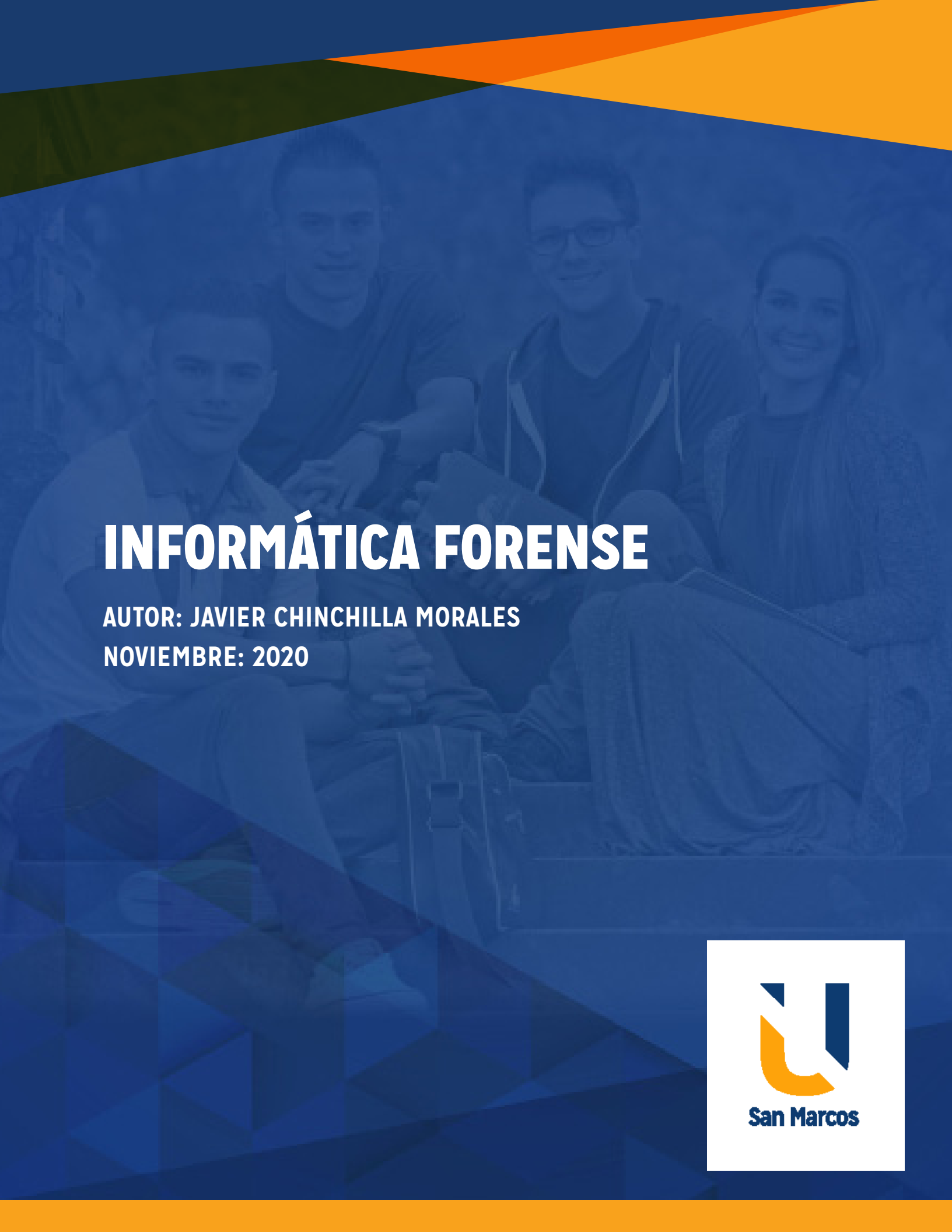

INFORMÁTICA FORENSE

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

Introducción

La Informática forense consiste en la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean validos dentro de un proceso legal.

Incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Esta técnica ayuda a encontrar pistas sobre ataques informáticos, robo de información conversaciones o pistas de emails y chats.

Tabla de contenido

La seguridad y los aspectos legales

La seguridad en la empresa - La red

Impulso Tecnológico recomienda una estrategia de seguridad de redes multi-capa a partir de una Defensa en Profundidad. Podemos ver algunos aspectos a tener en cuenta en una auditoria de seguridad de redes informaticas.

- Bloqueo de ataques basados en la red local
  - Ejemplos: cortafuegos, antivirus para gateways (puertas de enlace), correo electrónico seguro, protección contra el spam, filtrado seguro de contenido web, detección y prevención de intrusiones
- Bloqueo de ataques basados en equipo local
  - Ejemplos: antivirus personal, cortafuegos personal, eliminación de spyware, prevención de intrusiones en el equipo local
- Eliminación de vulnerabilidades de seguridad
  - Ejemplos: gestión de la configuración de parches de seguridad, gestión de vulnerabilidades y pruebas de penetración
- Soporte seguro a usuarios autorizados
  - Ejemplos: contraseñas seguras, VPN, acceso remoto seguro, cifrado de archivos, acceso y gestión de ID

Herramientas para minimizar las pérdidas de negocio y maximizar la eficacia
Ejemplos: copias de seguridad, administración de registros, herramientas de cumplimiento de normativas
Cada capa de recomendaciones de seguridad de redes se basa en la anterior y si una capa es “omitida”, entonces su empresa es vulnerable y está en riesgo. Lo ideal sería que la empresa implementara cada una de estas capas para tener una red y un entorno informático seguro, sin embargo, puede tener un costo prohibitivo y siempre hay que usar el sentido común para cada empresa.
Impulso Tecnoógico puede ayudarle a determinar la mejor estrategia de seguridad de redes informaticas para su empresa que reduzca al mínimo los riesgos para sus datos, redes y usuarios.

Generalidades sobre la seguridad en las redes

La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red. Los usuarios eligen o se les asigna una identificación y contraseña u otra información de autenticación que les permite acceder a información y programas dentro de sus autorizaciones. La seguridad de red cubre una variedad de redes de computadoras, tanto públicas como privadas, que se usan en trabajos cotidianos; realizar transacciones y comunicaciones entre empresas, agencias gubernamentales e individuos. Las redes pueden ser privadas, como dentro de una empresa, y otras que pueden estar abiertas al público. La seguridad de la redes está presente en organizaciones, empresas y otros tipos de instituciones. Hace como su nombre indica: protege la red, además de proteger y supervisar las operaciones que se realizan. La forma más común y simple de proteger un recurso de red es asignándole un nombre único y la contraseña correspondiente.

Introducción a la tecnología firewall

Básicamente un-Firewall, también conocido como “cortafuegos”, es un sistema de seguridad incluido en todos los sistemas operativos, pero que sin embargo también puede ser obtenido de otro fabricante, es decir

de terceros desarrolladores, y que nos permite bloquear o permitir las conexiones que entran o que salen de nuestra computadora en forma manual o automática.
Un firewall o cortafuegos es un dispositivo de hardware o un software que nos permite gestionar y filtrar la totalidad de trafico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.
Si el tráfico entrante o saliente cumple con una serie de Reglas que nosotros podemos especificar, entonces el tráfico podrá acceder o salir de nuestra red u ordenador sin restricción alguna. En caso de no cumplir las reglas el tráfico entrante o saliente será bloqueado.
Por lo tanto a partir de la definición podemos asegurar que con un firewall bien configurado podemos evitar intrusiones no deseadas en nuestra red y ordenador así como también bloquear cierto tipo de tráfico saliente de nuestro ordenador o nuestra red.

Las funcionalidades del firewall

El firewall normalmente se encuentra en el punto de unión entre 2 redes, así mismo también vemos que cada una de las subredes dentro de nuestra red puede tener otro firewall, y cada uno de los equipos a la vez puede tener su propio firewall por software. De esta forma, en caso de ataques podemos limitar las consecuencias ya que podremos evitar que los daños de una subred se propaguen a la otra. Lo primero que tenemos que saber para conocer el funcionamiento de un firewall es que la totalidad de información y tráfico que pasa por nuestro router y que se transmite entre redes es analizado por cada uno de los firewalls presentes en nuestra red. Si el tráfico cumple con las reglas que se han configurado en los firewalls el trafico podrá entrar o salir de nuestra red.

Los diferentes tipos de cortafuegos

Los diferentes tipos de firewall son de software y hardware, los cuales es importante destacar que el primero de ellos es mas barato, por lo cual las empresas pequeñas o personales suelen instalar de éste tipo, el mismo debe ser instalado directamente en cada una de las computadoras, en el caso del Segundo tenemos que es una caja que se coloca entre el router y una computadora o una red y lo que hace es que oculta la computadora de un usuario ante la red de internet. La mejor protección con firewall es instalar ambos tipos: el firewall de software y el firewall de hardware.

Elección de un dispositivo de firewall para la empresa

Gran parte de la decisión depende de las circunstancias y necesidad más comunes. Los usuarios de desktop, cuyas computadoras raramente cambian de red, van a ser atendidos por un firewall de hardware. Éste ofrece la configuración más fácil, combinandolo con la mayor flexibilidad. Notebooks y laptops, especialmente de usuarios que hacen desplazamiento con frecuencia, van a necesitar de un software de firewall para garantizar la protección, dónde quiera que vayan. Una posible opción también es mezclar ambas: optar por un firewall de hardware cuando usted esté trabajando en una red doméstica o en la oficina y un software de firewall cuando esté en movimiento.

La política de configuración del firewall

En un firewall se define por medio de una política de reglas, qué tipo de tráfico se permite en una red y en el que podemos indicar el tipo de conexión autorizada, definiendo los protocolos, puertos y las direcciones IP

permitidas. Con ello podemos decir que encontramos que las políticas tienen una serie de reglas y en cada una se han definido los siguientes valores:

- Protocolo: el protocolo de red.
- Puerto desde: El número de puerto desde el cual aplica esta regla.
- Puerto hasta: El número de puerto hasta el cual aplica esta regla.
- Dirección IP permitida: Si es una, varias o todas las direcciones IP desde las que se permite el acceso.

Esos datos son importantes, porque definen nuestra regla de manera conjunta y son los que usaremos más adelante para crear nuestras propias políticas.

Conclusiones y recomendaciones

En cuanto al tema de seguridad física y lógica de las redes, hemos logrado comprender el Soporte que nos brindan los firewalls y como es que los mismos se rigen bajo el modelo de estandar implentado por las capas del modelo OSI y con ello se ven los tipos de cortafuegos que existen y las recomendaciones que se nos hacen para aplicarlas a nivel físico como es la seguridad de las redes, edificios, datos entre otros, se recomienda incursionar en la investigación de temas que se han visto muy superficialmente como son las normas ISO.

Referencias bibliográficas

- Carpentier, J. (2016). *La seguridad informática* en la PYME. Editorial ENI.
- Cañon, L. (2015). *Ataques Informáticos Ethical Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado).* Universidad Piloto, Colombia.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica