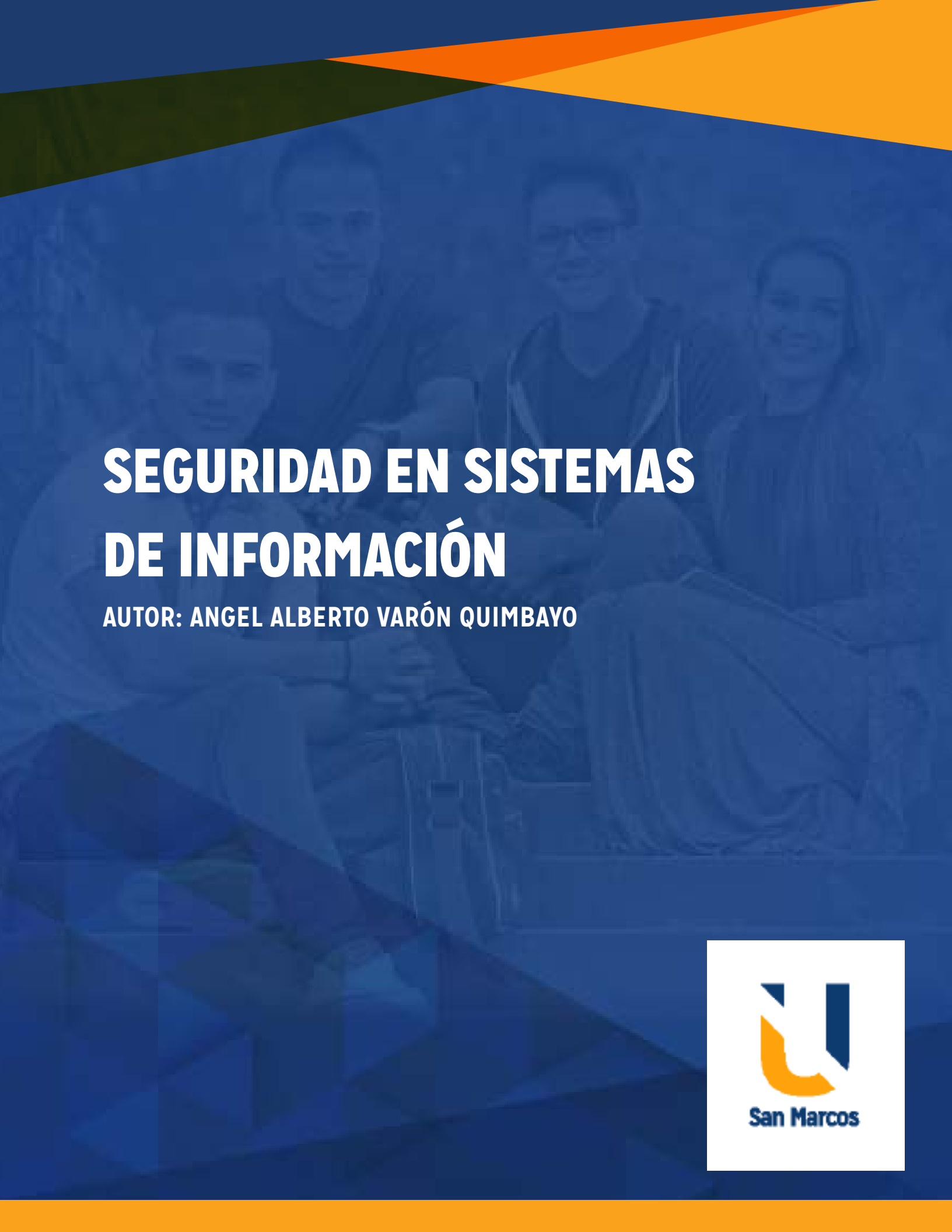
SEGURIDAD EN SISTEMAS DE INFORMACIÓN

AUTOR: ANGEL ALBERTO VARÓN QUIMBAYO



San Marcos

ÍNDICE

Introducción 3

Seguridad en Sistemas de Información 4

- Seguridad física 5
- Seguridad humana 6
- Seguridad en la red 9
- Seguridad en Sistemas Operativos 9
- Seguridad en aplicaciones 10
- Seguridad en los SGBD o Sistemas de Gestión de Bases de Datos 11

Medidas 11

- Medidas de seguridad 11
- Protocolos de Seguridad en aplicaciones 13

Aplicaciones Web 15

Aplicaciones Móviles 17

Bibliografía 19

INTRODUCCIÓN

En los últimos años la información se convirtió en uno de los insumos más importantes para una organización, por este motivo se debe proteger de la mejor manera, garantizando su seguridad, integridad, confidencialidad y su disponibilidad a los usuarios en cualquier momento y lugar.

La importancia de este tema radica en que hoy día las organizaciones exigen la implementación de prácticas de seguridad informática a los profesionales en TI, no importa el rol que desempeñe, ya sea de CIO líder de administración estratégica de tecnología, administrador de bases de datos, analista de sistemas de información, desarrollador de software etc., para garantizar la seguridad en las aplicaciones y minimizar los riesgos en la vulnerabilidad que se presente en la misma. Los ciber-delincuentes o Hackers a diario desarrollan nuevas modalidades para atacar los sistemas informáticos.

Los constantes ataques a los sistemas informáticos, la importancia y relevancia de la información dentro de las organizaciones y el crecimiento de delitos informáticos, han permitido que en los últimos años las organizaciones apliquen las medidas necesarias para tratar de asegurar algunos de sus activos más importantes: la información; esto lleva a que muchos profesionales de las TI se vean en la obligación de capacitarse día tras día en temas relacionados con la seguridad física y lógica en sistema de datos. Por tanto, se debe plantear si

¿Qué conceptos en seguridad de aplicaciones y legislación de la seguridad debe tener en cuenta el profesional en Ingeniería de sistemas?

Seguridad en Sistemas de Información

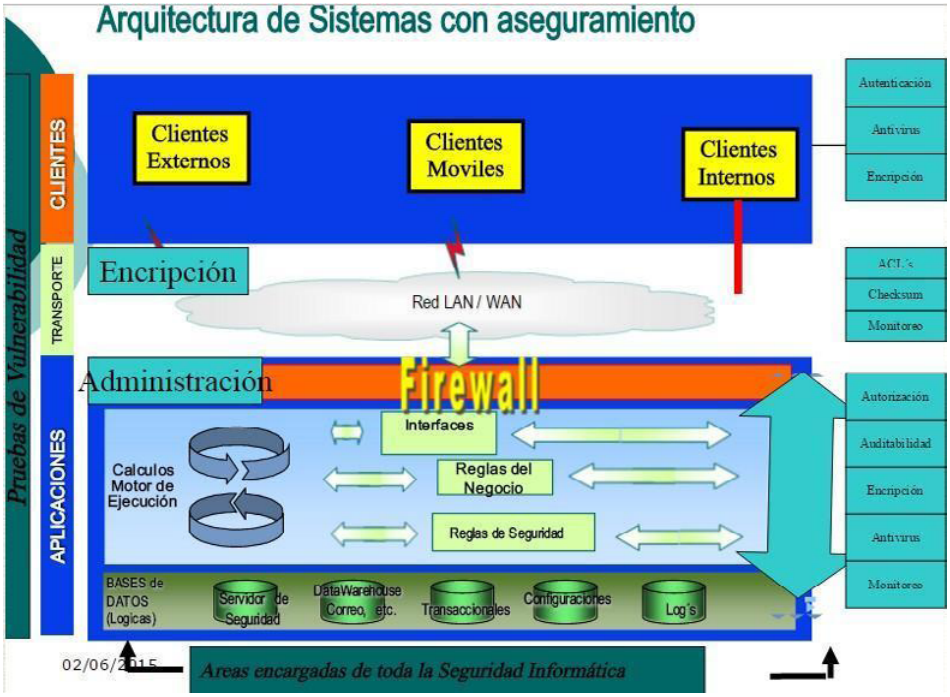


Figura 1. Arquitectura de sistemas con aseguramiento
Fuente: Propia.

Seguridad física

Se refiere a los dispositivos de prevención y detección para proteger recursos del sistema (personal, sitio donde se labora, datos, equipos y medios con los que el personal interactúa), el hardware y el almacenamiento de información, así como las vías de acceso remoto para limitar los posibles actos dañinos a que puedan ser víctimas, de la relevancia que se le dé a estos dependerá del entorno y los sistemas a proteger, así como de la determinación de procedimientos para reconocer las técnicas e identificar los riesgos que puedan afectar la seguridad de una instalación, los bienes y procesos que se desarrollen, para de esta manera implementar sistemas prácticos para su protección y tomar medidas frente a las posibles amenazas de los recursos informáticos.

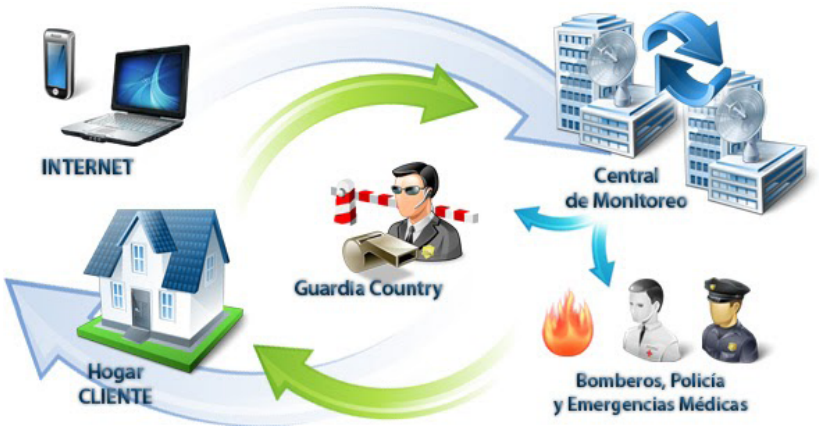


Figura 2. Riesgos y amenazas
Fuente: https://bit.ly/2yPdSFN

Garantizar la seguridad física de la tecnología es uno de los procedimientos más acertados para reducir riesgos en su uso. Tener control en el ambiente y acceso físico permite integrar la seguridad como función esencial para disminuir siniestros y tener los medios para contrarrestar accidentes.

Varios de los problemas que se prevén en seguridad física son:

Desastres naturales	Amenazas causadas por el hombre
Incendios accidentales Inundaciones Tormentas Terremotos	Disturbios Sabotajes deliberados tanto internos como externos Todo tipo de acciones de agresión Robo Destrucción de la información

Seguridad humana

El factor humano se convierte en la principal amenaza para un sistema, por lo que es donde más se invierte en recursos para controlar y contrarrestar sus efectos. Principalmente compuesto por malintencionados o incumplimiento en las políticas de seguridad pueden dividen en:

- Curiosos: personas que entran al sistema motivados por curiosos desafío personal.
- Intrusos remunerados: atacantes que penetran los sistemas a cambio de dinero, gente experta en vulneración de sistemas.
- Personal enterado: personas que tienen acceso y conocen el sistema u organización.
- Terroristas: gente con objetivos de causar daños con fines proselitistas o religiosos.
- Robo: extraer información por medio de dispositivos electrónicos sin autorización de la organización.
- Sabotaje: dañar o reducir la funcionalidad del sistema de manera liberada.
- Fraude: aprovecharse de la confianza brindada para beneficiarse con la información de la empresa.
- Ingeniería social: obtener información confidencial a través de la manipulación de usuarios legítimos.

Cada persona en una empresa debe tener muy claro, cuál es su responsabilidad en la seguridad de los elementos a su cuidado, por medio de las políticas de seguridad, se establece lo que los usuarios pueden y no pueden hacer al usar los recursos informáticos, teniendo en cuenta que las operaciones están vinculadas con validación periódica, tipo de acceso, nivel de permisos, supervisión y auditoría.

Se debe tener claridad sobre el compromiso que se toma sobre la información, las normas, protocolos de conducta, el desarrollo de habilidades para reconocer evitar y defender de peligros, la protección de la información y la seguridad de la misma recae en las personas que la manejan, gestionan, transportan o acceden a ella así sea de forma accidental.

Por tal motivo se deben aplicar un conjunto de medidas eficaces y procedimentales con el objetivo de reducir al máximo los niveles de riesgo que comprometan la información por causa exclusiva del personal que accede a ella, ya sea de forma voluntaria, involuntaria, autorizada e inclusive sin autorización.

Por eso es de vital importancia establecer los niveles de responsabilidad sobre quién debe de velar por la custodia, y correcto manejo de la información clasificada para que asuman y cumplan sus obligaciones y responsabilidad al respecto.

Para hacer control de los procesos que se den en el sistema, se deben asignar personas responsables de supervisar y que incluya copias de seguridad, almacenamiento de datos e incluso verifique que las copias se hayan hecho perfectamente.

La autorización de seguridad del personal con acceso a información confidencial, se compromete a cumplir con los siguientes requisitos:

Conciencia de seguridad: implica que cada usuario conozca las obligaciones y los conceptos básicos del deber de reserva que se adquiere y las responsabilidades penales y disciplinarias que son de aplicación en caso de desacato, para tal efecto en Colombia se aplican las siguientes leyes:

- Ley 603 de 2000, la cual hace referencia a los derechos de autor.

- Ley 1273 de 2009: esta ley reforma el Código Penal, que establece un nuevo recurso jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

- Ley estatutaria 1266 de 2008: que modera las condiciones habituales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial: la financiera, crediticia, comercial, de servicios y la proveniente de terceros países, y se dictan otras disposiciones.

- Ley 1341 de 2009: Ley que aclara el reglamento y la concepción sobre la colectividad de la información y la estructura de las tecnologías TIC y crea la agencia nacional del espectro.

- Ley 1581 de 2012: reza que toda organismo público o privado, cuenta

con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva orden.

Instrucción de seguridad: proporciona el conocimiento detallado que precisa todo usuario de información clasificada para su manejo correcto, esta debe impartirse antes del primer acceso a la información confidencial y debe repetirse habitualmente.

Las personas que van a estar a cargo de custodiar la información confidencial se deben considerar con base en el grado de lealtad, honradez, fiabilidad e idoneidad, para esto se deben aplicar criterios que permitan determinar que no se encuentran inmerso en algunas de estas causales:

- Asociación, adscripción, afinidad, participación en grupos al margen de la ley conspiración ayuda o inducción a actos terrorista o sabotaje, espionaje o terrorismo.
- Existencia de dificultades financieras graves.
- La existencia de ingresos patrimoniales injustificados.
- Consumo de drogas ilegales.
- Abuso en el consumo de bebidas alcohólicas.
- Falta de lealtad, fiabilidad y honradez.
- Existencia de informes laborales que evidencien conductas conflictivas.
- Existencia de informes médicos que evidencien psicopatología con afectación al juicio de realidad o a la responsabilidad de sus actos.
- Existencia de evidencias de grado inasumible de estulticia que pudiera derivar en una vulnerabilidad personal.

Video

Para complementar el tema se recomienda ver:

Seguridad en los sistemas informáticos

https://vimeo.com/240863734

Seguridad en la red

Los elementos de la seguridad en la red, incluyen las precauciones que se toman para proteger tanto la información como la infraestructura tecnológica, al referirnos a la protección de la red, se hace énfasis en el acceso a Internet, puesto que es dentro de esta red de magnitud mundial que se generan con mayor frecuencia y facilidad diferentes ataques a toda clase de equipos.

El Internet ha ido avanzando y convirtiéndose en la actualidad en una de las herramientas y medios de comunicación más usados con la mayor cobertura, situación que implica también que cada vez, más usuarios están riesgo, el elemento básico de protección es el antivirus, seguido por los cortafuegos y las actualizaciones periódicas de seguridad

Actualmente los cibercriminales utilizan y crean distintas formas para atacar en línea, vulnerar accesos, robo de información, ataques de denegación de servicios, siendo los más frecuentes:

- Troyanos, gusanos y virus.
- Ataques de día cero (ataques de hora cero).
- Software espía y publicitario.
- Intercepción o robo de datos.
- Robo de identidad.
- Ataques de hackers.
- Ataques de denegación de servicios.

Seguridad en Sistemas Operativos

La seguridad en los sistemas operativos avala la solidez del entorno y el control en los recursos ya que los sistemas operativos son el ámbito físico en el que se efectúa la aplicación, cualquier debilidad en el sistema operativo puede comprometer a una o varias aplicaciones, los riesgos son múltiples, desde accesos en línea y terminales físicos, por ello, los desarrolladores de aplicaciones o de los sistemas operativos emiten actualizaciones con paquetes de seguridad integrando novedades en cuanto a seguridad y así prevenir tales ataques.

Figura 3. Seguridad.
Fuente: https://bit.ly/2PzXTVk

El sistema operativo

- Administra recursos.
- Coordina hardware.
- Regula archivos.
- Organiza directorios en dispositivos de almacenamiento.

Sin embargo, el sistema operativo no engloba todos los aspectos en cuanto a seguridad se trata, sólo cumple ciertas funciones de administrador.

La concepción que se tiene de la seguridad viene presentando cambios, ya que actualmente se es posible tener acceso remoto a los equipos, con lo que se busca que sea más fácil el desarrollo de los procesos, de igual forma, tales accesos deben cumplir con los estándares actuales y requerimientos de seguridad.

Seguridad en aplicaciones

Las aplicaciones suelen ser modelos de programas creados para efectuar funciones o como elementos para acciones básicas rápidas y de fácil empleo del usuario.

Resulta de gran importancia saber cómo usar funciones de seguridad para prevenir y minimizar amenazas, crear una aplicación segura requiere de estudiar y entender la vulnerabilidad de la misma, también es indispensable amoldarse con los medios que nos ofrece las herramientas.

Existen una serie de medidas de seguridad mínimas, que se deberían seguir y adaptar a todas las aplicaciones:

- Conocer a los usuarios.
- Tener acceso seguro a bases de datos.
- Mantener segura los datos confidenciales.
- Ejecutar aplicaciones con facultad mínima.
- Usar cookies de manera segura.
- Crear mensajes de error seguros, entre muchas otras.

Las aplicaciones permiten el acceso a los recursos centrales por parte de los usuarios, por tanto, se hace necesario adaptar las medidas de seguridad adecuadas, como: la protección de los recursos propios contra accesos no autorizados, instaurar la confidencialidad e integridad en datos para trabajar adecuadamente con un programa, limitar niveles de acceso por usuario y por función, tener garantía que el código de la aplicación se ejecute de la manera que se espera, tener adecuado control de cómo la aplicación consigue tener acceso a recursos restringidos.

Pese a que los procedimientos de seguridad de aplicaciones se pueden ver expuestos, por tanto, se deben:

- Establecer mecanismo para la detección de usuarios no autorizados.
- Realizar copias de seguridad para evitar pérdidas de información.
- Cerrar puertos.
- Desactivar servicios que no estén en uso.
- Comprobar entradas y salidas.
- Usar las funciones de registro de eventos de Windows.
- Crear contraseñas.
- Usar un firewall y antivirus.
- Instalar paquetes de actualizaciones de manera periódica.

Seguridad en los SGBD o Sistemas de Gestión de Bases de Datos

Su objetivo principal es proteger la información contra accesos no autorizados, garantizando la confidencialidad, confiabilidad e integridad de las bases de datos, teniendo en cuenta que la mayoría de los esquemas actuales operan en línea, facilitando el acceso a los usuarios, pero también generando espacios de vulnerabilidad.

Tipos de usuarios

- Administrador: DBA o administradores de bases de datos, son los gestores de establecer usuarios conceder autorización o permisos,
- Usuario con permisos para crear, borrar y modificar objetos y que además puede conceder privilegios a otros usuarios sobre los objetos que ha creado.
- Usuario con derecho a consultar, o actualizar, y sin derechos a crear o borrar objetos.
- Usuario anónimo: Puede existir o no dentro un sistema, sin embargo, el abanico de permisos es muy reducido, empleándose generalmente para efectos de lectura.

Lectura recomendada

Se invita al estudiante a realizar la siguiente lectura:

Avances en técnicas biométricas y sus aplicaciones en seguridad

León, S.

Medidas

Frente a las posibles situaciones de vulnerabilidad, el profesional de TI puede implementar una cantidad de medidas preventivas a fin de reducir la posibilidad y el impacto de un posible incidente.

Medidas de seguridad

- Físicas: establece quienes dominan el equipo.
- Personal: autoriza el personal que puede acceder a la BD.
- SO: establece las técnicas para la protección del sistema operativo.
- SGBD: aplica las herramientas que suministra el sistema gestor de bases de datos.

Herramientas de seguridad de la Base de Datos

- Control de acceso.
- Control de inferencia.
- Encriptado.
- Control de flujo.

Herramientas para el control de accesos

- Control de acceso discrecional: da garantía de exclusividad al usuario como acceder a archivos de información específica, acceder a registros para trabajar de manera determinada (*read, update, insert, o delete*)

- Control de acceso delegatorio: cataloga usuarios e información en varios niveles de seguridad.

Mecanismos para la seguridad

- Aplicar técnicas de cifrado en bases de datos distribuidas para la protección de la información.
- Los datos deben ser reconstruibles, ya que siempre pueden ocurrir accidentes.
- Los mecanismos de protección deben ser: simples, uniformes y construidos en las capas más básicas del sistema.
- Se deben emplear diferentes tipos de cuenta.
- Manipulación de la tabla con usuario y contraseña para tener un mejor control.
- Para el acceso emplea palabras claves.
- Sometidos a procesos de auditoría.
- El sistema debe diseñarse a prueba de intromisiones, no deben poder pasar por alto los controles.
- Ningún sistema puede evitar las intromisiones malintencionadas, pero es posible hacer que resulte muy difícil eludir los controles.
- El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas.
- Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.
- La base de datos debe ser protegida contra el fuego, el robo y otras formas de destrucción.

La fiabilidad del sistema

Hace referencia al grado de confianza que se tiene en relación a la protección y seguridad de los datos, teniendo como premisa que no existe un sistema 100% seguro.

El concepto de seguridad lo medimos en:

- La custodia del sistema frente ataques externos.
- La protección frente a caídas o fallos en el software o en el equipo.
- El cuidado frente a ejecución por parte de usuarios no autorizados.

Seguridad a cargo del SGBD

- Encriptado de datos: seguimiento de rastros (audit trail), datos ilegibles a menos que se conozca el código, si ingresan a la base de datos a que datos accedieron y que se hizo con ellos.

Seguridad a nivel de usuario SQL

- Cada uno de los usuarios posee un determinado nivel de permisos para acceder y manipular la información.

Los SGBD en el manejo de la base de datos permite el acceso a distintos usuarios de manera simultánea, permitiendo la actualización, consulta y modificación de la información.

Seguridad en Aplicaciones

La seguridad en aplicaciones hace posible la detección de problemas en una fase temprana del desarrollo, minimizando costos, ahorrando trabajo e incrementando la calidad de la aplicación final, así como mejorando la ejecución y el desempeño general.

Contiene varias herramientas para configurar un sistema seguro, desde: actualización típica, definición de virus, pasando por un escaneo de disco de alto nivel y otras posibilidades de configuración, se podría decir que uno de los puntos más frágiles de la seguridad son estas herramientas porque están interactuando de manera directa con los usuarios.

El aumento de aplicaciones que se están usando ha cambiado de manera radical el diseño del software, impulsando cada vez: una mayor flexibilidad, velocidad, originalidad e innovación al personal que conforma los equipos de desarrollo, programar aplicaciones seguras no es fácil, ya que, se pide al programador no solo el propósito básico de la aplicación, sino una idea general de los riesgos que puede correr la información al ser procesada y manejada cotidianamente.

No se debe olvidar que la tecnología y las aplicaciones avanzan y evolucionan al igual que los delitos cibernéticos, con lo que es necesario parches, actualizaciones de software, adquisición de nuevos productos tanto en software como hardware, ya que el desarrollo de aplicaciones abarca: la usabilidad, la utilidad y rapidez de ejecución, surge entonces poner al alcance de los usuarios aplicaciones seguras y las formas que existen para proteger los sistemas informáticos.

Figura 4. Elementos de la información
Fuente: http://www.agro.uba.ar/uti/servicios/seguridad_informacion

Instrucción

Se invita al estudiante a revisar el recurso de aprendizaje: infografía.

Protocolos de Seguridad en aplicaciones

A través de internet se operan gran cantidad de aplicaciones web, lo que lo convierte en uno de los lugares más inseguros, y a pesar de que se utilizan protocolos, algunos carecen de seguridad, lo que hace que la información esté expuesta, ya que los ciberdelincuentes interceptan con frecuencia información y descifran contraseñas, razón por la cual, aplicaciones que mandan contraseña cifrada por red son completamente vulnerables.

Los Protocolos de seguridad en cada aplicación, deben contener normas que minimicen los riesgos de la información que dicha aplicación suministra y todo lo necesario que permita un buen nivel de seguridad informática.

Actualmente, la seguridad en las aplicaciones y programas se ha convertido en un requerimiento fundamental, por tanto, se deben tener en cuenta los siguientes aspectos a fin de evitar vulnerabilidades al sistema.

La seguridad del sistema debe garantizar:

- Autenticidad: consiste en certificar un usuario dado por un directorio activo
- Confidencialidad: documento o archivo para que éste solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.
- Integridad: es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.
- Disponibilidad: capacidad de un servicio, de unos datos o de un sistema a ser accesible y utilizable por los usuarios o procesos autorizados cuando lo requiere.

Los protocolos de aplicaciones hacen viable la comunicación entre una aplicación y un servidor a la vez que dispone de la interacción entre el usuario y el servidor. Se fundamentan en: Abrir y cerrar, manejar e informar errores, hacer y satisfacer solicitudes de servicio.

Los protocolos más frecuentes de aplicación son:

- **Protocolo S-HTTP:** permite el cifrado de documentos y autenticación a través de firma y certificados digitales.
- **Protocolo SET:** se fundamenta en el uso de certificados digitales para asegurar la identificación de las partes que influyen en una transacción on-line fundamentado, en el uso de tarjetas de pago y en el uso de sistemas criptográficos de clave pública para dar protección al envío de datos entre los distintos servidores.
- ***Secure Socket Layer* SSL/TLS:** Son protocolos criptográficos que proporcionan comunicaciones seguras por una red, son parte necesaria de la seguridad de los sitios web, este protocolo cifra los datos que se envían como información sobre tarjetas de créditos, nombres y direcciones para que ningún atacante pueda accederlos.

Figura 5. Protocolo Secure Socket Layer SSL
Fuente: Propia.

- Transport Layer Security TLS: (seguridad de la capa de transporte) solo es una versión actualizada y más segura de SSL con la opción de cifrado.

Video

Para complementar el tema se recomienda ver:

Protocolos de seguridad

https://vimeo.com/240861566

Aplicaciones Web

Es una sección de la seguridad informática que se hace cargo de la seguridad en sitios, servicios y aplicaciones web.

Son herramientas que los usuarios suelen utilizar a través del acceso a un servidor web por medio de Internet o intranet mediante un navegador por lo que solo se necesitan los datos de acceso (nombre, contraseña), el significado de aplicaciones web está ligado al termino almacenamiento en la nube, ya que la información se guarda de manera permanente en servidores y facilita su acceso por medio de distintos dispositivos o equipos.

Algunos de los beneficios de las aplicaciones web son:

- Ahorrar tiempo.
- Comunicar.
- No ocupa espacio físico.
- Consume bajos recursos.
- Actualizaciones diarias.
- Puede ser colaborativa.
- Recurso de alta disponibilidad.
- Es portable.
- Es multiplataforma.

Existen aplicaciones web que se usan para:

- Enviar email.
- Encontrar lugares.
- Hacer llamadas de voz.
- Chatear.
- Hacer búsqueda en la red.
- Montar un negocio o tienda on-line.

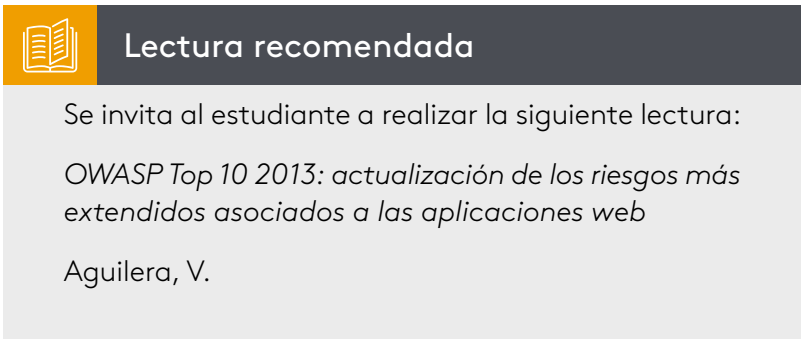
Las aplicaciones web son utilizadas para acceder a la información, generalmente se desarrollan como multiplataforma, lo que permite emplear cualquier dispositivo, sin tener relevancia el sistema operativo instalado, para tal efecto, sólo se requiere de un navegador, estas aplicaciones son creadas utilizando lenguajes para el desarrollo web, algunas de ellas son: HTML, CSS, JavaScript y frameworks como Sencha, Kendo UI, jquery Mobile, entre otros.

En las aplicaciones web hay ciertas ventajas como:

- Poder ser usadas por cualquier dispositivo sin interesarle el sistema operativo.
- No solicita aprobación para su publicación.
- El costo de desarrollo si se solicita ha de ser mínimo al compararlo con las nativas.
- Actualización.
- Compatibilidad multiplataforma.
- Comodidad al trabajar a distancia.
- La mayoría son gratuitas.

Y ciertas desventajas como:

- Se hace necesario internet.
- No usan los medios ni el dispositivo del sistema de forma perfecta.
- No poseen dominio para ser publicadas en plataformas para distribuirlas.
- Existe dependencia de Plugins.
- Pérdida a gran escala de los datos.



Aplicaciones Móviles

Las aplicaciones móviles o APP son parte de la nueva tendencia a la hora de manejar información personal y/o laboral, estas aplicaciones han sido creadas para efectuar distintas tareas y se pueden descargar en cualquier dispositivo móvil, es decir, es una tecnología al alcance de todos, pero no todas las aplicaciones móviles tienen las mismas propiedades, tampoco son del mismo tipo, ni sirven para todos los equipos móviles, se tendrá que utilizar una tienda virtual que permita la descarga de las aplicaciones compatibles con el sistema operativo instalado.

Existen diferentes tipos de aplicaciones como:

- Aplicaciones nativas.
- Aplicaciones web móviles.
- Aplicaciones híbridas.

Son muchas las alternativas que existen a la hora de diseñar una aplicación móvil, por lo que es conveniente revisar componentes, antes de obtener aplicaciones, todo para poseer lo mejor del servicio; se cuenta con tiendas que operan en línea como Apple, Microsoft, Android y BlackBerry en donde se encuentran aplicaciones para descargar e instalar, pero no todas las aplicaciones son gratuitas.

Día tras día hay más personas que desean crear nuevas aplicaciones que puedan ser usadas dentro de estos dispositivos (Tablet, telefonía inteligente, reproductor mp4, etc.) Para así capturar a más consumidores por medio de aplicaciones: atrayentes, portables, atractivas a la vista; que satisfagan una necesidad o problema, que permiten leer correos, navegar por internet, entretener, hacer búsqueda de productos, pagar cuentas, capacitarse, tener acceso a servicios o redes sociales, etc.

Instrucción

Se invita al estudiante a realizar la actividad de aprendizaje: control de lectura.

A continuación, se nombrarán algunas características básicas que debe poseer toda plataforma de seguridad móvil:

- Cifrado de almacenamiento.
- Reservar seguro de llaves criptográficas.
- Comprobación de la integridad del firmware.
- Protección por pérdida de dispositivo.
- Confirmación de la integridad del sistema.
- Protección contra aplicaciones maliciosas y llamadas críticas al sistema.

En cuanto a la Seguridad en las aplicaciones, actualmente se habla de que deben cumplir un principio básico en las TI, como son: Confidencialidad, Integridad y la Disponibilidad de la información, teniendo en cuenta que la información que contiene el desarrollo es más importante que la misma infraestructura.

Otro de los temas importantes para aplicar son las operaciones de seguridad en las aplicaciones, por lo que es un tema que debe tratarse dentro de la organización, ya que el acceso a internet es muy necesario porque se requiere ejecutar y desarrollar las actividades diarias de cada proceso.

En el desarrollo de aplicaciones, se deben contemplar algunas técnicas al momento de trabajar en la seguridad informática, a fin de garantizar que un sistema sea confiable y seguro:

- Revisión de código (Code Review).
- Análisis de riesgos en la arquitectura.
- Test de penetración.
- Test de seguridad basada en los riesgos.
- Casos de abuso.
- Requerimientos de seguridad.
- Operaciones de seguridad.
- Análisis externo.

Por esto se han creado herramientas de aplicación que permiten la protección de ataques que produzcan riesgos en las organizaciones.

Una de las soluciones que se ofrece en el mercado es IBM Application Security Services, esta herramienta ayuda a evaluar los requisitos de uso web actual y futuro, adicionalmente, proporciona un esquema de protección basado en capas, ha sido diseñada para afrontar las amenazas actuales de mayor complejidad.

Cierre:

Resulta evidente la importancia y utilidad de implementar técnicas y mecanismo en el desarrollo de aplicaciones, teniendo en cuenta que cada vez son más y más los servicios migrados a la nube, principalmente porque brindan una mayor versatilidad, facilidad de acceso y alcance a los mismos, sin embargo, se debe tener presente que constantemente existen personas intentando identificar y explotar las vulnerabilidades de un sistema informático.

Instrucción

Ahora se invita al estudiante a realizar la actividad evaluativa.

BIBLIOGRAFÍA

Carrasco, R. S. (2011). *Seguridad en Aplicaciones, Redes y Sistemas Informáticos*. México: Editorial Librería Bubok.

Díaz, V. (2014). *OWASP Top 10 2013*. Recuperado de https://www.isecauditors.com/sites/default/files/files/SIC106_OWASP-ISECA.pdf

Fisher, R. (2010). *Seguridad en los sistemas informáticos*. Madrid, España: Ediciones Díaz de Santos.

Costas, J. (2010). *Seguridad informática*. RA-MA S.A. Editorial y Publicaciones.

León, S. (2016). *Avances en técnicas biométricas y sus aplicaciones en seguridad*. Universidad de Carabobo. Valencia. Edo Carabobo, Venezuela: Recuperado de http://www.alfa-redi.org/sites/default/files/articles/files/leon.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica