

Tecnológico Nacional de México

Instituto Tecnológico de Reynosa



Equipo conformado por:

Bermudez Dominguez Juan Carlos 19580585  
Castillo Jr Gregorio 19580589

Flores Acosta Sheila Lizeth 19580595

Morales Calixto Daniel Alexander 19580867

Gongora Raga Perla Elizabeth 19580603

Perez Romero Julio Alberto 19580633

La seguridad informática

# Índice

[Índice 1](#_Toc133441591)

[3.1 Conceptos básicos 2](#_Toc133441592)

[3.2 Tipos de ataques 18](#_Toc133441593)

[3.3 Creación del plan, procedimientos y políticas de seguridad 27](#_Toc133441594)

[3.4 Evaluación de riesgos 32](#_Toc133441595)

[3.4.1 Activos a proteger 32](#_Toc133441596)

[3.4.2 Amenazas contra las que se tiene que proteger 35](#_Toc133441597)

[3.4.3 Protección legal 43](#_Toc133441598)

[Bibliografía 47](#_Toc133441599)

# 3.1 Conceptos básicos

3.1. Conceptos básicos.

Una forma de mejorar la habilidad de un sistema de defensa contra intrusos y programas maliciosos, es implementar tecnología de Sistemas Confiables (Trusted

Systems).

La seguridad informática consiste en asegurar que los recursos del sistema de información (Material informático o programa) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

CIDAN

Actualmente se considera aceptado que la seguridad de los datos y de la información comprende 5 aspectos fundamentales:

Confidencialidad: Es decir, no desvelar datos a usuarios no autorizados. Esto comprende también la privacidad (Protección de datos personales).

Integridad: Permite asegurar que los datos no sean falseados.

Disponibilidad: Que la información se encuentre accesible en todo momento a los usuarios autorizados.

Autenticación: Es la situación en la cuál se puede verificar que un documento ha sido elaborado o pertenece a quien el documento dice.

No repudio: Permite probar las partes en una comunicación frente a un tercero. También se puede llamar irrenunciabilidad.

Gómez (2006) define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software.

Kissel (2012) la define como la protección de información y sistemas de información de acceso no autorizado. En efecto, con base en estos conceptos, la seguridad informática se vincula con tres elementos básicos: la información que, como activo intangible, representa quizá el elemento más sensible y vulnerable; el software, cuya pérdida o modificación mal intencionada puede representar severos quebrantos económicos u operativos no solo hacia el usuario sino a toda una institución; y el hardware, que al fallar provoca retrasos en la operación diaria y la consecuente pérdida de tiempo y costos elevados.

Existe un sin número de medidas preventivas que permiten prote­ger estos tres elementos, como respaldos de informaci6n (backups), controles de acceso de hardware y software, programas antivirus, an­tispyware y antispam, uso de firewalls, actualizaciones continuas al sistema operativo, mantenimiento al equipo de c6mputo y protección física en las áreas de operaciones de red (extintores, detectores de humo y calor, sistemas de anclaje, ventilaci6n, controles de tempera­tura y humedad, reguladores de voltaje, sistemas de suministro conti­nuo de energía, entre otros).

Sin embargo, para un usuario, la protección de su información es generalmente más importante que la protección misma del software o su equipo, razón por la cual, para garantizar la seguridad de los datos, es precise cumplir con tres componentes fundamentales: integridad, que significa que la información debe ser modificada solo por entida­des autorizadas; disponibilidad, es decir, tener acceso a la información cuando se lo requiera; y confidencialidad, donde solo instancias facultadas para ello podrán visualizar los datos.

Debido a la importancia que ha ido adquiriendo la seguridad en cómputo, en las siguientes ediciones de cápsulas TI se abordarán en detalle recomendaciones diversas que permitan evitar posibles pérdidas de datos, robos de información, accesos no autorizados, suplan­tación de identidad, presencia de malware, entre otros.

Para conseguir los objetivos enumerados anteriormente, 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.

Realización de copias de seguridad e imágenes de respaldo.

Antivirus.

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.

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.

Conjunto de leyes encaminadas a la protección de datos personales que obligan a las empresas a asegurar su confidencialidad.

¿Qué es “network security” o la seguridad en la red (servicios digitales en Internet)?

Definimos la seguridad de información como la protección de ventajas de información de la revelación no autorizada, de la modificación, o de la destrucción, o accidental o intencional, o la incapacidad para procesar esa información. La seguridad de la red, se compone de esas medidas tomadas para proteger una red del acceso no autorizado, interferencia accidental o intencionada con operaciones normales, o con la destrucción, inclusive la protección de facilidades físicas, del software, y de la seguridad del personal. La seguridad en el Web es un conjunto de procedimientos, prácticas y tecnologías para proteger a los servidores y usuarios del Web y las organizaciones que los rodean. La Seguridad es una protección contra el comportamiento inesperado [Garfinkel, 1999].

¿Por qué requiere atención especial la seguridad en el Web?

Internet es una red de dos sentidos. Así como hace posible que los servidores Web divulguen información a millones de usuarios, permite a los hackers, crackers, criminales y otros “chicos malos” irrumpir en las mismas computadoras donde se ejecutan los servidores Web.

Las empresas, instituciones y los gobiernos utilizan cada vez más el Word Wide Web para distribuir información importante y realizar transacciones comerciales. Al violar servidores Web se pueden dañar reputaciones y perder dinero.

Aunque el Web es fácil de utilizar, los servidores son piezas de software extremadamente complicadas y tienen diversas fallas de seguridad potenciales.

Es mucho más onerosa y tardada la recuperación de un incidente de seguridad que implementar medidas preventivas.

Por qué preocuparse sobre la seguridad en el Web?

Los servidores son un blanco atractivo para los trangesores por varias razones [Garfinkel, 1999]:

Publicidad. Los servidores web son la cara que las organizaciones presentan al público y al mundo electrónico. Un ataque exitoso a alguno de ellos es acto público que puede ser visto en unas horas por cientos de miles de personas. Los ataques pueden lanzarse por razones ideológicas o financieras, o ser simples actos vandálicos cometidos al azar.

Comercio. Muchos servidores web están relacionados con el comercio y el dinero. De hecho, los protocolos criptográficos integrados a Navegador de Netscape y otros navegadores fueron originalmente incluidos para permitir a los usuarios enviar números de tarjetas de crédito por Internet sin preocuparse de que fueran interceptados. De esta forma, los servidores web se han convertido en repositorios de información financiera confidencial, lo cual los convierte en un blanco atractivo para los atacantes. Información confidencial. Para las organizaciones, la tecnología del Web se ha convertido en una forma de distribuir información con gran sencillez, tanto internamente, a sus propios miembros, como de manera externa, a sus socios en todo el mundo. Esta información confidencial es un blanco atractivo para sus competidores y enemigos.

Acceso a las redes. Al ser utilizados por personas tanto dentro como fuera de las organizaciones, los servidores web sirven efectivamente como puente entre la red interna de la organización y las redes externas. Su posición privilegiada en cuanto a las conexiones de red los convierte en un blanco ideal para ser atacados, ya que un servidor web violado puede emplearse como base para atacar desde ahí a las computadoras de una organización.

Extensibilidad de los servidores. Debido a su naturaleza, los servidores están diseñados para ser extensibles, lo cual hace posible conectarlos con bases de datos, sistemas heredados y otros programas que se ejecutan en la red de una organización. Si no se implementan de modo adecuado, los módulos que se agregan a un servidor pueden comprometer la seguridad de todo el sistema.

Interrupción del servicio. Como la tecnología del Web se basa en la familia de protocolos TCP/IP, está sujeta a interrupciones del servicio: ya sea accidental o intencionalmente por medio de ataques de negación del servicio. Las personas que utilizan dichas tecnologías den estar enteradas de sus fallas y prepararse para interrupciones importantes del servicio.

Soporte complicado. Los navegadores necesitan servicios internos, como DNS (Servicio de nombres de Dominio, Domain Name Service) y el enrutamiento del protocolo IP (Protocolo Interne, Internet Protocol) para funcionar bien. La robustez y confiabilidad de tales servicios pueden ser desconocidas y vulnerables a errores de programación, accidentes y subversión, la subversión de un servicio de mas bajo nivel puede causar problemas también a los navegadores.

Objetivos de la Seguridad.

Seguridad informática es el conjunto de procedimientos, estrategias y herramientas que permitan garantizar la integridad, la disponibilidad y la confidencialidad de la información de una entidad.

Integridad. Es necesario asegurar que los datos no sufran cambios no autorizados, la pérdida de integridad puede acabar en fraudes, decisiones erróneas o como paso a otros ataques. El sistema contiene información que debe ser protegida de modificaciones imprevistas, no autorizas o accidentales, como información de censo o sistemas de transacciones financieras.

Disponibilidad. Se refiere a la continuidad operativa de la entidad, la pérdida de disponibilidad puede implicar, la pérdida de productividad o de credibilidad de la entidad. El sistema contiene información o proporciona servicios que deben estar disponibles a tiempo para satisfacer requisitos o evitar pérdidas importantes, como sistemas esenciales de seguridad y protección de la vida.

Confidencialidad. Se refiere a la protección de datos frente a la difusión no autorizada, la pérdida de confidencialidad puede resultar en problemas legales, pérdida del negocio o de credibilidad. El sistema contiene información que necesita protección contra la divulgación no autorizada, como información parcial de informes, información personal o información comercial patentada.

Estrategias de Seguridad.

La metodología de seguridad está diseñada para ayudar a los profesionales de la seguridad a desarrollar una estrategia para proteger la disponibilidad, integridad y confidencialidad de los datos de los sistemas informáticos (IT) de las organizaciones. Es de interés para los administradores de recursos de información, los directores de seguridad informática y los administradores, y tiene un valor especial para todos aquellos que intentan establecer directivas de seguridad. La metodología ofrece un acercamiento sistemático a esta importante tarea y, como precaución final, también implica el establecimiento de planes de contingencia en caso de desastre. Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados.

Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada sistema informático, entorno y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos. Sin embargo, los fundamentos de una buena seguridad siguen siendo los mismos y este proyecto se centra en dichos principios [Benson, 2001].

Identificar métodos, herramientas y técnicas de ataques probables. Las listas de amenazas, de las que disponen la mayor de las organizaciones, ayudan a los administradores de seguridad a identificar los distintos métodos, herramientas y técnicas de ataque que se pueden utilizar en los ataques. Los métodos pueden abarcar desde virus y gusanos a la adivinación de contraseñas y la interceptación del correo electrónico. Es importante que los administradores actualicen constantemente sus conocimientos en esta área, ya que los nuevos métodos, herramientas y técnicas para sortear las medidas de seguridad evolucionan de forma continua.

Establecer estrategias proactivas y reactivas. En cada método, el plan de seguridad debe incluir una estrategia proactiva y otra reactiva. La estrategia proactiva o de previsión de ataques es un conjunto de pasos que ayuda a reducir al mínimo la cantidad de puntos vulnerables existentes en las directivas de seguridad y a desarrollar planes de contingencia. La determinación del daño que un ataque va a provocar en un sistema y las debilidades y puntos vulnerables explotados durante este ataque ayudará a desarrollar la estrategia proactiva. La estrategia reactiva o estrategia posterior al ataque ayuda al personal de seguridad a evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, a documentar y aprender de la experiencia, y a conseguir que las funciones comerciales se normalicen lo antes posible.

Pruebas. El último elemento de las estrategias de seguridad, las pruebas y el estudio de sus resultados, se lleva a cabo después de que se han puesto en marcha las estrategias reactiva y proactiva. La realización de ataques simulados en sistemas de pruebas o en laboratorios permite evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia. Estas pruebas no se deben llevar a cabo en los sistemas de producción real, ya que el resultado puede ser desastroso Si es posible, se deben probar físicamente y documentar todos los casos de ataque para determinar las mejores directivas y controles de seguridad posibles que se van a implementar.

Equipos de respuestas a incidentes. Es aconsejable formar un equipo de respuesta a incidentes. Este equipo debe estar implicado en los trabajos proactivos del profesional de la seguridad. Entre éstos se incluyen:

El desarrollo de instrucciones para controlar incidentes.

La identificación de las herramientas de software para responder a incidentes y eventos.

La investigación y desarrollo de otras herramientas de seguridad informática.

La realización de actividades formativas y de motivación.

La realización de investigaciones acerca de virus.

La ejecución de estudios relativos a ataques al sistema.

Metodología para la definición de una estrategia de seguridad [Benson, 2001].

Predecir posibles ataques y analizar riesgos. La primera fase es determinar los ataques que se pueden esperar y las formas de defenderse contra ellos. Es imposible estar preparado contra todos los ataques; por lo tanto, hay que prepararse para los que tiene más probabilidad de sufrir la organización. Siempre es mejor prevenir o aminorar los ataques que reparar el daño que han causado. Para mitigar los ataques es necesario conocer las distintas amenazas que ponen en peligro los sistemas, las técnicas correspondientes que se pueden utilizar para comprometer los controles de seguridad y los puntos vulnerables que existen en las directivas de seguridad. El conocimiento de estos tres elementos de los ataques ayuda a predecir su aparición e, incluso, su duración o ubicación. La predicción de los ataques trata de pronosticar su probabilidad, lo que depende del conocimiento de sus distintos aspectos. Los diferentes aspectos de un ataque se pueden mostrar en la siguiente ecuación:

Amenazas + Motivos + Herramientas y técnicas + Puntos vulnerables = Ataque

Para cada tipo de amenaza, Considere todas las amenazas posibles que causan ataques en los sistemas. Entre éstas se incluyen los agresores malintencionados, las amenazas no intencionadas y los desastres naturales. Amenazas como empleados ignorantes o descuidados, y los desastres naturales no implican motivos u objetivos; por lo tanto, no se utilizan métodos, herramientas o técnicas predeterminadas para iniciar los ataques. Casi todos estos ataques o infiltraciones en la seguridad se generan internamente; raras veces los va a iniciar alguien ajeno a la organización.

Para cada tipo de método de ataque. Para iniciar un ataque, se necesita un método, una herramienta o una técnica para explotar los distintos puntos vulnerables de los sistemas, de las directivas de seguridad y de los controles. Los agresores pueden utilizar varios métodos para iniciar el mismo ataque. Por lo tanto, la estrategia defensiva debe personalizarse para cada tipo de método utilizado en cada tipo de amenaza. De nuevo, es importante que los profesionales de la seguridad estén al día en los diferentes métodos, herramientas y técnicas que utilizan los agresores. La siguiente es una lista breve de esta técnica:

Ataques de denegación de servicio.

Ataques de invasión.

Ingeniería social.

Virus.

Gusanos.

Caballos de Troya.

Modificación de paquetes.

Adivinación de contraseñas.

Interceptación de correo electrónico.

Estrategia proactiva. La estrategia proactiva es un conjunto de pasos predefinidos que deben seguirse para evitar ataques antes de que ocurran. Entre estos pasos se incluye observar cómo podría afectar o dañar el sistema, y los puntos vulnerables. Los conocimientos adquiridos en estas evaluaciones pueden ayudar a implementar las directivas de seguridad que controlarán o aminorarán los ataques. Éstos son los tres pasos de la estrategia proactiva:

Determinar el daño que causará el ataque.

Establecer los puntos vulnerables y las debilidades que explotará el ataque.

Reducir los puntos vulnerables y las debilidades que se ha determinado en el sistema para ese tipo de ataque específico.

El seguimiento de estos pasos para analizar los distintos tipos de ataques tiene una ventaja adicional: comenzará a emerger un modelo, ya que en los diferentes factores se superponen para diferentes ataques.

Determinar el daño posible que puede causar un ataque. Los daños posibles pueden oscilar entre pequeños fallos del equipo y la pérdida, catastrófica, de los datos. El daño causado al sistema dependerá del tipo de ataque. Si es posible, utilice un entorno de prueba o de laboratorio para clarificar los daños que provocan los diferentes tipos de ataques. Ello permitirá al personal de seguridad ver el daño físico que causan los ataques experimentales. No todos los ataques causan el mismo daño

Determinar los puntos vulnerables o las debilidades que pueden explotar los ataques. Si se pueden descubrir los puntos vulnerables que explota un ataque específico, se pueden modificar las directivas y los controles de seguridad actuales o implementar otras nuevas para reducir estos puntos vulnerables. La determinación del tipo de ataque, amenaza y método facilita el descubrimiento de los puntos vulnerables existentes. Esto se puede reconocer por medio de una prueba real. Se deben determinar los puntos vulnerables o debilidades en las áreas de seguridad física, de datos y de red.

Reducir los puntos vulnerables y debilidades que puede explotar un posible ataque. La reducción de los puntos vulnerables y las debilidades del sistema de seguridad que se determinaron en la evaluación anterior es el primer paso para desarrollar directivas y controles de seguridad eficaces. Mediante la reducción de los puntos vulnerables, el personal de seguridad puede hacer disminuir tanto la probabilidad de un ataque como su eficacia, si se produce alguno. Tenga cuidado de no implementar controles demasiado estrictos, ya que la disponibilidad de la información se convertiría en un problema. Debe haber un cuidado equilibrio entre los controles de seguridad y el acceso a la información.

Elaborar planes de contingencia. Un plan de contingencia es un plan alternativo que debe desarrollarse en caso de que algún ataque penetre en el sistema y dañe los datos o cualquier otro activo, detenga las operaciones comerciales habituales y reste productividad. El plan se sigue si el sistema no se puede restaurar a tiempo. Su objetivo final es mantener la disponibilidad, integridad y confidencialidad de los datos (es el proverbial "Plan B"). Debe haber un plan para cada tipo de ataque y tipo de amenaza. Cada plan consta de un conjunto de pasos que se han de emprender en el caso de que un ataque logre pasar las directivas de seguridad.

Estrategia reactiva. La estrategia reactiva se implementa cuando ha fallado la estrategia proactiva y define los pasos que deben adoptarse después o durante un ataque. Ayuda a identificar el daño causado y los puntos vulnerables que se explotaron en el ataque, a determinar por qué tuvo lugar, a reparar el daño que causó y a implementar un plan de contingencia, si existe. Tanto la estrategia reactiva como la proactiva funcionan conjuntamente para desarrollar directivas y controles de seguridad con el fin de reducir los ataques y el daño que causan. El equipo de respuesta a incidentes debe incluirse en los pasos adoptados durante o después del ataque para ayudar a evaluarlo, a documentar el evento y a aprender de él.

Evaluar el daño. Determine el daño causado durante el ataque. Esto debe hacerse lo antes posible para que puedan comenzar las operaciones de restauración. Si no se puede evaluar el daño a tiempo, debe implementarse un plan de contingencia para que puedan proseguir las operaciones comerciales y la productividad normales.

Determinar la causa del daño. Para determinar la causa del daño, es necesario saber a qué recursos iba dirigido el ataque y qué puntos vulnerables se explotaron para obtener acceso o perturbar los servicios. Revise los registros del sistema, los registros de auditoría y las pistas de auditoría. Estas revisiones suelen ayudar a descubrir el lugar del sistema en el que se originó el ataque y qué otros recursos resultaron afectados.

Reparar el daño. Es muy importante que el daño se repare lo antes posible para restaurar las operaciones comerciales normales y todos los datos perdidos durante el ataque. Los planes y procedimientos para la recuperación de desastres de la organización (que se tratan en el documento acerca del diseño de la seguridad) deben cubrir la estrategia de restauración.

Documentar y aprender. Es importante documentar el ataque una vez que se ha producido. La documentación debe abarcar todos los aspectos que se conozcan del mismo, entre los que se incluyen el daño que ha causado (en hardware y software, pérdida de datos o pérdida de productividad), los puntos vulnerables y las debilidades que se explotaron durante el ataque, la cantidad de tiempo de producción perdido y los procedimientos tomados para reparar el daño. La documentación ayudará a modificar las estrategias proactivas para evitar ataques futuros o mermar los daños.

Implementar un plan de contingencia. Si ya existe algún plan de contingencia, se puede implementar para ahorrar tiempo y mantener el buen funcionamiento de las operaciones comerciales. Si no hay ningún plan de contingencia, desarrolle un plan apropiado basado de la documentación del paso anterior.

Revisar el resultado y hacer simulaciones. Tras el ataque o tras defenderse de él, revise su resultado con respecto al sistema. La revisión debe incluir la pérdida de productividad, la pérdida de datos o de hardware, y el tiempo que se tarda en recuperarlos. Documente también el ataque y, si es posible, haga un seguimiento del lugar en el que se originó, qué métodos se utilizaron para iniciarlo y qué puntos vulnerables se explotaron. Para obtener los mejores resultados posibles, realice simulaciones en un entorno de prueba.

Revisar la eficacia de las directivas. Si hay directivas para defenderse de un ataque que se ha producido, hay que revisar y comprobar su eficacia. Si no hay directivas, se deben redactar para aminorar o impedir ataques futuros.

Ajustar las directivas en consecuencia. Si la eficacia de la directiva no llega al estándar, hay que ajustarla en consecuencia. Las actualizaciones de las directivas debe realizarlas el personal directivo relevante, los responsables de seguridad, los administradores y el equipo de respuesta a incidentes. Todas las directivas deben seguir las reglas e instrucciones generales de la organización.

Amenazas a la seguridad de la información.

Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos. Contra cualquiera de los tres elementos dichos anteriormente (pero principalmente sobre los datos) se pueden realizar multitud de ataques o, dicho de otra forma, están expuestos a diferentes amenazas. Generalmente, la taxonomía más elemental de estas amenazas las divide en cuatro grandes grupos: interrupción, interceptación, modificación y fabricación. Un ataque se clasifica como interrupción si hace que un objeto del sistema se pierda, quede inutilizable o no disponible. Se tratará de una interceptación si un elemento no autorizado consigue un acceso a un determinado objeto del sistema, y de una modificación si además de conseguir el acceso consigue modificar el objeto; algunos autores [Olovsson, 1992] consideran un caso especial de la modificación: la destrucción, entendiéndola como una modificación que inutiliza al objeto afectado. Por último, se dice que un ataque es una fabricación si se trata de una modificación destinada a conseguir un objeto similar al atacado de forma que sea difícil distinguir entre el objeto original y el “fabricado”.

Se presenta una relación de los elementos que potencialmente pueden amenazar a nuestro sistema. No pretende ser exhaustiva, ni por supuesto una taxonomía formal (para este tipo de estudios, se recomienda consultar [Landwher, 1994][Aslam, 1996]); simplemente trata de proporcionar una idea acerca de qué o quién amenaza un sistema.

Personas. No podernos engañarnos, la mayoría de ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o inintencionadamente, pueden causarnos enormes pérdidas Se listan los diferentes tipos de personas que de una u otra forma pueden constituir un riesgo para nuestros sistemas; generalmente se dividen en dos grandes grupos: los atacantes pasivos, aquellos que fisgonean por el sistema pero no lo modifican o destruyen, y los activos, aquellos que dañan el objetivo atacado, o lo modifican en su favor. Generalmente los curiosos y los crackers realizan ataques pasivos (que se pueden convertir en activos), mientras que los terroristas y ex-empleados realizan ataques activos puros; los intrusos remunerados suelen ser atacantes pasivos si nuestra red o equipo no es su objetivo, y activos en caso contrario, y el personal realiza ambos tipos indistintamente, dependiendo de la situación concreta

Personal.

Ex-empleados.

Curiosos.

Crackers.

Terroristas.

Intrusos (remunerados).

Amenazas lógicas. Bajo la etiqueta de “amenazas lógicas” encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (bugs o agujeros). Una excelente lectura que estudia las definiciones de algunas de estas amenazas y su implicación se presenta en [Garfinkel, 1996]; otra buena descripción, pero a un nivel más general, se puede encontrar en [Parker, 1981].

Software incorrecto. Las amenazas más habituales a un sistema provienen de errores cometidos de forma involuntaria por los programadores de sistemas o de aplicaciones.

Herramientas de Seguridad. Cualquier herramienta de seguridad representa un arma de doble filo: de la misma forma que un administrador las utiliza para detectar y solucionar fallos en sus sistemas o en la subred completa, un potencial intruso las puede utilizar para detectar esos mismos fallos y aprovecharlos para atacar los equipos.

Puertas traseras. Durante el desarrollo de aplicaciones grandes o de sistemas operativos es habitual entre los programadores insertar “atajos”. A estos atajos se les denomina puertas traseras. Algunos programadores pueden dejar estos atajos en las versiones definitivas de su software; la cuestión es que si un atacante descubre una de estas puertas traseras (no nos importa el método que utilice para hacerlo) va a tener un acceso global a datos que no debería poder leer.

Bombas lógicas. Las bombas lógicas son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas. Los activadores más comunes de estas bombas lógicas pueden ser la ausencia o presencia de ciertos ficheros, la llegada de una fecha concreta; cuando la bomba se activa va a poder realizar cualquier tarea que pueda realizar la persona, los efectos pueden ser fatales.

Virus. Un virus es una secuencia de código que se inserta en un fichero ejecutable (denominado huésped), de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

Gusanos. Un gusano es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos.

Caballos de Troya. Los troyanos o caballos de Troya son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas sin el conocimiento del usuario

Catástrofes. Catástrofes naturales o artificiales son la amenaza menos probable contra los entornos habituales: simplemente por su ubicación geográfica, a nadie se le escapa que la probabilidad de sufrir un terremoto o una inundación que afecte a los sistemas informáticos en una gran ciudad, es relativamente baja, al menos en comparación con el riesgo de sufrir un intento de acceso por parte de un pirata o una infección por virus. Sin embargo, el hecho de que las catástrofes sean amenazas poco probables no implica que contra ellas no se tomen unas medidas básicas, ya que sí se produjeran generarían los mayores daños.

# 3.2 Tipos de ataques

Tipos de ataques:

* Ataque de denegación de servicio (DoS)
* Ataque de denegación de servicio distribuido (DDoS)
* Ataque de fuerza bruta
* Ataque de inyección SQL
* Ataque de exploit
* Ataque de phishing
* Ataque de malware
* Ataque de ransomware
* Ataque de hombre en el medio

*Ataque de denegacion de servicio (DoS)*

Un ataque de denegación de servicio (DoS) es un tipo de ataque informático que tiene como objetivo abrumar un servidor o red con tráfico malicioso o solicitudes falsas, lo que provoca una caída del servicio para los usuarios legítimos. El objetivo de este ataque es dejar inoperable un sitio web o servicio en línea, impidiendo que los usuarios legítimos puedan acceder a él.

Los atacantes pueden realizar un ataque DoS de diferentes maneras. Algunos ejemplos incluyen:

Ataque de inundación de tráfico: Este tipo de ataque implica enviar una gran cantidad de tráfico a un servidor, sobrecargando el ancho de banda y haciendo que el servidor deje de responder.

Ataque de amplificación de tráfico: Este tipo de ataque implica aprovechar la vulnerabilidad de un protocolo de red para enviar paquetes de datos falsificados a un servidor, que responde a ellos enviando paquetes a una dirección IP de destino elegida por el atacante.

Ataque de solicitud falsificada: Este tipo de ataque implica enviar solicitudes falsas al servidor, haciéndole creer que está siendo utilizado por usuarios legítimos y agotando los recursos del servidor.

Los ataques DoS pueden ser realizados por un solo atacante o por un grupo de atacantes que coordinan sus esfuerzos. Los motivos detrás de los ataques DoS pueden variar, desde la extorsión hasta la venganza o simplemente por diversión.

Los ataques DoS pueden ser devastadores para las empresas y organizaciones que dependen de sus sitios web y servicios en línea para funcionar correctamente. Para protegerse contra los ataques DoS, es importante tener en cuenta las mejores prácticas de seguridad, como la implementación de firewalls y la gestión del tráfico de red para detectar y bloquear el tráfico malicioso.

*Ataque de denegación de servicio distribuido (DDoS)*

Un ataque de denegación de servicio distribuido (DDoS) es una variante del ataque de denegación de servicio (DoS), en la que un atacante utiliza múltiples dispositivos conectados a Internet para inundar el servidor objetivo con tráfico malicioso o solicitudes falsas.

En un ataque DDoS, los dispositivos utilizados para enviar el tráfico malicioso o las solicitudes falsas son a menudo dispositivos comprometidos o infectados con malware, como computadoras personales, servidores web, enrutadores y otros dispositivos de Internet de las cosas (IoT).

Los atacantes pueden controlar estos dispositivos de forma remota a través de una red botnet, que es una red de dispositivos infectados y controlados por el atacante. Estos dispositivos pueden ser utilizados para enviar tráfico malicioso al servidor objetivo, sobrecargando sus recursos y provocando una caída del servicio.

Una vez que el ataque comienza, puede ser muy difícil detenerlo, ya que el tráfico malicioso proviene de múltiples fuentes, lo que dificulta la identificación del atacante y la mitigación del ataque.

Los ataques DDoS pueden ser motivados por una variedad de razones, desde la extorsión hasta la venganza o simplemente por diversión. Los ataques DDoS pueden ser especialmente devastadores para las empresas y organizaciones que dependen de sus sitios web y servicios en línea para funcionar correctamente.

Para protegerse contra los ataques DDoS, es importante tener en cuenta las mejores prácticas de seguridad, como la implementación de firewalls, sistemas de detección de intrusiones y gestión del tráfico de red para detectar y bloquear el tráfico malicioso. También es importante mantener los dispositivos conectados a Internet actualizados y protegidos contra malware para evitar que sean utilizados como parte de una botnet.

*Ataque de fuerza bruta*

Un ataque de fuerza bruta es un tipo de ataque informático que implica intentar adivinar una contraseña o clave de cifrado mediante la fuerza bruta, es decir, probando todas las combinaciones posibles hasta que se encuentra la correcta.

En un ataque de fuerza bruta, un atacante intenta acceder a un sistema o servicio protegido por una contraseña o clave de cifrado mediante la prueba de diferentes combinaciones de caracteres, desde palabras comunes hasta números y símbolos.

Los ataques de fuerza bruta pueden ser automatizados con herramientas especiales que prueban todas las combinaciones posibles a alta velocidad. Si la contraseña es lo suficientemente débil o corta, el atacante puede tener éxito en adivinarla en un tiempo relativamente corto.

Los ataques de fuerza bruta pueden ser especialmente efectivos contra contraseñas débiles, como "1234" o "contraseña", que son fáciles de adivinar. También pueden ser efectivos contra contraseñas más fuertes si se utilizan técnicas de diccionario que prueban combinaciones de palabras comunes o variaciones de ellas.

Para protegerse contra los ataques de fuerza bruta, es importante utilizar contraseñas fuertes y complejas que contengan una combinación de letras mayúsculas y minúsculas, números y símbolos. También es importante evitar el uso de contraseñas comunes o fáciles de adivinar, como nombres propios, fechas de nacimiento o palabras simples. Además, se pueden utilizar herramientas de seguridad como bloqueos de cuentas después de un número determinado de intentos fallidos de inicio de sesión, la implementación de medidas de autenticación de dos factores y el cifrado de datos sensibles.

*Ataque de inyección SQL*

Un ataque de inyección SQL es un tipo de ataque informático en el que un atacante utiliza una vulnerabilidad en una aplicación web para manipular una base de datos a través de la entrada de datos del usuario.

En un ataque de inyección SQL, el atacante inserta código malicioso en los campos de entrada de una aplicación web, como un formulario de inicio de sesión o un campo de búsqueda. Este código malicioso se utiliza para engañar al servidor de la aplicación para que ejecute comandos SQL no autorizados.

Si el ataque es exitoso, el atacante puede obtener acceso no autorizado a la base de datos, modificar o eliminar datos, o incluso tomar el control del servidor.

Los ataques de inyección SQL pueden ser especialmente peligrosos porque pueden explotar vulnerabilidades en aplicaciones web legítimas y ampliamente utilizadas, como WordPress, Drupal y Joomla.

Para protegerse contra los ataques de inyección SQL, es importante utilizar las mejores prácticas de seguridad de aplicaciones web, como validar y filtrar los datos de entrada del usuario, utilizar consultas parametrizadas y evitar el uso de comandos SQL dinámicos. También es importante mantener las aplicaciones web actualizadas y parcheadas para evitar vulnerabilidades conocidas.

Ataque de exploit

Un ataque de exploit es un tipo de ataque informático en el que un atacante aprovecha una vulnerabilidad en un sistema operativo, una aplicación o un software para tomar el control del sistema o para ejecutar código malicioso.

Los exploits pueden aprovechar vulnerabilidades conocidas o recién descubiertas en el sistema o en la aplicación para ejecutar código arbitrario. Los atacantes pueden utilizar exploits para instalar software malicioso en el sistema de la víctima, robar datos confidenciales, obtener acceso no autorizado a un sistema, o incluso para causar daños físicos en un sistema conectado a Internet de las cosas (IoT).

Los exploits pueden ser específicos de un sistema operativo, una aplicación o un software, o pueden ser ataques de día cero que aprovechan vulnerabilidades desconocidas y sin parchear.

Para protegerse contra los ataques de exploit, es importante mantener todos los sistemas, aplicaciones y software actualizados y parcheados para evitar vulnerabilidades conocidas. También es importante implementar medidas de seguridad como firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para detectar y bloquear posibles ataques de exploit.

Ataque de phishing

Un ataque de phishing es un tipo de ataque informático en el que un atacante intenta engañar a una víctima para que revele información confidencial, como contraseñas, números de tarjetas de crédito, información bancaria o datos personales, a través de técnicas de ingeniería social.

Los ataques de phishing generalmente se realizan por correo electrónico, pero también pueden ser por mensajes de texto, redes sociales, mensajería instantánea o incluso por teléfono. Los atacantes a menudo utilizan tácticas de urgencia o miedo para convencer a la víctima de que revele información confidencial, como afirmar que su cuenta ha sido hackeada o que hay un problema con una transacción.

Los correos electrónicos de phishing suelen ser diseñados para parecer legítimos y engañar a la víctima para que haga clic en un enlace o descargue un archivo adjunto que contiene malware. Una vez que la víctima hace clic en el enlace o descarga el archivo, se puede instalar software malicioso en su dispositivo o se puede dirigir a la víctima a una página web falsa diseñada para parecerse a una página web legítima, como un sitio bancario o de compras en línea, para que revele información confidencial.

Para protegerse contra los ataques de phishing, es importante estar atento a los correos electrónicos o mensajes sospechosos, verificar la autenticidad de la fuente del correo electrónico o mensaje, no hacer clic en enlaces sospechosos, no descargar archivos adjuntos de remitentes desconocidos, y no revele información confidencial en respuesta a correos electrónicos, mensajes o llamadas no solicitadas. También es importante utilizar software de seguridad actualizado y tener medidas de seguridad como autenticación de dos factores y contraseñas fuertes.

*Ataque de malware*

Un ataque de malware es un tipo de ataque informático en el que un atacante utiliza software malicioso, o malware, para tomar el control de un sistema, robar datos confidenciales, o causar daño a un sistema o red.

El malware puede tomar muchas formas, incluyendo virus, gusanos, troyanos, ransomware, adware, spyware y bots. Una vez que el malware infecta un sistema, puede propagarse a otros sistemas en la red o incluso a sistemas externos conectados a la red.

Los atacantes pueden utilizar el malware para espiar a las víctimas, robar información confidencial como contraseñas, números de tarjetas de crédito y otra información personal, tomar el control de sistemas, cifrar archivos y exigir rescate, o incluso para causar daño físico en sistemas conectados a IoT.

Los ataques de malware pueden ocurrir a través de descargas maliciosas, correos electrónicos de phishing, sitios web comprometidos, dispositivos USB infectados y otras técnicas de ingeniería social.

Para protegerse contra los ataques de malware, es importante utilizar software de seguridad actualizado, mantener sistemas y software actualizados y parcheados para evitar vulnerabilidades conocidas, evitar descargas y correos electrónicos sospechosos, no hacer clic en enlaces o archivos adjuntos sospechosos, y tener medidas de seguridad como firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para detectar y bloquear posibles ataques de malware.

Ataque de ransomware

Un ataque de ransomware es un tipo de ataque informático en el que un atacante utiliza software malicioso para cifrar archivos o sistemas informáticos y luego extorsionar a la víctima para que pague un rescate a cambio de la clave de descifrado.

Los ataques de ransomware pueden ser muy dañinos y pueden afectar a individuos, empresas y organizaciones de todo tipo. Una vez que el malware cifra los archivos o sistemas, la víctima puede perder acceso a datos importantes o incluso a sistemas enteros, lo que puede provocar interrupciones graves en la operación de negocios y organizaciones.

Los ataques de ransomware generalmente se propagan a través de correos electrónicos de phishing o sitios web comprometidos. Los atacantes utilizan técnicas de ingeniería social para hacer que las víctimas hagan clic en enlaces o descarguen archivos que contienen el malware de ransomware.

Una vez que el ransomware infecta el sistema de la víctima, se cifran los archivos importantes, y el atacante muestra un mensaje de rescate en la pantalla, exigiendo un pago en criptomonedas a cambio de la clave de descifrado. Si la víctima no paga el rescate, los atacantes pueden borrar permanentemente los archivos cifrados.

Para protegerse contra los ataques de ransomware, es importante mantener los sistemas y el software actualizados, tener copias de seguridad de los datos importantes, evitar descargas y correos electrónicos sospechosos, tener medidas de seguridad como firewalls y sistemas de detección de intrusiones, y educar a los usuarios sobre las prácticas seguras de navegación en línea.

*Ataque de hombre en el medio*

Un ataque de hombre en el medio (MITM, por sus siglas en inglés) es un tipo de ataque informático en el que un atacante intercepta y manipula la comunicación entre dos partes que están intentando comunicarse. El atacante se sitúa en el medio de la comunicación y hace que ambas partes crean que están hablando directamente entre sí, cuando en realidad están hablando con el atacante.

El objetivo del ataque de MITM es permitir que el atacante obtenga información confidencial, como contraseñas, información de inicio de sesión, detalles de transacciones financieras o cualquier otro tipo de información que se intercambie entre las dos partes.

Los ataques de MITM pueden ocurrir en cualquier tipo de comunicación, incluyendo comunicaciones de red, correos electrónicos, mensajes instantáneos y llamadas telefónicas. Para llevar a cabo el ataque, el atacante puede utilizar una variedad de técnicas, como el secuestro de sesión, la falsificación de direcciones MAC y la suplantación de identidad.

Para protegerse contra los ataques de MITM, es importante utilizar conexiones seguras como HTTPS o SSL/TLS, utilizar una red privada virtual (VPN) para proteger las comunicaciones en línea, verificar la autenticidad de los sitios web y de los correos electrónicos, utilizar contraseñas fuertes y no compartirlas, y tener precaución al conectarse a redes públicas y abiertas. También es importante mantener el software actualizado y utilizar software de seguridad confiable.

# 3.3 Creación del plan, procedimientos y políticas de seguridad

Para empezar este tema es importante establecer medidas de seguridad para proteger la información y los recursos críticos de nuestra empresa u/o organización. Para esto implica deseñar i implementar un plan de seguridad el cual contenga políticas y procedimientos para minimizar los riesgos de seguridad y garantizar la continuidad del negocio.

3.3.1.- creación del plan.

Para lograr el proceso de creación de un plan de seguridad se debe implementar varios pasos importantes para lograr este hecho. El proceso de creación de un plan de seguridad es un proceso que debe ser llevado a cabo con mucho cuidado y atención para garantizar que se diseñen medidas de seguridad efectivas y adecuadas para proteger los recursos críticos de una organización.

1.- Identificación de los recursos críticos.

El primer paso en la creación de un plan de seguridad es identificar los recursos críticos que se necesitan proteger. Estos recursos pueden incluir datos, información, sistemas informáticos, redes, instalaciones y activos físicos.

2.- Evaluación de los riesgos.

El siguiente paso es realizar una evaluación de riesgos para identificar las amenazas y vulnerabilidades que pueden afectar los recursos críticos. Esto implica identificar las fuentes de amenazas, como los hackers, los virus informáticos, los desastres naturales, entre otros.

3.- Desarrollo de políticas y procedimientos.

Con base en la evaluación de riesgos, se pueden desarrollar políticas y procedimientos de seguridad para minimizar los riesgos. Las políticas establecen las normas y reglas que se deben seguir para proteger los recursos críticos, mientras que los procedimientos son los pasos específicos que se deben seguir para implementar estas políticas.

4.- Implementación de medidas de seguridad.

Una vez que se han desarrollado las políticas y los procedimientos, se pueden implementar las medidas de seguridad necesarias para proteger los recursos críticos. Esto puede incluir la instalación de software de seguridad, la configuración de cortafuegos y la realización de copias de seguridad de datos críticos.

5.- Monitoreo y evaluación.

Es importante monitorear y evaluar continuamente el plan de seguridad para garantizar que siga siendo efectivo y relevante en un entorno en constante cambio. Esto implica realizar revisiones regulares de las políticas y los procedimientos y llevar a cabo simulacros de seguridad para probar la eficacia del plan.

la creación de un plan de seguridad es un proceso que debe ser llevado a cabo con mucho cuidado y atención para garantizar que se diseñen medidas de seguridad efectivas y adecuadas para proteger los recursos críticos de una organización.

3.3.2.- políticas.

Las políticas de seguridad establecen las normas y reglas que deben seguirse para proteger los recursos críticos de la organización. Estas políticas deben ser claras y específicas para garantizar que todos los miembros de la organización comprendan sus responsabilidades y obligaciones en materia de seguridad. También estas políticas son esenciales para garantizar la seguridad de los datos, la información y los sistemas informáticos de una organización, y para minimizar los riesgos de seguridad.

Las políticas de seguridad pueden variar de una organización a otra, dependiendo de las necesidades y requisitos específicos.

1.- Política de acceso.

Esta política establece quiénes pueden acceder a los recursos críticos de la organización y cómo se puede acceder a ellos. Esta política puede incluir requisitos de autenticación, como contraseñas seguras, así como restricciones de acceso basadas en roles y responsabilidades.

2.- Política de seguridad de red.

Esta política establece las reglas y prácticas necesarias para proteger las redes de la organización. Puede incluir la configuración de cortafuegos, la detección de intrusiones y el monitoreo del tráfico de red para detectar y prevenir ataques maliciosos.

3.- Política de gestión de contraseñas.

Esta política establece las reglas y prácticas necesarias para garantizar que las contraseñas de los usuarios sean seguras y estén protegidas. Esto puede incluir requisitos de complejidad de contraseñas, políticas de cambio de contraseñas y requisitos de almacenamiento seguro de contraseñas.

4.- Política de seguridad física:

Esta política establece las medidas de seguridad necesarias para proteger los activos físicos de la organización, como los edificios y los equipos. Puede incluir la instalación de sistemas de seguridad física, como cámaras de vigilancia y cerraduras de alta seguridad.

5.- Política de gestión de datos.

Esta política establece las reglas y prácticas necesarias para garantizar que los datos y la información de la organización estén protegidos y sean gestionados de forma segura. Puede incluir requisitos de clasificación de datos, políticas de gestión de datos y requisitos de almacenamiento seguro de datos.

Estas son algunos ejemplos de políticas de seguridad comunes que se pueden encontrar en muchas organizaciones. las políticas de seguridad son esenciales para garantizar la protección de los recursos críticos de una organización. Las políticas pueden variar de una organización a otra, pero comúnmente incluyen políticas de acceso, de seguridad de red, de gestión de contraseñas, de seguridad física y de gestión de datos.

3.3.3.- procedimientos.

Los procedimientos de seguridad son los pasos específicos que deben seguirse para implementar las políticas de seguridad. Estos procedimientos pueden incluir la instalación de software de seguridad, la configuración de cortafuegos y la realización de copias de seguridad de los datos críticos.

Los procedimientos de seguridad son un conjunto de acciones y medidas específicas que deben seguirse para implementar las políticas de seguridad de una organización. Estos procedimientos son necesarios para garantizar la consistencia y la efectividad de las políticas de seguridad y para minimizar los riesgos de seguridad.

1.- Procedimiento de identificación y autenticación.

Este procedimiento establece cómo se deben identificar y autenticar los usuarios de la organización antes de que se les permita acceder a los recursos críticos. Puede incluir requisitos para la creación de cuentas de usuario, la verificación de identidad y la autenticación de contraseñas.

2.- Procedimiento de control de acceso.

Este procedimiento establece cómo se deben gestionar los permisos y el acceso a los recursos críticos de la organización. Puede incluir la asignación de permisos basados en roles y responsabilidades, la revisión regular de los permisos y la gestión de los cambios en los permisos de acceso.

3.- Procedimiento de monitorización y detección de amenazas.

Este procedimiento establece cómo se debe realizar la monitorización continua de los sistemas de la organización para detectar y responder a las amenazas de seguridad. Puede incluir la implementación de sistemas de detección de intrusiones, la monitorización del tráfico de red y la revisión regular de los registros de eventos.

4.- Procedimiento de gestión de incidentes.

Este procedimiento establece cómo se debe responder y gestionar los incidentes de seguridad que se produzcan en la organización. Puede incluir la creación de planes de respuesta a incidentes, la notificación de las partes afectadas y la realización de investigaciones para determinar la causa y el alcance del incidente.

5.- Procedimiento de gestión de vulnerabilidades.

Este procedimiento establece cómo se deben identificar y gestionar las vulnerabilidades en los sistemas y aplicaciones de la organización. Puede incluir la realización de pruebas de penetración regulares, la aplicación de parches de seguridad y la gestión de los riesgos asociados con las vulnerabilidades no resueltas.

# 3.4 Evaluación de riesgos

## 3.4.1 Activos a proteger

1. **Datos sensibles:** los datos confidenciales como información personal, financiera o de negocios deben protegerse para evitar el acceso no autorizado.
2. **Recursos de red:** los recursos de red como servidores, enrutadores y switches son críticos para la funcionalidad de la red y deben protegerse para evitar el acceso no autorizado o la manipulación.
3. **Contraseñas y credenciales de usuario:** las contraseñas y las credenciales de usuario son críticas para la autenticación y la seguridad de la red, por lo que deben protegerse para evitar el acceso no autorizado.
4. **Dispositivos de red:** los dispositivos de red como firewalls y sistemas de detección de intrusos (IDS) son críticos para la protección de la red y deben protegerse para evitar la manipulación o el acceso no autorizado.
5. **Software y sistemas operativos:** el software y los sistemas operativos de los dispositivos de red y las computadoras deben mantenerse actualizados y protegidos para evitar vulnerabilidades de seguridad.
6. **Datos de respaldo:** los datos de respaldo son críticos para la recuperación en caso de una interrupción o desastre, por lo que deben protegerse para evitar la pérdida o el acceso no autorizado.
7. **Infraestructura física:** la infraestructura física como los centros de datos y los dispositivos de almacenamiento deben protegerse contra robos, incendios, inundaciones y otros desastres naturales.

**Existen diversas formas de proteger los activos de una red de computadoras, algunas de las cuales son:**

**Implementar autenticación y control de acceso:** La autenticación y el control de acceso son importantes para evitar el acceso no autorizado a los datos y recursos de la red. Se pueden utilizar técnicas como contraseñas robustas, autenticación de dos factores y certificados digitales para garantizar que solo los usuarios autorizados puedan acceder a la red.

**Implementar encriptación de datos:** La encriptación es una técnica efectiva para proteger los datos en tránsito y en reposo. Se pueden utilizar protocolos de seguridad como HTTPS, SSL/TLS, VPNs y cifrado de disco completo para garantizar que los datos no puedan ser leídos por personas no autorizadas.

**Actualizar software y sistemas operativos**: Las actualizaciones de software y sistemas operativos incluyen parches y actualizaciones de seguridad que solucionan vulnerabilidades conocidas. Mantener el software y los sistemas operativos actualizados es una forma efectiva de proteger los activos de la red.

**Implementar software de seguridad:** Se pueden utilizar soluciones de seguridad como firewalls, sistemas de detección de intrusos y software antivirus para proteger la red contra amenazas de seguridad.

**Implementar políticas de seguridad:** Las políticas de seguridad claras y bien definidas son importantes para establecer expectativas claras en relación a la seguridad de la red. Las políticas de seguridad deben incluir pautas para la gestión de contraseñas, la configuración de dispositivos y la gestión de acceso.

**Realizar copias de seguridad regulares:** Las copias de seguridad regulares son importantes para garantizar que los datos críticos se puedan recuperar en caso de una interrupción o desastre. Se deben realizar copias de seguridad de forma regular y almacenarlas en un lugar seguro.

**Proteger la infraestructura física:** La infraestructura física, como los centros de datos, debe protegerse contra robos, incendios, inundaciones y otros desastres naturales mediante la implementación de medidas de seguridad física, como sistemas de vigilancia, control de acceso y protección contra incendios.

**Existen muchos programas de seguridad disponibles para proteger los activos de una red de computadoras. Algunos ejemplos de programas comunes incluyen:**

**Antivirus:** Los programas antivirus son importantes para detectar y eliminar virus y malware de los sistemas. Algunos ejemplos populares de programas antivirus incluyen Norton Antivirus, McAfee Antivirus y Kaspersky Antivirus.

**Firewall:** Los firewalls son importantes para proteger la red de amenazas externas. Algunos ejemplos de programas firewall incluyen Windows Firewall, ZoneAlarm y Norton Firewall.

**Sistema de detección de intrusos (IDS):** Los sistemas de detección de intrusos pueden detectar y prevenir intentos de ataque en la red. Algunos ejemplos de programas IDS incluyen Snort, OSSEC y Suricata.

**VPN:** Las redes privadas virtuales (VPN) son importantes para proteger la privacidad y seguridad de las conexiones de red. Algunos ejemplos de programas VPN incluyen NordVPN, ExpressVPN y CyberGhost VPN.

**Gestor de contraseñas:** Los gestores de contraseñas son importantes para proteger las contraseñas de los usuarios y garantizar que sean seguras. Algunos ejemplos de programas gestores de contraseñas incluyen LastPass, 1Password y Dashlane.

Es importante elegir programas que sean adecuados para las necesidades específicas de la red y los sistemas que se están protegiendo. Es recomendable investigar y evaluar varios programas antes de tomar una decisión.

## 3.4.2 Amenazas contra las que se tiene que proteger

**¿Qué son las amenazas?**

Las amenazas son cualquier acción o evento que pueda tener un impacto negativo en un sistema o en una organización. En el contexto de la seguridad informática, las amenazas son eventos o acciones que tienen el potencial de causar daño a los sistemas informáticos, las redes o la información almacenada en ellos.

Pueden venir de fuentes internas o externas, y pueden ser intencionales o no intencionales. Las amenazas tienen diversos objetivos, como robar información confidencial, dañar la reputación de una empresa o interrumpir las operaciones normales de una organización. Por lo tanto, es importante evaluar y comprender las amenazas que pueden afectar a un sistema u organización para poder implementar medidas de protección adecuadas.

**¿Por qué debemos de proteger?**

Hay varias razones por las cuales se debe proteger contra las amenazas de seguridad informática:

* Proteger la privacidad: Las amenazas de seguridad informática pueden comprometer la privacidad de las personas y las organizaciones, ya que pueden permitir el acceso no autorizado a información confidencial.
* Proteger los datos: La información es un activo valioso para las organizaciones y los individuos, y las amenazas de seguridad informática pueden resultar en la pérdida de datos valiosos.
* Mantener la integridad de los sistemas: Los ataques de seguridad informática pueden comprometer la integridad de los sistemas, lo que puede resultar en la pérdida de control sobre los sistemas y la información que contienen.
* Evitar la interrupción del negocio: Los ataques de seguridad informática pueden interrumpir los sistemas y servicios críticos, lo que puede resultar en la interrupción del negocio y la pérdida de ingresos.
* Evitar costos financieros: Los ataques de seguridad informática pueden resultar en costos financieros significativos, como reparación de sistemas dañados, recuperación de datos perdidos y pago de rescates en el caso de ransomware.

En resumen, la protección contra las amenazas de seguridad informática es esencial para proteger la privacidad, los datos, la integridad de los sistemas y para evitar la interrupción del negocio y los costos financieros. Es importante tomar medidas de seguridad adecuadas y mantenerlas actualizadas y monitoreadas continuamente para proteger adecuadamente la organización contra las amenazas identificadas.

**Amenazas contra las que se tienen que proteger**

En una evaluación de riesgos de seguridad informática, se deben considerar una amplia gama de amenazas que pueden afectar a una organización. Algunas de las amenazas más comunes que se deben tener en cuenta incluyen:

1. Malware.
2. Ataques de phishing.
3. Ataques de fuerza bruta.
4. Ataques de denegación de servicio (DoS).
5. Robo de identidad.
6. Vulnerabilidades de software.
7. Acceso no autorizado.
8. Intercepción de datos.

**Manera general de cómo protegerse**

Para proteger una organización contra las amenazas identificadas en una evaluación de riesgos de seguridad informática, se pueden implementar una variedad de medidas de protección. Algunas medidas comunes incluyen:

1. Implementar software de seguridad: se pueden instalar soluciones de seguridad, como antivirus, cortafuegos y software de detección de intrusiones, para proteger contra amenazas de malware y otros ataques.
2. Capacitar a los empleados: se deben educar a los empleados sobre cómo identificar y evitar ataques de phishing y otros intentos de engaño.
3. Fortalecer la autenticación: se pueden implementar medidas de autenticación fuertes, como contraseñas complejas, autenticación de dos factores o biométrica, para proteger contra ataques de fuerza bruta y robos de identidad.
4. Mantener el software actualizado: se deben aplicar regularmente las actualizaciones de seguridad del software y los parches para evitar vulnerabilidades de software conocidas.
5. Controlar el acceso: se deben establecer políticas de acceso para limitar el acceso a los sistemas y datos solo a los usuarios autorizados.
6. Monitorear la red: se pueden utilizar herramientas de monitoreo de red para detectar y prevenir ataques de denegación de servicio y otros intentos de ataque.
7. Realizar pruebas de seguridad: se pueden realizar pruebas de penetración y otros tipos de pruebas de seguridad para identificar vulnerabilidades en los sistemas y datos.

Es importante tener en cuenta que ninguna medida de protección es completamente efectiva en sí misma. Se deben implementar varias medidas de protección y mantenerlas actualizadas y monitoreadas continuamente para proteger adecuadamente la organización contra las amenazas identificadas. Además, se debe realizar regularmente una evaluación de riesgos para identificar nuevas amenazas y ajustar las medidas de protección según sea necesario.

**Manera individual de cómo protegerse**

* Malware

1. Mantener el software actualizado: Mantener el software, incluyendo el sistema operativo y las aplicaciones, actualizado con los últimos parches y actualizaciones de seguridad es esencial para proteger contra vulnerabilidades conocidas que pueden ser explotadas por el malware.
2. Utilizar software antivirus: Instalar un software antivirus actualizado y de buena reputación puede ayudar a detectar y eliminar el malware de los sistemas.
3. Ser cauteloso con los correos electrónicos y los enlaces sospechosos: No abrir correos electrónicos de remitentes desconocidos y no hacer clic en enlaces sospechosos que se encuentran en los correos electrónicos, sitios web y redes sociales.
4. Utilizar contraseñas seguras: Utilizar contraseñas seguras y únicas para cada cuenta y cambiarlas regularmente es una medida importante para protegerse contra el malware y otros ataques.
5. Utilizar el sentido común: Ser cauteloso al descargar archivos de Internet, y solo hacerlo desde sitios web de confianza.
6. Configurar cortafuegos: Utilizar un firewall es una medida importante para proteger la red y los dispositivos de los ataques de malware.

* Ataques de phishing.

1. Ser cauteloso con los correos electrónicos sospechosos: No abrir correos electrónicos de remitentes desconocidos o sospechosos y no hacer clic en enlaces o descargas en esos correos electrónicos. Verificar cuidadosamente la dirección de correo electrónico y la URL en los enlaces para asegurarse de que sean legítimos.
2. Verificar la autenticidad del sitio web: Verificar que el sitio web es legítimo y seguro antes de ingresar cualquier información personal o confidencial. Buscar indicadores de seguridad como un candado verde en la barra de direcciones y una dirección URL que comienza con "https".
3. No proporcionar información personal o confidencial: No proporcionar información personal o confidencial a sitios web o correos electrónicos sospechosos o desconocidos.
4. Utilizar software de seguridad: Utilizar software de seguridad como filtros anti-spam y software antivirus puede ayudar a detectar y bloquear correos electrónicos y sitios web maliciosos.
5. Capacitarse sobre los ataques de phishing: Capacitarse y estar al tanto de los diferentes tipos de ataques de phishing y cómo detectarlos puede ayudar a protegerse contra ellos.

* Ataques de fuerza bruta.

1. Utilizar contraseñas seguras: Utilizar contraseñas seguras y únicas para cada cuenta y cambiarlas regularmente es una medida importante para protegerse contra los ataques de fuerza bruta.
2. Utilizar autenticación de dos factores (2FA): Utilizar autenticación de dos factores (2FA) puede proporcionar una capa adicional de seguridad al requerir un código de seguridad adicional enviado a un dispositivo autorizado para acceder a la cuenta.
3. Limitar los intentos de inicio de sesión: Limitar los intentos de inicio de sesión, ya sea mediante la limitación de intentos de inicio de sesión fallidos o mediante la implementación de un sistema de bloqueo de cuenta después de un número determinado de intentos fallidos.
4. Monitorear las actividades de inicio de sesión: Monitorear las actividades de inicio de sesión para detectar patrones de actividad sospechosa y tomar medidas preventivas.
5. Utilizar herramientas de seguridad: Utilizar herramientas de seguridad como firewalls, software de detección de intrusiones y sistemas de prevención de intrusiones puede ayudar a detectar y prevenir los ataques de fuerza bruta.

* Ataques de denegación de servicio (DoS).

1. Implementar un sistema de detección y prevención de ataques DoS: Un sistema de detección y prevención de ataques DoS puede ayudar a detectar y bloquear los ataques de denegación de servicio en tiempo real.
2. Utilizar servicios de protección DDoS: Los servicios de protección DDoS, como Cloudflare, pueden proteger tu sitio web o servicio en línea contra ataques de denegación de servicio al filtrar el tráfico malicioso antes de que llegue a tu servidor.
3. Configurar adecuadamente los servidores y la red: Configurar adecuadamente los servidores y la red puede ayudar a reducir la vulnerabilidad de los sistemas a los ataques DoS. Algunas medidas incluyen limitar el número de conexiones simultáneas permitidas, limitar el ancho de banda utilizado por cada usuario y bloquear direcciones IP sospechosas.
4. Monitorear el tráfico de red: Monitorear el tráfico de red para detectar patrones de tráfico sospechosos puede ayudar a prevenir los ataques de denegación de servicio.
5. Preparar un plan de respuesta a incidentes: Preparar un plan de respuesta a incidentes puede ayudar a minimizar el impacto de un ataque de denegación de servicio y restaurar rápidamente el servicio después del ataque.

* Robo de identidad.

1. Utiliza contraseñas seguras: Utiliza contraseñas seguras y diferentes para cada cuenta. Evita usar la misma contraseña para varias cuentas, ya que, si un pirata informático obtiene una de tus contraseñas, podrá acceder a varias de tus cuentas.
2. No compartas tu información personal: Evita compartir tu información personal con personas que no conoces y no reveles información sensible, como tu número de seguridad social o información bancaria, a menos que sea absolutamente necesario.
3. Usa software de seguridad: Usa un software de seguridad, como un antivirus y un firewall, para proteger tu computadora y dispositivos móviles contra el malware y otras amenazas.
4. Protege tu correo electrónico: Muchos robos de identidad comienzan con un correo electrónico de phishing. Evita hacer clic en enlaces desconocidos o sospechosos en correos electrónicos, especialmente si solicitan información personal o financiera.
5. Revisa tus estados de cuenta: Revisa tus estados de cuenta bancarios y de tarjetas de crédito con regularidad para detectar transacciones sospechosas. Si ves algo que parece extraño o no autorizado, comunícate con el proveedor de la cuenta de inmediato.
6. Habilita la autenticación de dos factores: Habilita la autenticación de dos factores (2FA) en todas las cuentas que lo permitan. La autenticación de dos factores agrega una capa adicional de seguridad al requerir un código único que se envía a tu teléfono o correo electrónico antes de acceder a tu cuenta.
7. Mantén tus dispositivos actualizados: Mantén tus dispositivos y aplicaciones actualizados con las últimas actualizaciones de seguridad. Las actualizaciones a menudo incluyen parches de seguridad críticos que protegen contra las vulnerabilidades conocidas.

* Vulnerabilidades de software.

1. Mantén tus sistemas actualizados: Mantén tus sistemas operativos, aplicaciones y software antivirus actualizados con las últimas actualizaciones de seguridad. Las actualizaciones a menudo incluyen parches de seguridad críticos que protegen contra las vulnerabilidades conocidas.
2. Usa software de seguridad: Usa un software de seguridad, como un antivirus y un firewall, para proteger tu computadora y dispositivos móviles contra el malware y otras amenazas.
3. Utiliza contraseñas seguras: Utiliza contraseñas seguras y diferentes para cada cuenta. Evita usar la misma contraseña para varias cuentas, ya que, si un pirata informático obtiene una de tus contraseñas, podrá acceder a varias de tus cuentas.
4. Usa herramientas de detección de vulnerabilidades: Usa herramientas de detección de vulnerabilidades para escanear tus sistemas y aplicaciones en busca de vulnerabilidades conocidas. Estas herramientas pueden ayudarte a identificar y corregir vulnerabilidades antes de que los atacantes las exploren.
5. Limita los privilegios de usuario: Limita los privilegios de usuario y restringe el acceso a los sistemas y datos sensibles solo a los usuarios autorizados. Esto puede ayudar a evitar que los atacantes accedan a los datos confidenciales y a los sistemas críticos.
6. Realiza pruebas de penetración: Realiza pruebas de penetración periódicas para identificar y corregir vulnerabilidades en tus sistemas y aplicaciones. Las pruebas de penetración simulan un ataque real y pueden ayudarte a identificar debilidades que de otro modo podrían pasar desapercibidas.
7. Usa el principio de "menor privilegio": Usa el principio de "menor privilegio" para limitar los accesos de los usuarios y procesos a los recursos del sistema solo a los necesarios para realizar su trabajo. Esto puede ayudar a prevenir que los atacantes escalen privilegios y accedan a sistemas o datos sensibles.

* Acceso no autorizado.

1. Usa contraseñas seguras: Utiliza contraseñas fuertes y diferentes para cada cuenta. Evita utilizar contraseñas fáciles de adivinar, como "123456" o "contraseña". También evita utilizar la misma contraseña para varias cuentas.
2. Usa la autenticación de dos factores: La autenticación de dos factores agrega una capa adicional de seguridad al requerir una segunda forma de autenticación, como un código enviado a tu teléfono o una huella dactilar, además de tu contraseña.
3. Limita los privilegios de usuario: Limita los privilegios de usuario y restringe el acceso a los sistemas y datos sensibles solo a los usuarios autorizados. Esto puede ayudar a prevenir que los usuarios no autorizados accedan a los datos confidenciales.
4. Usa herramientas de monitoreo de acceso: Usa herramientas de monitoreo de acceso para registrar quién accede a los sistemas y datos sensibles, cuándo lo hacen y qué hacen mientras están allí. Esto puede ayudar a detectar actividades sospechosas y tomar medidas rápidamente.
5. Implementa políticas de seguridad: Implementa políticas de seguridad claras y aplicables para todos los empleados y contratistas. Las políticas de seguridad pueden incluir reglas sobre el uso de contraseñas seguras, la prohibición de compartir contraseñas, la responsabilidad de proteger la información confidencial, etc.
6. Educa a los usuarios: Educa a los usuarios sobre las mejores prácticas de seguridad informática, como el uso de contraseñas seguras, la protección de información confidencial y la detección de actividades sospechosas.
7. Usa tecnologías de seguridad: Usa tecnologías de seguridad, como firewalls, sistemas de detección de intrusos y sistemas de prevención de intrusiones, para proteger tus sistemas y datos sensibles.

* Intercepción de datos.

1. Usa conexiones seguras: Usa conexiones seguras, como HTTPS, SSL o TLS, para cifrar la comunicación entre tu dispositivo y el servidor. Estas conexiones cifran los datos que se envían y reciben, lo que dificulta que alguien los intercepte y los lea.
2. Usa redes seguras: Usa redes seguras, como una red privada virtual (VPN), para proteger tus datos mientras estás en línea. Una VPN cifra los datos que envías y recibes a través de la red, lo que ayuda a proteger tu información de posibles intrusos.
3. Actualiza tu software: Mantén tu software actualizado con las últimas versiones y parches de seguridad. Los desarrolladores de software suelen lanzar actualizaciones para solucionar vulnerabilidades conocidas y mejorar la seguridad.
4. Usa herramientas de seguridad: Usa herramientas de seguridad, como firewalls y software antivirus, para proteger tu dispositivo contra posibles amenazas. Estas herramientas pueden ayudar a detectar y bloquear la actividad malintencionada.
5. Sé consciente de los correos electrónicos y mensajes sospechosos: Ten cuidado al abrir correos electrónicos o mensajes sospechosos de remitentes desconocidos o que contengan enlaces o archivos adjuntos sospechosos. Estos pueden ser intentos de phishing para obtener acceso a tus datos.
6. Usa contraseñas seguras: Usa contraseñas seguras para tus cuentas y cambia las contraseñas regularmente. Evita usar contraseñas fáciles de adivinar o que hayas usado en otras cuentas.
7. Protege tus dispositivos: Usa contraseñas o patrones de desbloqueo para proteger tus dispositivos, y no los dejes desatendidos en lugares públicos.

## 3.4.3 Protección legal

La protección legal en la seguridad informática es esencial para garantizar la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos de una organización o individuo. Existen varias leyes y regulaciones que proporcionan un marco legal para la protección de los datos y sistemas informáticos.

Algunas de las leyes y regulaciones más relevantes en materia de seguridad informática incluyen:

Ley de Protección de Datos Personales: Esta ley establece las reglas para la recopilación, uso y protección de la información personal de los individuos.

En general, la ley de protección de datos personales establece lo siguiente:

Definición de datos personales: La ley define lo que se entiende por "datos personales", que incluye cualquier información que pueda identificar a un individuo, como el nombre, dirección, número de identificación, correo electrónico, número de teléfono, entre otros.

Consentimiento informado: La ley establece que la recopilación y uso de los datos personales solo puede realizarse con el consentimiento informado del individuo. Esto significa que la persona debe ser informada sobre el propósito de la recopilación de los datos y cómo serán utilizados.

Derechos de los individuos: La ley establece los derechos de los individuos en relación con sus datos personales, incluyendo el derecho de acceso, rectificación, cancelación y oposición.

Obligaciones de los responsables del tratamiento de los datos: La ley establece las obligaciones de las organizaciones o personas que recopilan, utilizan y almacenan datos personales, como garantizar la seguridad de los datos y notificar a los individuos en caso de una violación de datos.

Sanciones: La ley establece sanciones y multas en caso de incumplimiento de las reglas y principios de protección de datos personales.

Ley de Propiedad Intelectual: Esta ley protege los derechos de propiedad intelectual, como las patentes, marcas comerciales y derechos de autor, en el ámbito digital.

Algunos de los puntos importantes de la ley propiedad intelectual son:

Tipos de propiedad intelectual: La ley de propiedad intelectual protege varios tipos de propiedad intelectual, incluyendo patentes, marcas comerciales, derechos de autor, diseños industriales y secretos comerciales.

Protección de patentes: Las patentes protegen las invenciones y descubrimientos técnicos y conceden a su titular el derecho exclusivo de producir, vender y utilizar la invención por un período determinado.

Protección de marcas comerciales: Las marcas comerciales protegen los signos distintivos, como los nombres comerciales y los logotipos, y otorgan al titular el derecho exclusivo de usar la marca comercial en relación con los productos o servicios asociados a la marca.

Protección de derechos de autor: Los derechos de autor protegen las obras originales de autoría, como los libros, las películas y la música, y otorgan al titular el derecho exclusivo de reproducir, distribuir y mostrar la obra.

Protección de diseños industriales: Los diseños industriales protegen las características ornamentales o estéticas de un producto y otorgan al titular el derecho exclusivo de producir y vender productos que incorporen el diseño.

Secretos comerciales: La ley de propiedad intelectual también protege los secretos comerciales, como la información confidencial de una empresa, mediante la imposición de obligaciones de confidencialidad en las personas que tienen acceso a la información.

Sanciones por infracción: La ley de propiedad intelectual establece sanciones y multas en caso de infracción de los derechos de propiedad intelectual.

Ley de Delitos Informáticos: Esta ley establece los delitos informáticos, como el acceso no autorizado a sistemas informáticos, el robo de información y la distribución de virus informáticos.

Sus características son:

Amplia definición de delitos: La ley de delitos informáticos establece una amplia definición de los delitos informáticos, que pueden incluir actividades como el acceso no autorizado a sistemas informáticos, el robo de información, la distribución de virus informáticos, el ciberacoso y el fraude en línea.

Protección de la privacidad: La ley de delitos informáticos establece medidas para proteger la privacidad de los usuarios de Internet y de los sistemas informáticos, lo que incluye la protección de los datos personales y la privacidad de las comunicaciones electrónicas.

Investigación y recopilación de pruebas: La ley de delitos informáticos establece procedimientos para la investigación y la recopilación de pruebas de delitos informáticos, lo que incluye la intervención de comunicaciones electrónicas, el monitoreo de redes informáticas y la obtención de pruebas digitales.

Sanciones y penas: La ley de delitos informáticos establece sanciones y penas para las personas que cometen delitos informáticos, que pueden incluir multas, penas de prisión y otras sanciones, dependiendo de la gravedad del delito.

Cooperación internacional: La ley de delitos informáticos fomenta la cooperación internacional entre los países para prevenir y sancionar el cibercrimen, lo que incluye la extradición de delincuentes informáticos y la cooperación en la investigación y en la recopilación de pruebas.

Reglamento General de Protección de Datos (RGPD): Esta regulación establece las reglas para la protección de datos personales en la Unión Europea.

Información relevante acerca del reglamento de protección de datos

Ámbito de aplicación: El RGPD se aplica a todas las empresas y organizaciones que tratan datos personales de ciudadanos de la Unión Europea, independientemente de dónde se encuentren.

Consentimiento del titular de los datos: El RGPD establece que el tratamiento de datos personales solo es legal si el titular de los datos ha dado su consentimiento explícito para ello.

Derechos de los titulares de los datos: El RGPD establece una serie de derechos para los titulares de los datos, incluyendo el derecho a acceder a sus datos personales, el derecho a solicitar su eliminación, el derecho a la portabilidad de datos y el derecho a oponerse al tratamiento de sus datos personales.

Obligaciones de los responsables del tratamiento de datos: El RGPD establece una serie de obligaciones para las empresas y organizaciones que tratan datos personales, incluyendo la obligación de nombrar un delegado de protección de datos, la obligación de notificar a las autoridades en caso de una violación de datos y la obligación de realizar evaluaciones de impacto en la protección de datos.

Sanciones por incumplimiento: El RGPD establece multas significativas para las empresas y organizaciones que incumplen sus disposiciones, que pueden llegar hasta el 4% de la facturación global anual de la empresa.

Ley de Firma Electrónica: Esta ley regula el uso de firmas electrónicas y documentos electrónicos en transacciones comerciales.

Definición de firma electrónica: La ley de firma electrónica establece una definición de lo que se considera una firma electrónica, que puede incluir una firma manuscrita escaneada, una firma digital, un código PIN o cualquier otro método que permita identificar al firmante.

Características:

Validez jurídica: La ley de firma electrónica establece que las firmas electrónicas tienen la misma validez jurídica que las firmas manuscritas en los documentos impresos, siempre y cuando se cumplan ciertos requisitos de autenticidad y seguridad.

Tipos de firmas electrónicas: La ley de firma electrónica establece diferentes tipos de firmas electrónicas, que varían en nivel de seguridad y en requisitos de autenticidad, desde firmas electrónicas simples hasta firmas electrónicas avanzadas o cualificadas.

Procedimientos de autenticación: La ley de firma electrónica establece procedimientos para la autenticación y verificación de la identidad del firmante, lo que incluye la utilización de contraseñas, tokens, certificados digitales u otros medios de autenticación.

Responsabilidad legal: La ley de firma electrónica establece la responsabilidad legal de las partes involucradas en la utilización de firmas electrónicas, incluyendo al firmante, al proveedor de servicios de firma electrónica y a la entidad que recibe el documento firmado electrónicamente.

Es importante tener en cuenta que las leyes y regulaciones pueden variar según la región o país. Por lo tanto, es importante que las organizaciones y los individuos se informen sobre las leyes y regulaciones aplicables en su región y se aseguren de cumplir con ellas para proteger sus datos y sistemas informáticos.

# Bibliografía

Zanatta, M. (n.d.). Qué aspectos legales informáticos debes tener en cuenta en tu empresa. https://www.captio.net/blog/aspectos-legales-informatica-empresas

1.Conceptos básicos de seguridad informática - Seguridad informática Alberto Linares 2oSMR. (s. f.). https://sites.google.com/site/albertolinares2smr/1-conceptos-basicos-de-seguridad-informatica

Instituto Tecnológico Superior de Xalapa. (2019). Seguridad Informática: Conceptos básicos. studocu. https://www.studocu.com/es-mx/document/instituto-tecnologico-superior-de-xalapa/refrigeracion-y-aire-acondicionado/seguridad-informatica-conceptos-basicos/21796811

Seguridad Informática. (s. f.). http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/seguridadinformatica.aspx