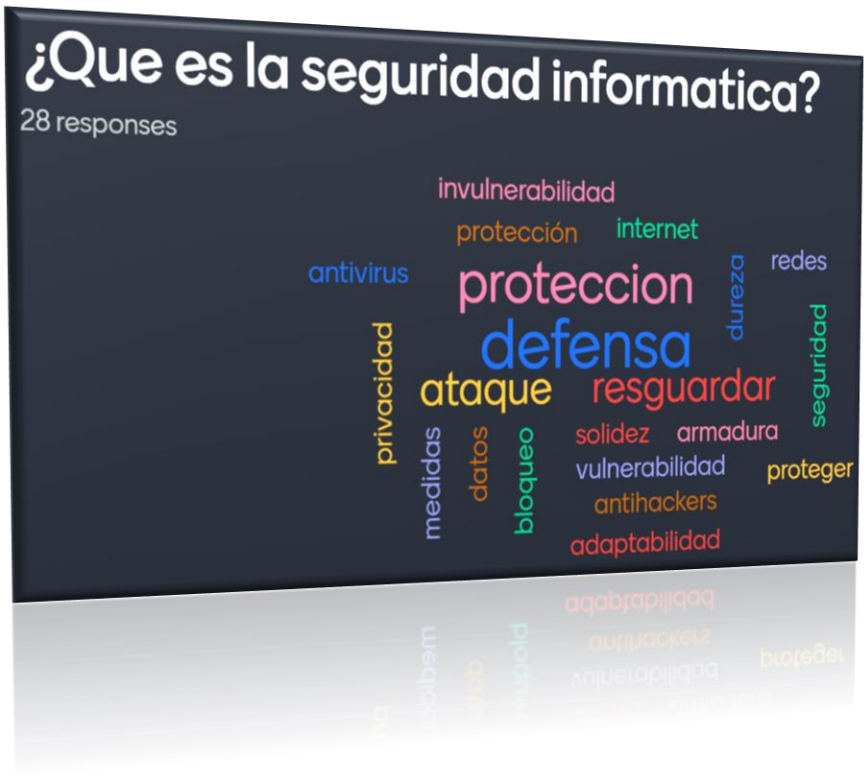
Universidad Paraguayo Alemana

UNIVERSIDAD PARAGUAYO ALEMANA
HEIDELBERG - ASUNCIÓN



Seguridad TICs

Prof.: Chrystian Ruiz Diaz

Contenido

Nota de Uso Académico

Este documento ha sido preparado exclusivamente para el uso académico del docente. Este documento no puede ser distribuido a ninguna otra parte ni utilizado para ningún otro propósito, diferente al establecido como alcance en el proyecto académico de la **UNIVERSIDAD PARAGUAYO ALEMANA**. El uso indebido del material fuera del ámbito académico no representa ninguna responsabilidad del docente.

VPN

¿QUÉ ES UNA RED PRIVADA RED PRIVADA VIRTUAL?

Una red privada virtual (VPN) es un mecanismo para establecer una conexión segura de acceso remoto a través de una red intermediario, a menudo Internet. Las VPNs permiten el acceso remoto, control remoto y comunicaciones altamente seguras dentro de una red privada. Las VPN emplean el cifrado y la autenticación para proporcionar confidencialidad, integridad y protección de la privacidad de las las comunicaciones de red.

El término VPN tiene su origen en el mundo de las telecomunicaciones. Una VPN telefónica creó un sistema similar a una centralita para para las empresas sin la necesidad de desplegar un verdadero de la centralita privada (PBX). En su lugar, el sistema utilizaba un servicio telefónico público y los servicios de PBX en las oficinas centrales centrales de la empresa de telecomunicaciones. Este servicio/producto se vendía con el nombre de Centrex (una combinación de central y de intercambio) en la década de 1960 hasta la década de 1980.

Tras la proliferación de las redes informáticas y la conectividad a Internet Internet, el término VPN evolucionó para referirse a las conexiones conexiones a través de enlaces de red. Las primeras VPN informáticas se centraban en los procesos de tunelización o encapsulación y rara vez incluían servicios de encriptación. Hoy en día, las VPN casi siempre están están aseguradas mediante encriptación. Sin embargo, nunca hay que dar por sentado que algo es totalmente seguro, especialmente las conexiones a través de redes públicas. Confirme siempre que un producto realiza encriptación correctamente antes de depender de él para operaciones operaciones sensibles.

Una VPN crea o simula una conexión de red a través de una red intermediaria. Pero, ¿qué hace que una VPN sea privada?

Existen varios mecanismos posibles:

La organización principal es propietaria de todos los componentes de la infraestructura de red componentes de la infraestructura de la red, incluidos los conmutadores, routers y cables. Una verdadera VPN privada se produce cuando una sola organización es propietaria de todo el hardware que soporta su VPN. Sin embargo, pocas organizaciones son propietarias de todas las conexiones entre sus ubicaciones, por lo que esto suele ser por lo que suele ser poco práctico o prohibitivo. Este sistema de propiedad exclusiva y operado constituye una VPN de confianza.

Se utiliza un conjunto de canales dedicados a través de conexiones alquiladas. Este método proporciona aislamiento físico incluso en equipos de terceros; por lo tanto, se

mantiene la privacidad. Este tipo de sistema es más práctico, pero sigue siendo caro. También puede llamarse VPN de confianza, ya que hay que debe poder confiar en el propietario de la infraestructura de alojamiento para proteger las comunicaciones de la red contra las escuchas. El cifrado garantiza la privacidad incluso en redes públicas, como como Internet. Este método es el más fiable, ya que las otras dos opciones siguen estando expuestas a las escuchas. Además, la encriptación para proporcionar privacidad no sólo es práctica, sino que también es la opción menos costosa. Este sistema puede denominarse VPN segura.

Una VPN híbrida establece una VPN segura sobre conexiones VPN de confianza. de confianza. Una VPN de confianza permite a una organización conocer y controlar la ruta de sus transmisiones. Sin embargo, una VPN de confianza no protege contra las escuchas o la alteración. Una VPN segura protege la confidencialidad y la integridad de los datos, pero no controla ni asegura la ruta de transmisión.

¿Cuáles son los beneficios de ¿desplegar una vpn?

Las razones para desplegar y utilizar las VPNs varían mucho entre organizaciones. El coste es siempre un factor importante en cualquier decisión empresarial. Los presupuestos nunca son ilimitados, por lo que las organizaciones deben considerar sus opciones en medio de fondos limitados para cumplir sus misiones y objetivos. Un objetivo común es la alta productividad. La concesión a los trabajadores de la capacidad de acceder y recursos de manera oportuna y eficiente ayuda a la finalización del trabajo. a la finalización del trabajo. Cuando esos recursos son archivos informáticos o servicios de red, los empleados ya no necesitan estar en el mismo edificio que esos recursos. El acceso remoto a los recursos por lo tanto, se está volviendo más común que nunca.

El acceso remoto seguro es esencial. A medida que la proliferación de acceso y la conectividad se extiende del trabajo al hogar y a los dispositivos portátiles/móviles, el acceso a Internet y a las LAN privadas se está convirtiendo en algo omnipresente. Las empresas deben utilizar controles de seguridad de seguridad en el acceso a los recursos o sufrir las consecuencias de métodos de acceso inseguros. Con la eliminación de las limitaciones físicas de las limitaciones físicas de acceso viene la pérdida de control sobre dónde y cómo se conectan los trabajadores a la LAN privada.

Los trabajadores pueden conectarse a la LAN de la empresa desde teléfonos móviles teléfonos móviles, a través de cibercafés, en redes de hoteles y en otros puntos de acceso Wi-Fi aleatorios. En esta época de "Traiga su propio dispositivo (BYOD), muchos utilizan ordenadores portátiles de propiedad personal

¿Cuáles son los beneficios de ¿desplegar una vpn?

Las razones para desplegar y utilizar las VPNs varían mucho entre organizaciones. El coste es siempre un factor importante en cualquier decisión empresarial. Los presupuestos nunca son ilimitados, por lo que las organizaciones deben considerar sus opciones en medio de fondos limitados para cumplir sus misiones y objetivos. Un objetivo

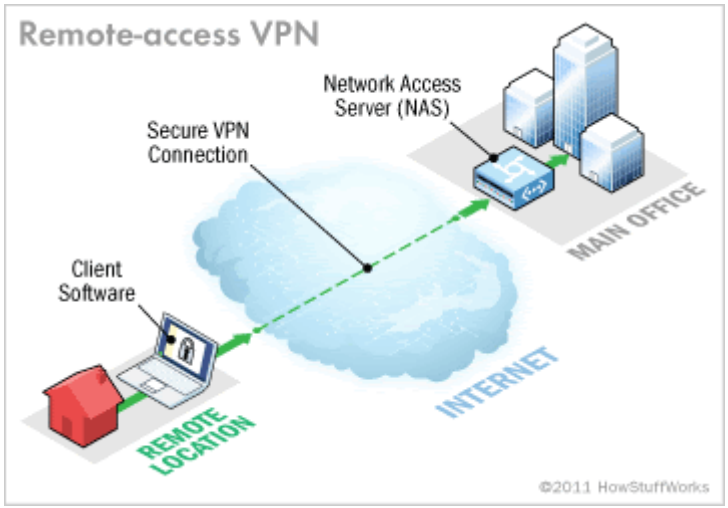
común es la alta productividad. La concesión a los trabajadores de la capacidad de acceder y recursos de manera oportuna y eficiente ayuda a la finalización del trabajo. a la finalización del trabajo. Cuando esos recursos son archivos informáticos o servicios de red, los empleados ya no necesitan estar en el mismo edificio que esos recursos. El acceso remoto a los recursos por lo tanto, se está volviendo más común que nunca.

El acceso remoto seguro es esencial. A medida que la proliferación de acceso y la conectividad se extiende del trabajo al hogar y a los dispositivos portátiles/móviles, el acceso a Internet y a las LAN privadas se está convirtiendo en algo omnipresente. Las empresas deben utilizar controles de seguridad de seguridad en el acceso a los recursos o sufrir las consecuencias de métodos de acceso inseguros. Con la eliminación de las limitaciones físicas de las limitaciones físicas de acceso viene la pérdida de control sobre dónde y cómo se conectan los trabajadores a la LAN privada.

Arquitecturas VPN

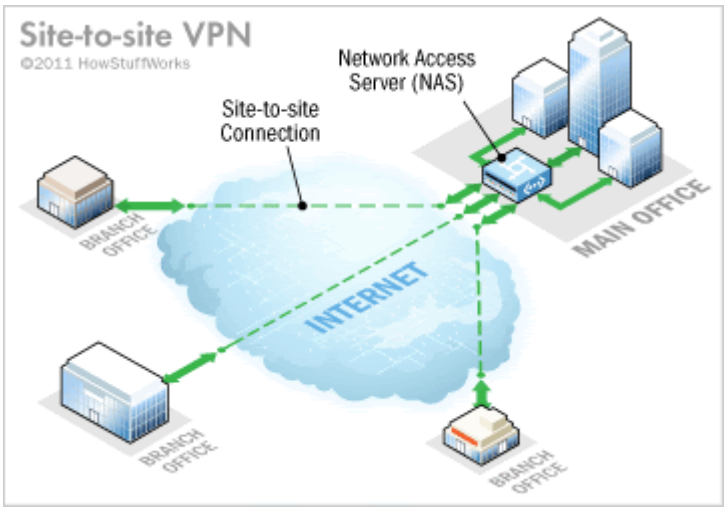
Además de la selección del dispositivo VPN, hay que tomar varias decisiones de arquitectura que hay que tomar. Éstas se centran en el propósito, la función o el uso de la VPN propósito, función o uso de la VPN, como el acceso remoto, acceso remoto, de host a host, de sitio a sitio y de extranet.

Remote Access



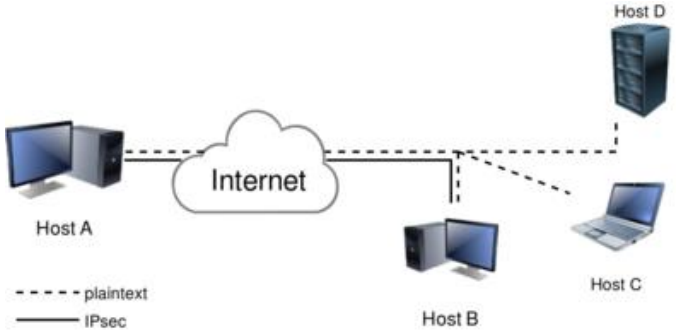
La VPN de acceso remoto también se conoce como VPN host-to-site porque admite conexiones VPN de un solo host en un sitio LAN. Este diseño permite a los teletrabajadores individuales o a los trabajadores que viajan trabajadores que viajan, un fácil acceso a la LAN privada. Una única LAN puede soportar varios usuarios remotos con cualquiera de los conceptos de punto final VPN de VPN: router de borde, firewall corporativo o dispositivo VPN.

Site-to-Site



Las VPN de sitio a sitio también se conocen como VPN de LAN a LAN o conexiones VPN WAN entre LANs. Independientemente del nombre, una VPN de sitio a sitio soporta conexiones seguras entre LANs a través de redes públicas intermediarias. Cuando se instala Cuando se instala correctamente, una VPN de sitio a sitio puede ser un mecanismo económico para crear una única LAN distribuida (también conocida como WAN) para una organización con múltiples ubicaciones. Una VPN de sitio a sitio utiliza cualquiera de los conceptos de punto final de VPN: router de borde, cortafuegos corporativo o dispositivo VPN.

Host-to-Host



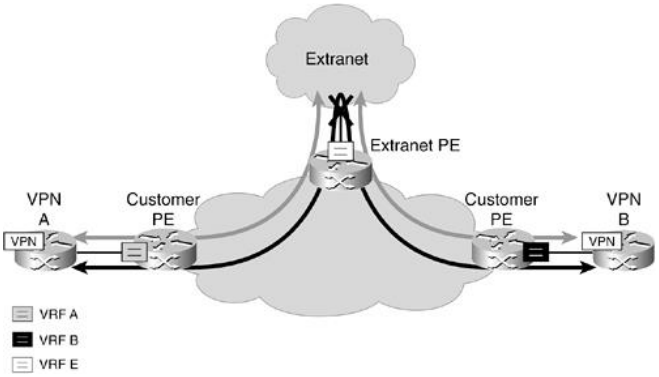
Una tercera arquitectura VPN es la de host-to-host. Las VPN de host a host también se conocen como VPN de cliente a servidor, de remoto a oficina o de remoto a casa. Una VPN de host a host es una conexión VPN directa entre un host y otro. Este mecanismo funciona en una red pública o en una red privada. En una red pública, una VPN de host a host proporciona una conexión segura desde el público. En una red privada red privada, proporciona un nivel adicional de seguridad para las transacciones o transacciones altamente sensibles.

Las VPN de host a host etiquetadas como VPN de cliente a servidor crean una interacción segura del cliente con los servicios de un recurso de recursos. Esto es similar, pero no exactamente igual, a un enlace web seguro entre un navegador web y un servidor. entre un navegador web y un servidor web. SSL puede ser utilizarse para la seguridad del protocolo de la aplicación, como ocurre con las sesiones o como protocolo VPN. Como protocolo VPN, SSL funciona en la capa de red de la Interconexión de Sistemas Abiertos (OSI). Interconexión de Sistemas Abiertos (OSI); como herramienta de seguridad de como herramienta de seguridad de la sesión web, opera en la Capa de Transporte.

Una VPN remota a la oficina es un enlace directo entre un sistema portátil o doméstico y una estación de trabajo de oficina. Este enlace VPN permite a un usuario trabajar desde casa o mientras viaja sin sacrificar el acceso a recursos, servicios o aplicaciones que sólo pueden estar instalados (o con licencia) para su uso en el ordenador

de la estación de trabajo de la oficina. de la oficina. Esta VPN puede establecer una sesión de control remoto con la misma facilidad que una sesión de acceso remoto.

Extranet Access



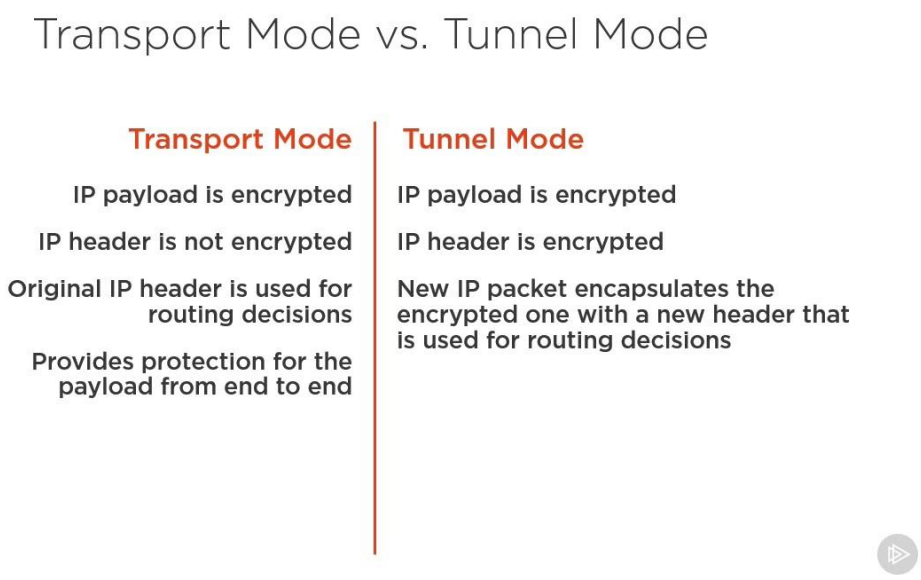
Una cuarta arquitectura VPN es el acceso a la extranet. Con un punto final de túnel VPN túnel VPN situado en el perímetro de una extranet o dentro de él. extranet, esta opción sirve como vía para que los socios comerciales distribuidores, proveedores, etc. para acceder a los recursos corporativos sin exponer su tráfico a Internet ni o concederles un acceso innecesario a la LAN privada.

Una VPN conectada a la extranet, a diferencia de la DMZ proporciona mayor seguridad a las entidades remotas. Un enlace VPN a la DMZ expone a las entidades remotas a cualquier amenaza que se encuentre en la DMZ. Dado que la DMZ es de acceso público, es arriesgada. Una VPN extranet de VPN de extranet garantiza a la entidad remota comunicaciones seguras comunicaciones seguras sin riesgos significativos en el punto de punto de terminación de la VPN.

Las VPN suelen servir como punto de estrangulamiento para controlar qué entidades externas tienen acceso a la extranet. Sólo aquellos a los que se les ha concedido acceso específico, las cuentas de usuario asignadas y los detalles de detalles de configuración son capaces de configurar y establecer un enlace VPN con una extranet.

TUNNEL VERSUS TRANSPORT MODE

Las VPNs pueden utilizar dos tipos principales de encapsulación de cifrado. Se conocen como cifrado en modo túnel y en modo transporte de transporte.



El cifrado en modo túnel protege todo el encabezado y la carga útil del paquete IP original. original y la carga útil del paquete. El paquete encriptado se convierte en la carga útil de un nuevo paquete IP con una nueva cabecera IP. Esta forma Esta forma de encriptación asegura que las identidades de los originales de la comunicación se mantienen confidenciales mientras el mientras el tráfico atraviesa el enlace seguro. El cifrado en modo túnel es comúnmente utilizado por las VPN que conectan sitios de red entre sí o que proporcionan un acceso remoto seguro.

El cifrado en modo transporte sólo protege la carga útil del paquete IP original. original del paquete. La carga útil cifrada conserva su cabecera IP original. original. Esta forma de encriptación sólo protege la carga útil, no las identidades de los puntos finales. El cifrado en modo transporte ayuda a las VPN a enlazar ordenadores individuales.

LA RELACIÓN ENTRE EL CIFRADO Y LAS VPNS

El cifrado y una VPN segura son prácticamente inseparables. A VPN segura sólo existe porque el tráfico está cifrado, pero algunas VPN de confianza pueden o no utilizar el cifrado. Para entender entender y apreciar el funcionamiento de las VPNs, necesitas un comprensión razonable de la encriptación.

El cifrado es sólo un aspecto del tema más amplio de la criptografía. La criptografía es el arte y la ciencia de cambiar la información para que no sea fácilmente reconocida o que no sea fácilmente reconocida o entendida por terceros no autorizados. La criptografía se produce a través de un conjunto de

procesos complementarios y reversibles: el cifrado y el descifrado. El cifrado es el proceso de convertir los datos originales utilizables, llamados texto plano, en una forma caótica inutilizable, llamada texto cifrado. La desencriptación es el proceso de convertir el texto cifrado en texto plano. Un producto de comunicación producto de comunicación seguro debe proporcionar tanto encriptación como descifrado.

VPN Deployment Models and Architecture

Una de las primeras decisiones a las que se enfrenta al desplegar una VPN es,

¿Qué dispositivo puede servir como punto de terminación del túnel seguro?

Tiene varias opciones, pero a menudo la decisión se basa en el lugar de la infraestructura de red en el que desea situar el punto final del túnel. Además, las características que ofrece el dispositivo VPN pueden ser un factor de decisión.

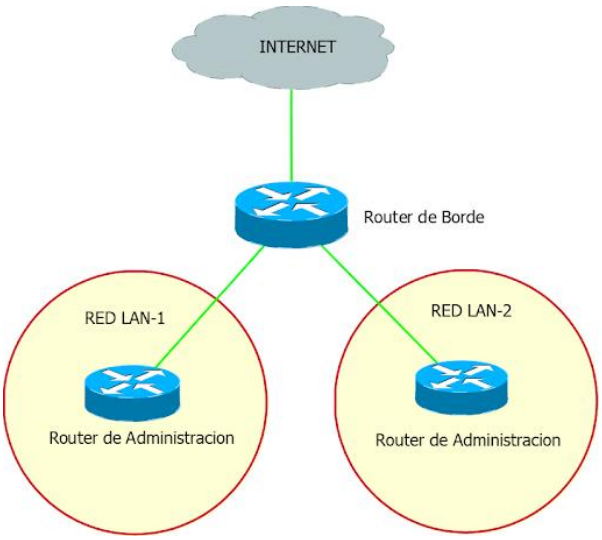
Estos factores incluyen la decisión de qué dispositivos tienen suficiente potencia de procesamiento potencia de procesamiento suficiente para mantener la velocidad de los cables incluso con un tráfico intenso y un cifrado complejo. Otra preocupación es si hay NAT, ya que esto puede imponer problemas para encriptación en modo túnel.

Los tres principales modelos de dispositivos VPN son el router de borde, el firewall corporativo y el dispositivo VPN. Además de la selección del dispositivo VPN, hay que varias decisiones arquitectónicas que tomar. Estas se centran en el propósito previsto, función o uso de la VPN, como el acceso remoto, de host a host, de sitio a sitio y acceso a la extranet.

Edge Router

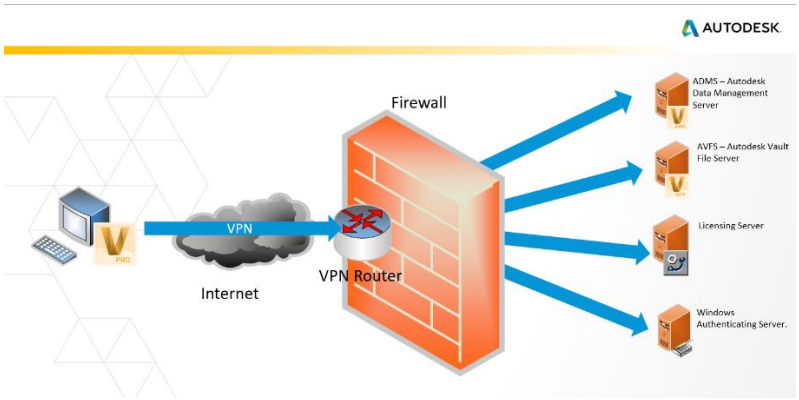
Con los routers de borde como punto de terminación de la VPN, el enlace VPN sólo existe sobre las redes públicas intermediarias, no dentro de la(s) LAN(s) privada(s). Esto requiere requiere que el router de borde soporte la conectividad VPN.

La terminación de la VPN del router de borde garantiza que un cortafuegos pueda filtrar el tráfico que sale de la VPN en su camino hacia la LAN. Este método garantiza que todo el tráfico, independientemente del medio de transporte, cumpla con las reglas de filtrado del cortafuegos. Si la VPN termina dentro del cortafuegos, el tráfico de la VPN podría



Firewall corporativo

La terminación de la VPN en el firewall corporativo es posible si el firewall soporta servicios VPN. No todos los cortafuegos proporcionan este servicio, por lo que esto depende de su elección de la marca y el modelo del producto de cortafuegos.



Con una VPN de cortafuegos a cortafuegos VPN a través de la red pública, los usuarios de una red LAN pueden acceder recursos en otra red LAN sin complejidades adicionales. Principalmente, esta configuración trata el enlace de la VPN entre los puntos finales del cortafuegos como una ruta más en la LAN (en realidad, una ruta W). otra ruta en la LAN (en realidad WAN). El beneficio aquí es que los usuarios no no tienen que volver a autenticarse ni cumplir con las restricciones adicionales del cortafuegos cuando la VPN termina en el firewall corporativo.

VPN Appliance

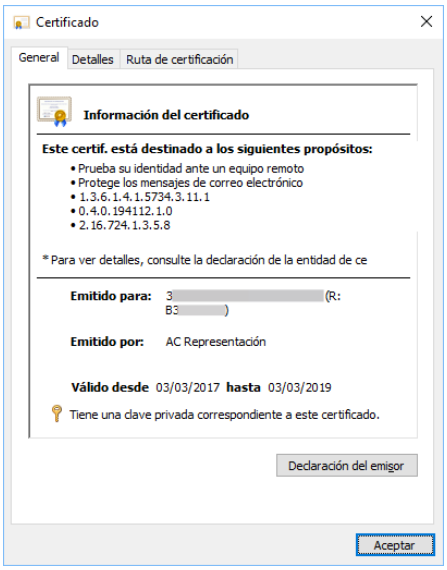
Una tercera opción de dispositivo es un dispositivo VPN dedicado. A diferencia de un router de borde o punto de terminación del cortafuegos, un dispositivo VPN dedicado maneja específicamente la carga de una VPN en lugar de que el soporte de VPN sea un servicio adicional.

Puede colocar un dispositivo VPN fuera del cortafuegos de la empresa, en un entorno similar al de la red.

Un dispositivo VPN también puede residir dentro de los cortafuegos corporativos para evitar la filtración del cortafuegos. Este despliegue es similar al concepto de cortafuegos corporativo, al menos en términos de no filtrar el tráfico VPN. Este segundo método de despliegue también garantiza que ninguna entidad externa pueda interferir con los puntos finales del túnel VPNtúnel (STEWART, 2013)

Certificados Digitales

Para solucionar el problema de la autenticación en las transacciones por Internet se buscó algún sistema identificativo único de una entidad o persona. Ya existían los sistemas criptográficos de clave simétrica, mediante los cuales una persona disponía de dos claves, una pública, al alcance de todos, y otra privada, solo conocida por el propietario.



El problema era asegurar que, efectivamente, la clave pública que se recibía era de la persona correcta y no de un suplantador. Entonces se pensó en implementar una especie de documento de identidad electrónica que identificara sin lugar a duda a su emisor.

La solución a este problema vino con la aparición de los certificados digitales o certificados electrónicos, documentos electrónicos basados en la criptografía de clave pública y en el sistema de firmas digitales.

La **misión principal de un certificado digital** es garantizar, con toda confianza, el vínculo existente entre una persona, entidad o servidor web con una pareja de claves correspondientes a un sistema criptográfico de clave pública.

Concepto y características

El certificado digital, certificado de clave pública o certificado de usuario, es un documento electrónico, identificado por un número de serie único y con un periodo de validez incluido en el propio certificado, que contiene varios datos. Está emitido por una entidad de confianza, denominada autoridad de certificación y vincula a su propietario con una clave pública.

Un certificado emitido por una autoridad certificadora, además de estar firmado digitalmente por esta, debe contener por lo menos lo siguiente:

– Nombre, dirección y domicilio del suscriptor.

– Identificación del suscriptor nombrado en el certificado.

– El nombre, la dirección y el lugar donde realiza actividades la entidad

de certificación.

– La clave pública del usuario.

– La metodología para verificar la firma digital del suscriptor impuesta

en el mensaje de datos.

– El número de serie del certificado

– Fecha de emisión y expiración del certificado.

Como el certificado está firmado por la autoridad de certificación, se garantiza que el mensaje no ha sido modificado (**la firma garantiza la integridad del mensaje**), que la clave pública pertenece al usuario con el identificador indicado y que el certificado es accesible para todos (para poder leer el certificado es necesaria la clave pública de la

autoridad de certificación, que se pone a disposición de todo el mundo). Para comprobar la autenticidad de un certificado, hay que tener instalado en el equipo el certificado raíz de la autoridad certificadora, mientras que su vigencia puede comprobarse consultando el propio certificado y acudiendo a la autoridad certificadora para cerciorarse de que el certificado no ha sido revocado.

Existen varios tipos de certificados, pero los más usados se rigen por el estándar

UIT-T X.509. Su estructura es la siguiente:

– Certificado:

• Versión.

• Número de serie.

• ID del algoritmo.

• Organismo emisor.

• Periodo de validez.

• Información de la clave pública del usuario.

• Otros campos opcionales (ID del emisor, ID del usuario, etc.).

– Algoritmo usado para firmar el certificado.

– Firma digital del certificado.

Los certificados no se emiten con carácter indefinido, sino que, como se ha indicado mas arriba, deben expresar su fecha de expiración, pasada la cual dejarán de tener validez. El periodo de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos, este periodo no podrá ser superior a cuatro años.

No obstante, esto, un certificado puede ser renovado antes de que expire su periodo de validez.

También es posible revocar un certificado. Revocar un certificado significa privarle de validez antes de que finalice el periodo incluido en el propio certificado. Un certificado puede ser revocado por los siguientes motivos:

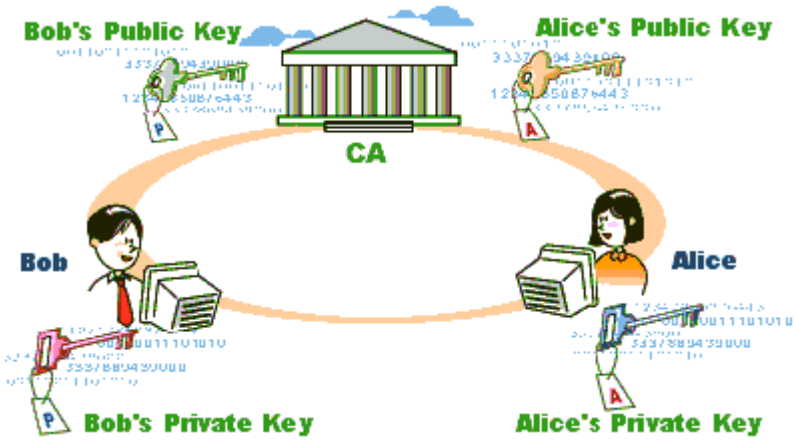
– Los datos que contiene han dejado de ser válidos.

– La clave privada ha sido comprometida o ha llegado a conocimiento de terceras personas.

– El certificado ha dejado de tener validez dentro del contexto para el que ha sido emitido.

Autoridades de certificación

Una autoridad de certificación (AC o CA por sus siglas en inglés *Certification Authority*) es una entidad a la que uno o más usuarios confían la creación, asignación y revocación de los certificados digitales. Su misión es asegurar que un certificado es válido, está vigente y corresponde al usuario poseedor del mismo. Por tanto, permiten garantizar la autenticidad y veracidad de los datos que aparecen en los certificados digitales.



En resumen, las autoridades de certificación son responsables de la emisión y administración de los certificados y del mantenimiento de las listas de revocación de certificados.

Algunas autoridades certificadoras son:

– A nivel español: CERES, desarrollada por la Fábrica Nacional de Moneda y Timbre (FNMT); la Dirección General de la Policía (para la obtención del DNIe); la Autoridad de Certificación de la Abogacía (ACA), etc.

– A nivel internacional: Verisign, GlobalSign, Thawte Certification, Go- Daddy, Comodo, etc.

– En Paraguay

https://www.digito.com.py/

https://www.code100.com.py/

https://www.efirma.com.py/

Otros…

Uso de los certificados

Los certificados de usuario pueden ser utilizados tanto para firmar documentos como para garantizar la confidencialidad en las comunicaciones.

En este caso, los pasos del proceso serían los siguientes.

Clases de certificados

Existen multitud de clases de certificados digitales, que generalmente se diferencian en función de la entidad certificadora que los emite y de su finalidad. Así, por ejemplo, CERES diferencia, atendiendo a sus destinatarios, entre certificados de persona física, de persona jurídica y de entidad sin personalidad jurídica.

Otros organismos reconocen otros certificados personales o corporativos, como por ejemplo los certificados de pertenencia a empresa, de atributo (profesión, cargo, etc.), de representación de empresa, etc.

También se distinguen distintos tipos de certificados atendiendo a su función:

– Certificados de servidor seguro: identifican que una página web pertenece a una determinada persona o empresa y que la información transmitida

entre el servidor y los usuarios de la web está cifrada y es segura.

– Certificado de firma de código: se usa para asegurar que el código que se ejecuta ha sido firmado por su desarrollador y no es malicioso (ESCRIVA, 2013).

CERTs

CERT (del inglés *Computer Emergency Response Team)* O Equipo de Respuesta ante Emergencias Informáticas es un centro de respuesta a incidentes de seguridad en tecnologías de la información.

Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

CERT-PY Centro de Respuestas a Incidentes Cibernéticos dependiente de la Dirección General de Ciberseguridad del Ministerio de Tecnologías de la Información y Comunicación, fue creada el 30 de Noviembre del 2012 con el objetivo principal de actuar como coordinador central para las notificaciones de incidentes de seguridad en Paraguay, dando el apoyo necesario para dar respuesta a estos incidentes, actuando como coordinador entre las partes afectadas e involucradas para la solución de los mismos (MITIC, 2021).

Funciones

- Implementar mecanismos de gestión, coordinación, respuesta e investigación de incidentes cibernéticos que pongan en riesgo el ecosistema digital nacional.
- Implementar y promover los mecanismos de monitoreo y detección de incidentes cibernéticos en organismos y entidades del Estado, así- como también en las infraestructuras crí-ticas nacionales.

- Establecer e incentivar mecanismos de intercambio de información relacionado a incidentes cibernéticos y amenazas, entre el sector gubernamental, privado, regional e internacional.
- Implementar mecanismos y desarrollar actividades para la generación, captación, procesamiento y análisis de información de ciberseguridad entre actores del ecosistema.
- Implementar y promover mecanismos de alerta temprana a incidentes y amenazas.

SOFTWARE MALICIOSO

Con el nombre **software malicioso o malware** agrupamos los virus, gusanos, troyanos y en general todos los tipos de programas que han sido desarrollados para entrar en ordenadores sin permiso de su propietario, y producir efectos no deseados. Estos efectos se producen algunas veces sin que nos demos cuenta en el acto.

¿Qué son los virus?

Los virus son programas maliciosos creados para manipular el normal funcionamiento de los sistemas, sin el conocimiento ni consentimiento de los usuarios.

Breve Historia

En sus comienzos, la motivación principal para los creadores de virus era la del reconocimiento público. Cuanta más relevancia tuviera el virus, más reconocimiento obtenía su creador. Por este motivo, las acciones a realizar por el virus debían ser visibles por el usuario y suficientemente dañinas como para tener relevancia, por ejemplo, eliminar ficheros importantes, modificar los caracteres de escritura, formatear el disco duro, etc.

Sin embargo, la evolución de las tecnologías de la comunicación y su penetración en casi todos los aspectos de la vida diaria ha sido vista por los ciberdelincuentes como un negocio muy lucrativo. Los creadores de virus han pasado a tener una motivación económica, por lo que actualmente son grupos mucho más organizados que desarrollan los códigos maliciosos con la intención de que pasen lo más desapercibidos posible, y dispongan de más tiempo para desarrollar sus actividades maliciosas.

¿A qué afectan los códigos maliciosos?

Los programas maliciosos afectan a cualquier dispositivo que tenga un sistema operativo que pueda entender el fichero malicioso, es decir:

- Ordenadores personales.
- Servidores.
- Teléfonos móviles.
- PDA.
- Videoconsolas.

Motivación: inicialmente reconocimiento público, mayormente beneficio económico.

Formas de obtener beneficios económicos:

- Robo información sensible del ordenador infectado
- Crear una red de Botnet
- Vender falsas soluciones de seguridad
- Cifrar el contenido de los ficheros del ordenador y solicitar un "rescate"

CLASIFICACIÓN

Según Su Capacidad De Propagación

Virus: Su nombre es una analogía a los virus reales ya que infectan otros archivos, es decir, sólo pueden existir en un equipo dentro de otro fichero.

Gusanos. Son programas cuya característica principal es realizar el máximo número de copias posible de sí mismos para facilitar su propagación. A diferencia de los virus no infectan otros ficheros. Los gusanos se suelen propagar por los siguientes métodos:

- Correo electrónico.
- Redes de compartición de ficheros (P2P).
- Explotando alguna vulnerabilidad.
- Mensajería instantánea.
- Canales de chat.

Troyanos. Carecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas, las más comunes son:

- Descargado por otro programa malicioso.
- Descargado sin el conocimiento del usuario al visitar una página web maliciosa.
- Dentro de otro programa que simula ser inofensivo

Según Las Acciones Que Realizan

Adware. Muestra publicidad, generalmente está relacionado con los espías, por lo que se suelen conectar a algún servidor remoto para enviar la información recopilada y recibir publicidad.

Bloqueador. Impide la ejecución de determinados programas o aplicaciones, también puede bloquear el acceso a determinadas direcciones de Internet. Generalmente impiden la ejecución de programas de seguridad para que, de este modo, resulte más difícil la detección y eliminación de programas maliciosos del ordenador

Bomba lógica. Programa o parte de un programa que se instala en un ordenador y no se ejecuta hasta que se cumple determinada condición, por ejemplo, ser una fecha concreta, ejecución de determinado archivo.

Broma (Joke). No realiza ninguna acción maliciosa en el ordenador infectado pero, mientras se ejecuta, gasta una "broma" al usuario haciéndole pensar que su ordenador está infectado, por ejemplo, mostrando un falso mensaje de que se va a borrar todo el contenido del disco duro o mover el ratón de forma aleatoria.

Bulo (Hoax). Mensaje electrónico enviado por un conocido que intenta hacer creer al destinatario algo que es falso, como alertar de virus inexistentes, noticias con contenido engañoso, etc. y solicitan ser reenviado a todos los contactos. Algunos de estos mensajes pueden ser peligrosos por la alarma innecesaria que generan y las acciones que, en ocasiones, solicitan realizar al usuario, por ejemplo, borrando ficheros del ordenador que son necesarios para el correcto funcionamiento del equipo.

Capturador de pulsaciones (Keylogger). Monitoriza las pulsaciones del teclado que se hagan en el ordenador infectado, su objetivo es poder capturar pulsaciones de acceso a determinadas cuentas bancarias, juegos en línea o conversaciones y mensajes escritos en la máquina.

Clicker. Redirecciona las páginas de Internet a las que intenta acceder el usuario, de este modo logra aumentar el número de visitas a la página redireccionada, realizar ataques de Denegación de Servicio a una página víctima o engañar al usuario sobre la página que está visitando, por ejemplo, creyendo que está accediendo a una página legítima de un banco cuando en realidad está accediendo a una dirección falsa.

Criptovirus (Ransomware). Hace inaccesibles determinados ficheros en el ordenador y coacciona al usuario víctima a pagar un "rescate" (ransom en inglés) para poder acceder a la información. Generalmente lo que se hace es cifrar los ficheros con los que suela trabajar el usuario, por ejemplo, documentos de texto, hojas Excel, imágenes…

Descargador (Downloader). Descarga otros programas (generalmente también maliciosos) en el ordenador infectado. Suelen acceder a Internet para descargar estos programas

Espía (Spyware). Roba información del equipo para enviarla a un servidor remoto. El tipo de información obtenida varía según el tipo de espía, algunos recopilan información relativa a los hábitos de uso del ordenador, como el tiempo de uso y páginas visitadas en Internet; sin embargo, otros troyanos son más dañinos y roban información confidencial como nombres de usuario y contraseñas. A los espías que roban información bancaria se les suele llamar "troyanos bancarios".

Exploit. Tipo del software que se aprovecha de un agujero o de una vulnerabilidad en el sistema de un usuario para tener el acceso desautorizado al sistema

Herramienta de fraude. Simula un comportamiento anormal del sistema y propone la compra de algún programa para solucionarlo. Los más comunes son los falsos antivirus, que informan de que el ordenador está infectado, cuando en realidad el principal programa malicioso que tiene es la herramienta fraudulenta.

Instalador (Dropper). Instala y ejecuta otros programas, generalmente maliciosos, en el ordenador

Ladrón de contraseñas (PWStealer). Roba nombres de usuario y contraseñas del ordenador infectado, generalmente accediendo a determinados ficheros del ordenador que almacenan esta información

Marcador (Dialer). Actúa cuando el usuario accede a Internet, realizando llamadas a Números de Tarificación Adicional (NTA), lo que provoca un considerable aumento en

la factura telefónica del usuario afectado. Este tipo de programas está actualmente en desuso porque sólo funcionan si la conexión a Internet se hace a través del Módem, no se pueden realizar llamadas a NTA en conexiones ADSL o WiFi.

Puerta trasera (Backdoor). Permite el acceso de forma remota a un sistema operativo, página web o aplicación, haciendo que el usuario evite las restricciones de control y autenticación que haya por defecto. Puede ser utilizado por responsables de sistemas o webmasters con diversos fines dentro de una organización, pero también puede ser utilizado por atacantes para realizar varias acciones en el ordenador infectado

Rootkit. Toma control de Administrador ("root" en sistemas Unix/Linux) en el sistema, generalmente para ocultar su presencia y la de otros programas maliciosos en el equipo infectado; la ocultación puede ser para esconder los ficheros, los procesos generados, conexiones creadas…

También pueden permitir a un atacante remoto tener permisos de Administrador para realizar las acciones que desee.

Cabe destacar que los rootkits hay veces que se utilizan sin fines maliciosos.

Secuestrador del navegador (browser hijacker). Modifica la página de inicio del navegador, la página de búsqueda o la página de error por otra de su elección, también pueden añadir barras de herramientas en el navegador o incluir enlaces en la carpeta de "Favoritos". Todas estas acciones las realiza generalmente para aumentar las visitas de la página de destino.

OTRAS CLASIFICACIONES

Ladrones de información (infostealers). Agrupa todos los tipos de códigos maliciosos que roban información del equipo infectado, son los capturadores de pulsaciones, espías y ladrones de contraseñas

Código delictivo (crimeware). Hace referencia a todos los programas que realizan una acción delictiva en el equipo, básicamente con fines lucrativos. Engloba a los ladrones de información, mensajes de phishing y clickers que redirecciona al usuario a falsas páginas bancarias o de seguridad. Las herramientas de fraude, marcadores y criptovirus también forman parte de esta categoría.

Greyware (grayware). Engloba todas las aplicaciones que realizan alguna acción que no es, al menos de forma directa, dañina, tan sólo molesta o no deseable. Agrupa el adware, espías que sólo roban información de costumbres del usuario (páginas por las que navegan, tiempo que navegan por Internet…), bromas y bulos (COSTAS SANTOS, 2014)

ANALISIS DE RIESGOS

Fase 1. Definir el alcance

El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Director de Seguridad. Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad. Por otra parte, también es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas. Por ejemplo, análisis de riesgos sobre los procesos del departamento Administración, análisis de riesgos sobre los procesos de producción y gestión de almacén o análisis de riesgos sobre los sistemas TIC relacionados con la página web de la empresa, etc. En este caso práctico consideramos que el alcance escogido para el análisis de riesgos es "Los servicios y sistemas del Departamento Informática".

Fase 2. Identificar los activos

Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Para mantener un inventario de activos sencillo puede ser suficiente con hacer uso de una hoja de cálculo o tabla como la que se muestra a continuación a modo de ejemplo:

ID	Nombre	Descripción	Responsable	Tipo	Ubicación	Crítico
ID_01	Servidor 01	Servidor de contabilidad.	Director Financiero	Servidor (Físico)	Sala de CPD1	Sí
ID_02	RouterWifi	Router para la red WiFi de cortesía a los clientes.	Dept. Informática	Router (Físico)	Sala de CPD1	No
ID_03	Servidor 02	Servidor para la página web corporativa.	Dept. Informática	Servidor (Físico)	CPD externo	Sí
...						

Fase 3. Identificar / seleccionar las amenazas

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado. Por ejemplo, si nuestra intención es evaluar el riesgo que corremos frente a la destrucción de nuestro servidor de ficheros, es conveniente, considerar las averías del servidor, la posibilidad de daños por agua (rotura de una cañería) o los daños por fuego, en lugar de plantearnos el riesgo de que el CPD sea destruido por un meteorito.

A la hora de identificar las amenazas, puede ser útil tomar como punto de partida el catálogo de amenazas que incluye la metodología MAGERIT v3.

Fase 4. Identificar vulnerabilidades y salvaguardas

La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyo sistemas antivirus no están actualizados o una serie de activos para los que no existe soporte ni mantenimiento

por parte del fabricante. Posteriormente, a la hora de evaluar el riesgo aplicaremos penalizaciones para reflejar las vulnerabilidades identificadas.

Por otra parte, también analizaremos y documentaremos las medidas de seguridad implantadas en nuestra organización. Por ejemplo, es posible que hayamos instalado un sistema SAI (Sistema de Alimentación Ininterrumpida) o un grupo electrógeno para abastecer de electricidad a los equipos del CPD. Ambas medidas de seguridad (también conocidas como salvaguardas) contribuyen a reducir el riesgo de las amenazas relacionadas con el corte de suministro eléctrico.

Estas consideraciones (vulnerabilidades y salvaguardas) debemos tenerlas en cuenta cuando vayamos a estimar la probabilidad y el impacto como veremos en la siguiente fase.

Fase 5. Evaluar el riesgo

Llegado a este punto disponemos de los siguientes elementos:

• Inventario de activos.

• Conjunto de amenazas a las que está expuesta cada activo.

• Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).

• Conjunto de medidas de seguridad implantadas

Con esta información, nos encontramos en condiciones de calcular el riesgo. Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos. Pero para entenderlo mejor, veremos a modo de ejemplo las tablas para estimar los factores probabilidad e impacto.

Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Cálculo del riesgo

A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto:

RIESGO = PROBABILIDAD x IMPACTO.

Si por el contrario hemos optado por el análisis cualitativo, haremos uso de una matriz de riesgo como la que se muestra a continuación:

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Tal y como indicábamos en el apartado anterior, cuando vayamos a estimar la probabilidad y el impacto debemos tener en cuenta las vulnerabilidades y salvaguardas existentes. Por ejemplo, la caída del servidor principal podría tener un impacto alto para el negocio. Sin embargo, si existe una solución de alta disponibilidad (Ej. Servidores redundados), podemos considerar que el impacto será medio ya que estas medidas de seguridad harán que los procesos de negocio no se vean gravemente afectados por la caída del servidor. Si por el contrario hemos identificado vulnerabilidades asociadas al activo, aplicaremos una penalización a la hora de estimar el impacto. Por ejemplo, si los equipos de climatización del CPD no han recibido el mantenimiento recomendado por el

fabricante, incrementaremos el impacto de amenazas como “condiciones ambientales inadecuadas” o “malfuncionamiento de los equipos debido a altas temperaturas”.

Fase 6. Tratar el riesgo

Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. Por ejemplo, trataremos aquellos riesgos cuyo valor sea superior a “4” o superior a “Medio” en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

• **Transferir el riesgo a un tercero**. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.

• **Eliminar el riesgo**. Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado. En el caso práctico que hemos expuesto, podríamos eliminar la wifi de cortesía para dar servicio a los clientes si no es estrictamente necesario.

• **Asumir el riesgo**, siempre justificadamente. Por ejemplo, el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.

• **Implantar medidas para mitigarlo**. Por ejemplo, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

Por último, cabe señalar que como realizamos este análisis de riesgos en el contexto de un PDS, las acciones e iniciativas para tratar los riesgos pasarán a formar parte del mismo. Por lo tanto, deberemos clasificarlas y priorizarlas considerando el resto de proyectos que forman parte del PDS. Asimismo, tal y como indicábamos en la introducción, llevar a cabo un análisis de riesgos nos proporciona información de gran valor y contribuye en gran medida a mejorar la seguridad de nuestra organización. Dada esta situación, animamos a nuestros lectores a llevar a cabo este tipo de proyectos ya bien sea de forma aislada o dentro del contexto de un proyecto mayor como es el caso del Plan Director de Seguridad (INCIBE-Riesgos, 2021).

Responda a las siguientes preguntas:

https://adl.incibe.es/questions.php

https://download.microsoft.com/download/9/D/A/9DA51D54-5BAE-4197-9343-3400FC49C70D/MSATSpanish.zip

Referencias

BUENDIA, J. F. (2013). *Seguridad informática.* España: McGraw-Hill.

COSTAS SANTOS, J. (2014). Seguridad informática. *RA-MA, SA.*

ESCRIVA, G. R. (2013). *Seguridad Informática.* España: Macmillan Iberia SA .

GMV SECTORES Ciberseguridad. (18 de 03 de 0221). Obtenido de GMV SECTORES Ciberseguridad

INCIBE. (18 de 03 de 2021). *INCIBE - Taxonomia*. Obtenido de https://www.incibe-cert.es/taxonomia

INCIBE-Riesgos. (18 de 03 de 2021). Obtenido de Analisis de Riesgos: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

MITIC. (23 de 03 de 2021). Obtenido de CERT-PY: https://www.cert.gov.py/institucional

STEWART, J. M. (2013). *Network Security, Firewalls and VPNs.* Jones & Bartlett Publishers.

VIEITES, Á. G. (2014). *Gestión de Incidentes de Seguridad Informática.* . RA-MA Editorial.

