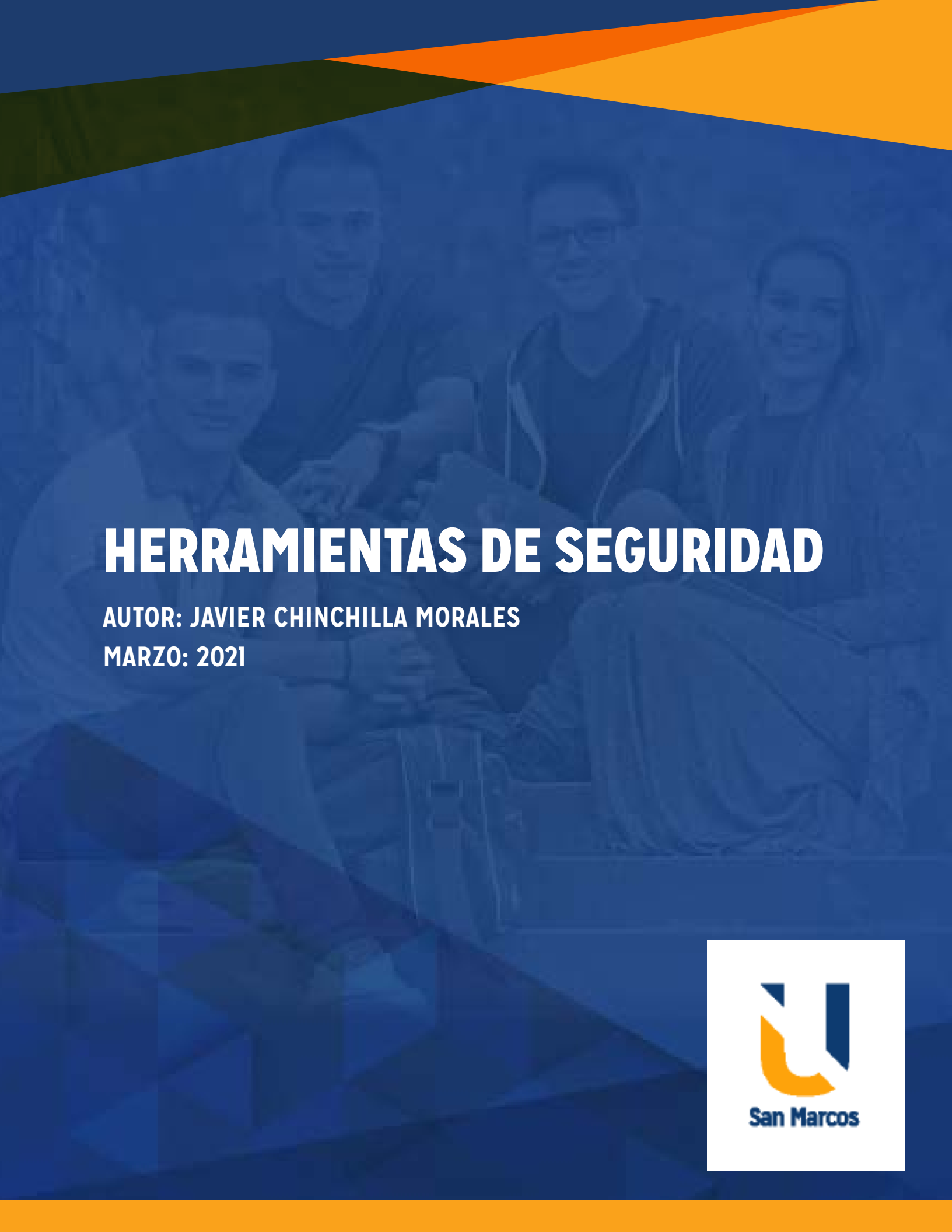

HERRAMIENTAS DE SEGURIDAD

AUTOR: JAVIER CHINCHILLA MORALES

MARZO: 2021

San Marcos

Tabla de contenido

Introducción

- Las amenazas de seguridad están continuamente evolucionando, por lo tanto las herramientas y tecnologías de seguridad para las redes no pueden quedarse estáticas, especialmente si su objetivo es analizar el *payload* o "contenido" de los paquetes de información y no el medio en que son transportados, considerando la existencia de amenazas como *bots*, *ramsomware*, *APTs* (*Advanced persistent threats*), *malware* o *spam* (Kennet T., 2013).

Herramientas de seguridad

La seguridad informática se define como la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. De acuerdo con el marco de gestión de COBIT las características con las que debe contar la información son:

- Eficacia: La información debe proporcionarse de una manera oportuna, correcta, consistente y utilizable.
- Eficiencia: Debe ser generada con un uso óptimo de recursos.
- Confidencialidad: Es necesario que se proteja la información sensitiva contra revelación no autorizada.
- Integridad: La información debe ser precisa y completa.
- Disponibilidad: Debe estar disponible cuando el negocio la necesite.
- Cumplimiento normativo: La organización, en el uso de la información, debe acatar aquellas leyes, reglamentos y acuerdos contractuales.
- Confiabilidad: Ha de proporcionarse la información apropiada para que la Dirección administre y ejercite sus responsabilidades de gobierno.

En seguridad informática, además de las características anteriores, es necesario cuidar ciertos aspectos como el control de acceso y la autenticación de un usuario o de una entidad o sitio en la red, la autenticación consiste en verificar los accesos, otra característica es la privacidad que se relaciona con la protección de identidad de los usuarios y sus actividades, otro concepto es la Seguridad en la comunicación lo cual indica que la información solo se transmitirá entre los puntos extremos autorizados, o sea controlar el tránsito de la información

Los tipos de seguridadinformática pueden calificarse en: externos, internos y electrónicos que son los provenientes de internet. En la actualidad, hay tantos tipos de seguridad informática como fuentes de amenaza existen para esa seguridad; por ello, se debe garantizar la seguridad informática tanto para los agentes externos e internos, así como para los agentes electrónicos o lógicos. Dentro de los agentes externos e internos, el factor humano juega un papel muy importante como amenaza.

Encriptación de los datos

La criptografía se define con el termino proviene del griego cripta que significa esconder o encubrir. La Real Academia Española (RAE) la define como un lugar subterráneo donde se enterraba a los muertos. Por extensión, la criptografía se define como el arte de escribir con claves secretas o de manera enigmática. Así, la criptología se considera un tratado acerca de los escritos secretos o cifrados, un criptograma es un documento cifrado y el criptoanálisis es el arte de descifrar criptogramas. Y todo esto lleva a esconder información al enviar el mensaje, para que el mismo no fuera interpretado por terceros, es un tema que tiene origenes en las antiguas guerras y hoy en día con mucha frecuencia requerimos pasar datos que son vitals como cuentas bancarias, entre otros y la información debe llevar un cifrado.

El protocolo IP seguro

Este protocolo IP va de la mano con la seguridad del protocolo de HTTP que en conjunto forman el HTTPS(protocolo de Transferencia de Hiper Texto), el cual es un protocolo que permite establecer una conexión segura entre el servidor y el cliente, que no puede ser interceptada por personas no autorizadas, aca lo que se hace es encriptar los datos para asegurar una transmisión de datos segura. Todo esto tiene sentido cuando un usuario hace clec en un enlace y aquí es donde el navegador establece una conexión, para lo cual el servidor presenta un certificado que lo autentica como un proveedro genuino y confiable, y una ez que el cliene ha verificado la autenticidad, envía una clave de sesión que sólo puede leer el servidor, normalmente se utiliza un certificado SSL.

La seguridad en las aplicaciones

La seguridad de las aplicaciones es el proceso de hacer que las aplicaciones sean más seguras al encontrar, corregir y mejorar su seguridad. Gran parte de esto sucede durante la fase de desarrollo, pero incluye herramientas y métodos para proteger las aplicaciones una vez que se implementan. Esto se está volviendo más importante a medida que, con cada vez más frecuencia, las aplicaciones son el objetivo de los ataques de los hackers.

La seguridad de las aplicaciones está recibiendo mucha atención. Existen cientos de herramientas disponibles para asegurar varios elementos de su cartera de aplicaciones, desde bloquear los cambios en la codificación hasta evaluar las amenazas de codificación involuntarias, evaluar las opciones de encriptación, así como los permisos de auditoría y los derechos de acceso. Existen herramientas especializadas para aplicaciones móviles, para aplicaciones basadas en la red y para firewalls diseñados especialmente para aplicaciones web.

El protocolo de seguridad SSL

El SSL (Secure Sockets layer o nivel de conectores seguros) fue el prococolo de cfrdo más utilizado para garantizar las comunicaciones a través de internes antes de ser sustituído por el TLS (Transport Layer Security o Seguridad de la capa de transporte). Aunque la mayoría de personas siguen refiriéndose a este tipo de tecnología como SSL.

El SSL proporciona un canal seguro entre dos computadoras o dispositivios que operan a través de internet o de una misma red. El SSL es compatible con los siguientes principios de seguridad:

- Cifrado: protege la transmisión de datos.
- Autenticación: garantiza que el servidor al que se conecta es, en efecto, el servidor correcto.
- Integridad de los datos: garantiza que los datos solicitados o enviados son realmente los datos legítimos.

La seguridad de la mensajería electrónica y de lo servidores de nombres

El Sistema de nombres de dominio (DNS por sus siglas en inglés) es uno de los componentes más necesarios para la funcionalidad de Internet. Muy a menudo, las empresas de Internet no actúan correctamente con la

seguridad de su identidad digital. Esta escasa seguridad del DNS lo hace vulnerable a muchos ciberataques que son beneficiosos para los atacantes. En este artículo vamos a hablar de qué riesgos existen y cómo podemos protegernos.
Recomendaciones para la seguridad del DNS

- Para minimizar la posibilidad de riesgo y vulnerabilidades, debemos parchear servidores DNS regularmente.
- Para determinar el túnel de DNS y la extorsión de datos existe un puerto UDP 53 que analizará el tráfico.
- Hay que asegurarse de que los servidores DNS tengan acceso restringido solo para las personas que lo requieran. Esto disminuiría las posibilidades de vulnerabilidades accidentales y la mala configuración maliciosa.
- Mantener servidores DNS distintos para la resolución interna y de Internet con el servidor interno detrás de las defensas de la red para que el acceso a los atacantes externos esté restringido.

La detección de intrusiones

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS (Instrusion Detection System o Sistema de detección de intrusiones) no solo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.
Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.
Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.
Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

El control de acceso

La definición mas generalizada para este tipo de control hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos, básicamente los encontramos en múltiples formas y para diversas aplicaciones, los mismos se clasifican en dos tipos: Sistemas de control de acceso autónomos y sistemas de control de acceso en red.

Protección y gestión de las infraestructuras de comunicación

Existen distintas formas para proteger la infranestructura las cuales son Seguridad física y la Seguridad lógica, en el primero de los tipos es importante tomar en cuenta los siguientes factores:

- Estricto control de accesos de personas y materiales.
- Instalación de cerraduras electrónicas mancomunadas en áreas críticas.
- Contar con diferentes tipos de detectores y equipo de alarmas conectados a una central externa y centro de monitoreo propio.

- Contar con equipo de videovigilancia distribuido de manera estratégica en zonas vulnerables o críticas.
- Contar con *software* analítico de vídeo que coadyuve en la detección preventiva de irregularidades en los protocolos de seguridad establecidos por la empresa.
- Complementar con personal de seguridad debidamente capacitado y entrenado.
- Desarrollar normas, políticas y procedimientos de seguridad específicos para este tipo de industria.
- Contar con un centro de monitoreo propio que valide de manera permanente la aplicación de los protocolos de seguridad de todas las personas que ingresan a las instalaciones y que además coordine acciones en caso de emergencia.
- Evaluar periódicamente los sistemas y procesos de seguridad mediante la ejecución de simulacros y auditorías.
- Establecer un esquema de denuncia confidencial para que el personal pueda reportar cualquier tipo de irregularidades que detecte.

En el Segundo tipo nos tenemos que encargar de la parte lógica la cual día con día es más preocupante dado que los Ciberataques comprometen la disponibilidad, integridad y confidencialidad de la información mediante accesos no autorizados, la modificación, degradación o destrucción de los sistema de información y Telecomunicaciones o incluso las infraestructuras que los soportan, acá las medidas a implementar son:

- Instaurar una cultura de ciberseguridad para todo el personal de la empresa, incluido el comité directivo.
- Determinar qué datos recauda la empresa y asegurarse de que la información sensible está debidamente protegida.
- Utilizar diversos métodos de autenticación.
- Habilitar el protocolo https en el sitio web.
- Actualizar de manera permanente todo el *software*.
- Realizar siempre un respaldo de seguridad de todos los datos.
- Contar siempre con un *firewall* para proteger la conexión a Internet.
- Desarrollar una estrategia de respuesta frente a incidentes.
- Certificar que los empleados buscan la S del protocolo https al navegar por Internet.
- Habilitar comunicaciones seguras a través de correo electrónico y ofrecer capacitación para mitigar los riesgos de sufrir ataques de *phishing*.
- Establecer pruebas de simulación de ataques de *phishing* para mantener alerta al personal.
- Formar un equipo de respuesta frente a incidentes.
- Elaborar periódicamente un análisis de amenazas internas y externas.
- Comunicar claramente a los empleados cómo responder frente a un incidente.
- Intercambiar información sobre buenas prácticas con otros colegas.
- Asumir en todo momento que existe una vulnerabilidad. No existe el riesgo cero.
- Asegurarse (mediante una póliza) de que la infraestructura de informática está cubierta frente a ciberataques.
- Comprobar que solamente es posible acceder a los sistemas tras un proceso de autenticación seguro.
- Contratar un servicio de *hacking* ético que verifique de manera preventiva las vulnerabilidades del sistema.
- Verificar las condiciones de seguridad del proveedor de servicios en la nube.

- Asegurarse de que la red está segmentada de forma que desde un sistema no sea posible acceder a otro.
- Mantenerse al día sobre las últimas normativas que rigen la industria.
- Continuar investigando las nuevas tecnologías y analizando nuevos proveedores.

Conclusiones y recomendaciones

Conocer qué herramientas existen en el mercado y como aplicarlas es uno de los principales objetivos de ese capítulo ya que la mismas son las que nos previenen de los ciberataques, lo cual va de la mano con la seguridad lógica de aplicaciones y además reforzar con el tema de seguridad física. Nunca es tarde para iniciar la revisión de la seguridad de los datos e instalaciones de una compañía para de ésta forma lograr brindarles a nuestros clientes el servicio y confidencialidad que requieren.

Referencias bibliográficas

- Corletti, A. (2017). *Ciberseguridad (una estrategia informático (militar).* www.darFe.es. Recuperado de https://www.slideshare.net/acorletti/libro-ciberseguridad-una-estrategia-informtico-militar?from_action=save
- Salas, A. (2015). *Los hombres que susurran a las máquinas*. Espasa Libros, S. L. U. Recuperado de https://www.planetadelibros.com/libros_contenido_extra/32/31258_1_PREFACIO_Los_hombres_que_susurran_a_las_maquinas.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica