositorio de certificados. Hace disponibles las claves públicas de las identidades registradas antes de que puedan utilizar sus certificados.

Políticas y prácticas de certificación.

La seguridad informática es un área de las empresas que engloba tecnologías y procesos para proteger datos, redes y sistemas de ataques y acceso no autorizado a información confidencial.

Importancia de la Ciberseguridad

La ciberseguridad juega un papel preponderante en negocios digitales, ya que la integridad de los datos es clave para la operación, productividad y competitividad en los diferentes mercados.

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%).

Gestión de una PKI.

PKI, Web Services y SOA. 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, cambia la interoperación de las organizaciones a nivel interno y externo. Conduce sistemas de información conectados e integrados en una infraestructura de Internet, e introduce un nuevo entorno donde la funcionalidad de aplicaciones se ofrece y accede como servicio, se tiene una baja dependencia entre componentes de software, y esto permite dotar de flexibilidad la infraestructura, para responder a los cambios organizacionales u operacionales.

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

Estándares y protocolos de certificación

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

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.

Este tipo de estándares está relacionado con las especificaciones de la OGC. Esta especificación proporciona tanto a los desarrolladores de software como a los usuarios de información geográfica, unas interfaces comunes 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 un protocolo de seguridad: HTTPS

Una conexión HTTP puede ser fácilmente secuestrada y el propósito de una conexión HTTPS es evitar esto: encripta los datos para asegurar una transmisión de datos segura. La transmisión está encriptada y el servidor autenticado.

Cuando un usuario confirma una entrada de URL en la barra de direcciones, 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, y se realiza el cifrado. Normalmente, se utiliza un certificado SSL.

Objetivos

El propósito de una conexión HTTPS es proteger los datos que se transmiten. Otro problema es la suplantación de identidad (phishing), en la cual los datos introducidos se envían a personas no autorizadas que utilizan sitios web falsos. El objetivo de HTTPS es proporcionar a los usuarios privacidad, seguridad y protección de datos.

Uso y relevancia

Un campo de aplicación importante es la banca online. En cualquier lugar donde se utilice una cuenta protegida por contraseña. Esto incluye el acceso a redes sociales, o

SSL

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.

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.

SSH

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

¿Cómo lo hace?

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.