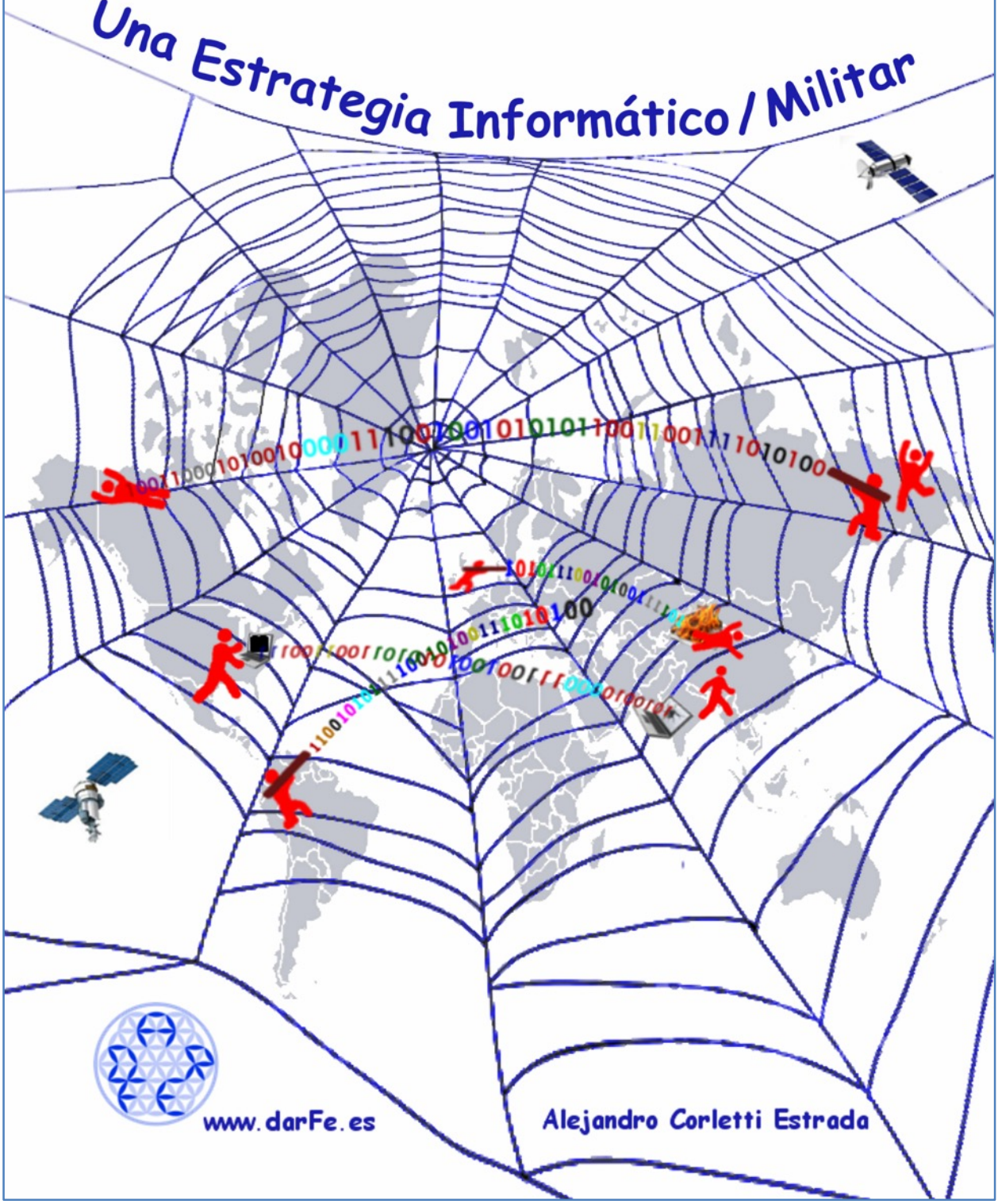
CIBERSEGURIDAD

Una Estrategia Informático / Militar



www.darFe.es

Alejandro Corletti Estrada

"Ciberseguridad"

(Una Estrategia Informático/Militar)

Madrid, noviembre de 2017

RPI (Madrid): M-006991/2017

ISBN: 978-84-697-7205-8

Alejandro Corletti Estrada

(acorletti@DarFe.es - acorletti@hotmail.com)

www.darFe.es

“La tercera Guerra Mundial será una Ciber guerra”

John McAffe

Agradecimientos

A Julián, Carla Iván y Miri

Índice

Prólogo

Una de las principales necesidades que tenemos los seres humanos es la seguridad. Desde que nacemos necesitamos "seguridad" en los distintos aspectos de nuestra vida, y ello es algo que siempre nos acompaña y forma parte de nuestra naturaleza.

Hace unos 40 años, la tecnología de la información trajo consigo la introducción de la seguridad informática con el objetivo de proteger los sistemas tecnológicos que utilizamos. Hace unos 15 años, este concepto se fue transformando en la seguridad de la información con el objetivo de proteger la información (nuestra información) que se encuentra almacenada en los sistemas tecnológicos que utilizamos. Y más recientemente, comenzamos a hablar de ciberseguridad, ya que actualmente el objetivo se extendió no solo a proteger nuestra información, sino también a proteger la infraestructura tecnológica que la soporta y nos hace funcionar como sociedad.

La ciberseguridad incluye una serie de estrategias, metodologías y tecnologías para protegernos de las amenazas actuales y es un nuevo punto de partida para lo que vendrá en el futuro.

Las amenazas tecnológicas que veíamos en una película hace algunos años y que parecían de ciencia ficción, hoy están sucediendo, y afectan a todo el mundo sin distinción de país, ideología o raza… nos afectan a todos. En Latinoamérica vemos cada vez más ataques a sistemas financieros e industriales, a infraestructuras críticas y gobiernos, … hoy en día nadie está a salvo.

Muchas de estas amenazas están llegando al borde de una ciberguerra y con este concepto se suma a la ciberseguridad un nuevo jugador que hasta ahora venía mirando de costado: el entorno militar. Ya dejó de ser un juego de chicos.

Este excelente libro que Alejandro ha escrito recorre la problemática actual a la cual nos estamos enfrentando y describe claramente conceptos,

metodologías, herramientas e ideas que nos ayudarán a estar más preparados para prevenir y contener estas nuevas amenazas.

A Alejandro lo conocí en 1999, hace 18 años, y juntos creamos en el año 2000 el CISIAR, un Centro de Investigaciones en Seguridad Informática en Buenos Aires, Argentina que fue un generador de ideas, proyectos, empresas y, sobre todo, de grandes personas que hoy siguen resonando en el mundo de la ciberseguridad a nivel mundial.

Creamos al CISIAR como una organización sin fines de lucro, con el objetivo de promover el desarrollo de la seguridad informática, y esta línea de compartir el conocimiento es algo que Alejandro siempre ha mantenido toda su vida. Un claro ejemplo de ello son sus dos libros anteriores publicados y el desinteresado esfuerzo de Alejandro por concientizar y compartir su conocimiento.

Realmente es para mí un gran orgullo presentar el libro "Ciberseguridad (una Estrategia Informático/Militar)" ya que considero que será un pilar fundamental en la educación de las futuras generaciones que nos ayudarán a tener un mundo más seguro.

Buenos Aires - Argentina, Noviembre 2017

Julio César Ardita

Experto en Seguridad de la Información y Amigo de Alejandro

1. Presentación

Si bien vivo en Madrid, en virtud de mi trabajo, viajo mucho por sud y centro América. Sigue siendo "mi casa" y como buen latinoamericano, me siento a gusto con su gente, su amistad, su "calor latino", su sencillez, su alegría, sus diferentes acentos y miles de detalles más que nos unen mucho más de lo que pensamos.

También me duele cada más el egoísmo y la soberbia de sus gobernantes, su falta de empatía y solidaridad para su propia gente, pero mucho más aún para sus vecinos.

Tenemos uno de los continentes más bonitos y ricos del planeta, pero somos incapaces de ponernos de acuerdo en nada.

Todo esto viene a cuento porque desde el punto de vista de Ciberseguridad, **cada país aislado NO PUEDE HACER NADA…… ABSOLUTAMENTE NADA** (así de duro).

Todos los informes, estudios y resultados serios sobre Ciberseguridad, sólo pudieron realizarse a través de la unión de grandes (enormes) empresas internacionales. Esas que tienen acceso a las grandes troncales, a los grandes routers, firewalls, DNSs, a los masivos volúmenes de datos, a millones de cuentas de usuarios, a bases de datos de contenidos masivos e internacionales, al código fuente de las grandes plataformas o infraestructuras, a las salas de cómputo que operan miles de procesadores en paralelo, etc.

No podemos pensar que un país de habla hispana pueda llegar a las fuentes del problema de Ciberseguridad por sí solo (*sin incluir a España que, a través de la Unión Europea, ha encontrado alianzas importantes*).

En este tema "**la unión hace la fuerza**" más que nunca.

Tenemos una situación privilegiada como continente, pues es probable que seamos el único que tiene tan sencillas sus telecomunicaciones y habla un único lenguaje (*con mi mayor cariño a Brasil, con quienes, sin hablar su idioma, me comunico perfectamente cada vez que viajo*).

Está rodeada por una fibra óptica con puntos de amarre en cada uno de los países y salida internacional únicamente por Centroamérica, cuestión que permitiría (*si hiciéramos las cosas bien y UNIDOS*) poder hacer un análisis detallado de los flujos de información y como ningún otro continente está en capacidad de hacerlo. Este desafío es IMPOSIBLE de realizar si no existe un acuerdo común y unívoco al respecto por parte del 100% de sus integrantes… pero si lo lográramos, podríamos hacer maravillas.

La presentación de este libro intenta ser un llamado a esta unión de esfuerzos sobre ciberseguridad, pero no solo compartiendo conocimientos, trabajos, monografías, seminarios, sino creando uno o dos centros únicos para todo LATAM con recursos unificados para ello. Si nuestros gobernantes fueran capaces de dejar egoísmos y protagonismos de lado podríamos tener un verdadero protagonismo en Ciberseguridad, obteniendo resultados concretos que beneficiarían de forma concreta a cada uno de sus países.

Si no somos capaces de seguir una línea de acción de este tipo, afirmo categóricamente que lo que haga cada país de forma aislada no producirá el más mínimo impacto sobre su propia "Ciberdefensa", solo lograrán apagar algún que otro fuego menor.

2. Introducción

Sobre la experiencia y la difusión de los anteriores libros:

- **Seguridad por Niveles**
- **Seguridad en Redes**

He pensado que podría ser de utilidad a la comunidad que ha participado y leído los temas allí expuestos, seguir avanzando en los mismos, con esta nueva visión que estamos escuchando casi a diario de "Ciberseguridad".

Durante el 2017 he impartido una serie de Webinar y charlas sobre "Ciberseguridad". En este libro, se encuentran la mayoría de ellas, más algunos conceptos y temas adicionales que he desarrollado en diferentes secciones de la presente obra.

"La tercera Guerra Mundial será una Ciberguerra"

John McAffe

Así comenzamos este libro… ¿Será cierto?

Lo que sí es una realidad según se afirmó en la **cumbre de la OTAN en Varsovia 2016** textualmente:

> *"Habiéndose constatado que un ciberataque puede ser tan perjudicial como un ataque convencional, en el campo de la ciberdefensa se han adoptado varias decisiones relevantes, una de ellas es que:*
>
> *El ciberespacio se reconoce como un nuevo dominio de las operaciones, al lado de los de tierra, mar, aire y espacio".*

La historia de los conflictos bélicos nace con dos dominios: tierra y agua. Cuando aparecen los primeros aviones, se abre un nuevo escenario en los

cielos y comienza el temido espacio aéreo como una herramienta de combate que desestabilizaba cualquier batalla. Estos tres dominios fueron los dominantes hasta muy pasada la segunda guerra mundial.

Recordemos que luego de esta última, comienza lo que todos conocimos como "guerra fría". Esta etapa histórica es muy importante para lo que trataremos más adelante, pues este tipo de guerra se definía por una "capacidad potencial" que tenía un determinado país, y sobre esa base podía disuadir más o menos a sus oponentes. La escalada nuclear llevó a una nueva doctrina denominada "Destrucción Mutua Organizada", o también "Mutua Destrucción Asegurada". Como su nombre lo indica con total claridad, este nuevo escenario nos lleva a un conflicto en el cual su nivel de escalada ocasionaría un nivel de destrucción que afectaría al planeta en su totalidad. Cabe mencionar que esta doctrina está aún vigente y continuamos viendo a diario cómo diferentes países siguen avanzando en esta línea, ignorando que es un camino de autodestrucción asegurado…

Estos nuevos misiles, comenzaron a elevar sus alturas de vuelo, llegando a lo que conocemos como espacio. Un hito muy significativo sucedió hace pocos años cuando el gobierno chino tuvo la brillante ocurrencia de derribar con un misil un satélite de su propio país. Con ello demostró que estaba en capacidad de hacerlo con cualquier otro. A caballo de estos hechos, se acuerda en definir un nuevo dominio de conflicto: el espacio.

Hoy en día, todos sabemos que ese mismo satélite chino, podría haber sido igualmente dejado fuera de combate si comprometemos sus sistemas informáticos o de telecomunicaciones. Esta realidad aplica también a los sistemas de un barco, avión, sistema antiaéreo, de comunicaciones, sistemas **C^3I** (*Comando Control Comunicaciones e Informática*), un misil, un tanque, etc.

> ANÉCDOTA DE EXPERIENCIA PROPIA: Desearía poner de manifiesto un hecho para mí muy significativo. En el año 1987, me encontraba realizando el "curso de teniente" (*una fase de la formación militar, previa al ascenso a teniente primero, que capacita para conducir unidades más grandes: Compañías*). Mientras realizaba ese curso, yo estaba destinado en una unidad

Mecanizada (*tanques, pero para el transporte de personal de infantería*), esos tanques eran de última generación para esa época. Durante la realización de ese curso, me tocó preparar y conducir un "ejercicio militar" (*tema que trataremos al final del libro*). Como en esa época ya me dedicaba a temas informáticos, con mi "Commodore 64" preparé un ejercicio de ataque, en el cual el enemigo interceptaba las comunicaciones de una "sección de tanques" (*4 tanques*); por lo tanto, una vez interceptada (*hoy en día podríamos decir: "**hackeada**"),* no existía contacto de voz entre estos cuatro. Por supuesto que, lanzada la operación, los tanques debían continuar su avance (*a 80 km/h, a una distancia mínima entre sí de unos 50 m y un recorrido de unos 3 km*, que a esta velocidad es cuestión de un par de minutos). A partir del momento en que se cortaban las comunicaciones, aparecía un obstáculo cubierto por fuego, ante el cual, al menos dos de esos tanques debían cambiar su rumbo. En el monitor (*único que soportaba un Commodore 64*) se veía como los cuatro tanques avanzaban en el rumbo que se había establecido inicialmente, el jefe de sección debía impartir órdenes por señales, pues ya no podía hacerlo por voz…. Mientras los tanques, por software, seguían avanzando recto hasta no recibir nuevas órdenes (*si las recibía y el jefe de ese tanque le respondía su "comprendido" todo por medio de las señales pertinentes, yo iba modificando por teclado la trayectoria en tiempo real, tanque a tanque, caso contrario no*). El ejercicio, se repitió en varias oportunidades, el obstáculo que aparecía tenía programada sólo cuatro "ocurrencias" diferentes. No recuerdo exactamente cuántas veces lo ejecutamos, serían cerca de diez… en ninguna de ellas el jefe de sección (*que iba cambiando*) pudo controlar sus cuatro tanques por señales y reconducir la situación una vez que fuera "hackeado" su sistema de radio…

Volviendo a nuestro texto, con el dominio del espacio, se presentaban cuatro escenarios de conflicto. Como acabamos de desarrollar, en la actualidad es posible dejar fuera de combate por medio de un "Ciberataque" las más sofisticadas maquinarias bélicas, entonces es

natural lo que se ha decidido en Varsovia y reconozcamos como un nuevo dominio el "**Ciberespacio**", con lo cual podemos concluir que los dominios para el arte de la guerra son:

- Tierra
- Mar
- Aire
- Espacio
- Ciberespacio

Sigamos adelante con este análisis.

En los tiempos de la guerra fría, el avance nuclear iba determinando la capacidad de "tierra arrasada". Es decir, un país que tuviera suficiente fuerza nuclear podía arrasar un territorio al completo, este fue el hecho desencadenante de la rendición de Japón luego de Hiroshima y Nagasaki. Por otro lado, si su rival también posee un nivel semejante, llegamos nuevamente a la "Mutua Destrucción Asegurada". Ante esta realidad los países conscientes de ello, poco a poco fueron adoptando medidas para tranquilizar a la población mundial e intentar demostrar que no tienen intención de ni siquiera "aproximarse" a esta situación, aunque continuamos viendo ciertos estados al límite de la demencia que no lo ven así.

Sea cual fuere el enfoque, cuando aún se consideraban "cuatro dominios" e Internet no entraba en juego, el tema era **radicalmente distinto** por las siguientes razones:

1) Identificación del enemigo o agresor
2) Hipótesis de conflicto
3) Mutua Destrucción Asegurada
4) Capacidad bélica
5) Tipo de respuesta
6) Por último, el gran interrogante:

El ciberespacio ¿Es un dominio militar?

Desarrollemos estos puntos:

1) Identificación del enemigo o agresor.

   En los tres primeros dominios, es bastante claro quién es el enemigo. Con los misiles intercontinentales, ojivas nucleares, ataques empleando el espacio, etc. Puede caber alguna posibilidad que en los primeros instantes surja algún tipo de incertidumbre, pero en poco tiempo se aclarará el panorama y a nivel mundial se aclararán rápidamente los actores.

   Tal vez el primer problema del "ciberespacio", es que existen muchas probabilidades que el enemigo no pueda ser identificado. Esta realidad la vivimos a diario con cualquier tipo de incidente de seguridad informática, el cuál cuando está bien organizado, se hace cada vez más difícil su análisis forense.

   Hoy en día, las medidas de "**velo y engaño**" (como se denominan militarmente) del Ciberespacio no tienen límites.

   Un principio básico y por excelencia de todo intruso es "no dejar rastros", todo Internet ofrece millones de posibilidades para cumplir este objetivo.

   A nivel Ciberataques a grandes países, tenemos varios ejemplos ya que aún no se ha podido afirmar con total certeza su origen.

   Algunos de ellos son:

   - Las elecciones de EEUU *(siguen las sospechas, pero la certeza de quien fue no está).*
   - El ministerio de Exteriores italiano sufrió hace un par de años un ciberataque masivo *(siguen las sospechas, pero la certeza de quien fue no está).*
   - Del Ciberataque a la red SWIFT de este año (*de la que le "desaparecieron" 81 Millones de Euros y sólo se recuperaron 15*) aún no se ha podido identificar, quién, ni dónde está el dinero… y estamos hablando de unos 70M de euros…. Convengamos que justamente el dinero es uno de los bienes más fácilmente rastrearles dentro del planeta y de la red (*en*

algún momento se convierte en papel y allí es donde suele cerrarse la investigación)

- Los sistemas informáticos de los medios de comunicación surcoreanos sufrieron un importante ciberataque que inutilizó numerosos ordenadores *(siguen las sospechas, pero la certeza de quien fue no está).*
- En 2013, Corea del Norte denunció un ciberataque contra varios de los sistemas informáticos del país, incluidas páginas oficiales *(Se acusó a EEUU, siguen las sospechas, pero la certeza de quien fue no está).*
- En Ucrania, el Banco Central, el metro de Kiev, la compañía estatal de la energía o la red informática del Gobierno ucranio, han sido atacados *(siguen las sospechas, pero la certeza de quien fue no está).*
- En 2016 varios ataques de denegación de servicio (DDoS) fueron registrados contra los servidores de grandes empresas estadounidenses de internet como Twitter, Spotify, Github o el diario The New York Times *(siguen las sospechas, pero la certeza de quien fue no está).*
- En 2014 Canadá responsabilizó públicamente a China sobre un ciberataque contra el Consejo Nacional de Investigación, el principal centro de investigación de este país. Los portavoces de la Embajada china en Ottawa calificaron las conclusiones de "especulaciones sin base alguna" y condenó la conducta canadiense asegurando que esta no era "ni responsable ni profesional". *(siguen las sospechas, pero la certeza de si fue China o no, aún no está).*
- El gusano Stuxnet infectó mil máquinas de la planta nuclear de Natanz de Irán. El reconocido experto Ralph Langner dijo que el gusano fue creado en laboratorio por Estados Unidos e Israel para sabotear el programa nuclear de Irán, pero las autoridades jamás han confirmado esa afirmación. *(siguen las sospechas, pero la certeza de quien fue no está).*

Evidentemente en este nuevo dominio, no será nada fácil identificar con certeza al enemigo.

2) Hipótesis de conflicto.

"La guerra es la continuación de la política por otros medios" Carl von Clausewitz

Clásicamente, un conflicto se origina por una cuestión de intereses contrapuestos. Se puede solucionar por medio del diálogo, la negociación, la política o en un caso extremo, con la violencia, hasta que una de las partes asuma su victoria o derrota.

Cuando dos estados, tienen intereses contrapuestos, se origina un conflicto y mientras estos intereses se mantengan, continuará existiendo el conflicto, o para ser más estrictos un "posible" conflicto. La probabilidad de que el mismo se materialice, es un factor clave. Ejemplos de esto tenemos cientos: Islas Malvinas, Peñón de Gibraltar, Tíbet. En todos ellos el conflicto de intereses está, pero la probabilidad de escalada en estos momentos es lejana.

Sobre la base de su probabilidad, los diferentes estados, organizan sus "Hipótesis de conflicto" y esta debería ser la base de la asignación presupuestaria para defensa. Sobre este análisis, se invierte más (*o se debería…*) en ciertas tecnologías, dominios, armamento, ubicaciones geográficas, capacitación, personal, recursos en general, etc.

Para el dominio de "Ciberespacio" aparecen varios interrogantes nuevos.

a) Tradicionalmente el principal origen de conflicto eran factores geográficos, limítrofes o intereses cercanos. ¿Hoy es así?

b) ¿Cuál debería ser el destino de estas asignaciones presupuestarias?

c) ¿Cómo se planifica la capacidad de reacción ante esta nueva hipótesis?

d) ¿Es dominio de las Fuerzas armadas?

e) ¿Cuáles son los posibles destinos de estos ataques potenciales?

f) ¿Qué impacto puede causar un conflicto de este dominio?

g) ¿Está acotado a países, gobiernos, estados, o puede involucrar más actores?

h) ¿Se puede identificar el potencial enemigo?

i) Si el conflicto busca destrucción masiva, ¿se puede pensar como estrategia de Mutua Destrucción Asegurada?

j) ……

Seguramente podríamos seguir con muchos interrogantes más.

3) Mutua Destrucción Asegurada.

Este tema ya lo hemos presentado, pero lo determinante ahora es que esta estrategia antes del dominio del "ciberespacio" era un hecho suficientemente claro, en relación directa a la envergadura de la "potencia bélica" de cada actor, y los actores eran perfectamente identificables, tema que como acabamos de ver ya no es así.

Cuando analizamos el ciberespacio sobre los puntos anteriores, perfectamente podemos presentar el supuesto de comprometer informáticamente las máximas estructuras bélicas y de destrucción masiva del oponente, con lo que llegamos por este medio al mismo efecto devastador de las cabezas o centrales nucleares.

4) Capacidad bélica.

A diferencia de los cuatro dominios anteriores, donde la capacidad bélica de las partes era un claro factor de éxito. En Este nuevo dominio, la misma no guarda absolutamente ninguna relación. Hoy la más grande potencia bélica mundial puede ser desbordada por una nación que no tenga ni ejército.

Es más, hasta podríamos pensar que cuanto mayor sea su potencial bélico o tecnológico, mayor riesgo tiene. Un parámetro clásico de

toda defensa (militar e informática) es "reducir la superficie de ataque" (*tema que veremos más adelante*). Es decir, ofrecer lo mínimo posible, pues todo recurso expuesto, es un potencial foco a ser atacado u ofrecer problemas de seguridad.

No cabe duda que la dependencia tecnológica de los países del primer mundo es infinitamente superior al resto, por lo tanto, es probable que, por ejemplo: sin la red de telefonía móvil pueda morir gente, cosa que sin duda en Uganda es probable que no sea así.

Hoy en día la capacidad bélica de un país no necesariamente es un factor de éxito en el ciberespacio.

Ya se ha demostrado en reiteradas oportunidades, que un adolescente que opere sólo puede tirar por tierra la infraestructura de una gran empresa y/o gobierno. ¿Cuánto más puede hacer un pequeño grupo organizado que cuente con el apoyo de un gobierno, por mínimo que sea este? En estos nuevos conflictos, ya no existe el concepto de capacidad bélica dominante o equiparable.

5) Tipo de respuesta.

La respuesta ante una agresión convencional está suficientemente estudiada. Pueden cometerse infinitos errores en la forma de aplicarla, pero es claro que ante un ataque terrestre se tienen opciones adecuadas, estudiadas e históricamente probadas para su respuesta.

¿Cómo debemos plantearnos la respuesta ante agresiones del ciberespacio?:

- ¿pasivas?,
- ¿ofensivas?,
- ¿preventivas?,
- ¿reactivas?,
- ¿en el mismo orden de magnitud?,
- ¿con qué fronteras?,

- ¿tengo derecho o no a "escuchar" en Internet?,
- ¿puedo interpretar datos?,
- ¿hacer Big Data?
- ¿Puedo interferir tráfico?,

Sobre este tema, por ejemplo, uno de las filtraciones que más ruido mediático ocasionó de las que difundió el ex agente de la **NSA** (*Agencia Nacional de Seguridad*) **Edward Snowden**, fue la del programa "Politerain" que se había puesto en marcha por parte de esta agencia, y cuyo objetivo es diseñar estrategias de combates en Internet destinados a infiltrar y paralizar las redes de ordenadores enemigas y, de esta forma, tener acceso al suministro de agua potable, electricidad, fábricas, aeropuertos, sistemas de pago, etc. enemigos…… pero…… ¿esto está bien, o está mal? Por qué razón nadie critica que existe una bomba nuclear capaza de arrasar una provincia entera o contaminar todos los ríos, o sistemas de interferencia de las comunicaciones, o lanzallamas. ¿En el ciberespacio, aplican otras reglas de juego?

6) Por último, el gran interrogante:

El ciber espacio ¿Es un dominio militar?

Hasta las últimas guerras de este siglo, no nos cabe duda que una vez que se declara el estado de guerra, los principales actores son las Fuerzas Armadas, para ello fueron creadas, dotadas y entrenadas.

Con el cuarto dominio "El espacio", la cuestión ya empieza a cambiar, pues nace un aparato militar cuyo diseño, implementación, operación y control está en manos de ingenieros. El "Know How" necesario para todo el ciclo de vida de este tipo de herramientas, no necesita de la experiencia militar. Así y todo, hasta este dominio, podemos todavía considerar como importante el rol del comandante en la toma de decisiones

sobre objetivos, respuesta, planificación y operación de este tipo de armas.

En el Ciberespacio, ¿la situación es similar?, o debemos pensar en otro tipo de estrategia.

En principio, analicemos las diferentes hipótesis de conflicto, ¿Dónde creemos que pueden estar dirigidos estos ataques?:

- Instalaciones o redes de energía (eléctrica, gas o combustibles).
- Redes de telecomunicaciones (telefonía, voz, datos, satélites).
- Infraestructuras de potabilización y distribución de agua.
- Infraestructuras de comunicaciones (trenes, transportes, barcos, aviones, control de tránsito, control aéreo y marítimo).
- Infraestructuras sanitarias y bioquímicas.
- Infraestructuras financieras (bancos, medios de pago, cajeros, tarjetas, etc.).
- Infraestructuras de investigación de cualquier área.
- Infraestructuras de tratamiento alimentario.
- Medios de comunicación (televisión, radio, prensa, internet).
- Industrias de producción importantes.
- Infraestructuras gubernamentales.
- Aparato bélico (centros de control, barcos de guerra, aeronaves, blindados, sistemas, C^3I, sistemas de navegación, sistemas antiaéreos, misiles, instalaciones o infraestructuras militares, etc.).
- …..

Ante cualquiera de los supuestos anteriores (tal vez, *con excepción del aparato bélico*), ¿en qué difiere la respuesta que

pueden ofrecer las Fuerzas Armadas, respecto a cualquier ente civil especializado en el tema?

No estoy para nada seguro que este nuevo quinto dominio del arte de la guerra deba ser tratado desde el punto de vista militar. Tal vez sí sea claro que deba tener dependencia del Ministerio de Defensa, pero ¿No será que debemos crear una nueva "arma", fuerza o disciplina? sobre la cual, tal vez la instrucción, formación y jerarquía militar no sea necesaria sino un importantísimo componente técnico.

Sería un tema muy interesante para debatir y obtener conclusiones desde varios puntos de vista.

3. Presentación, conceptos y situación de Ciberseguridad.

¿De quién nos defendemos?

Resumen del tema

Como primera charla, se presentarán diferentes enfoques sobre Ciberseguridad, se desarrollarán conceptos que son base de esta nueva línea de pensamiento y realizaremos un resumen de la situación en que se encuentran las grandes empresas en este tema frente a las ciberamenazas vigentes.
Luego de estos conceptos pasaremos al foco de esta charla donde definiremos: ***¿De quién nos defendemos?*** Como suelo hacerlo, nos basaremos en el "análisis de situación" que se aplica en la metodología militar, simularemos una situación de guerra (*pues estamos hablando de una Ciberguerra: Ciberataques y Ciberdefensa*). Cada uno de los pasos a seguir, se confrontarán con la metodología de ¿Cómo opera un intruso en una infraestructura informática?

3.1. Desarrollo

3.1.1. Conceptos

Según la RAE:

ciber: *"Del ingl. cyber-, acort. de cybernetic 'cibernético'. Indica relación con redes informáticas. Ciberespacio, cibernauta".*

Cibernética: *"Ciencia que estudia las* ***analogías*** *entre los sistemas de control y comunicación de los seres vivos y los de las máquinas".*

Ciberespacio: *"Ámbito artificial creado por medios informáticos".*

Cibernauta: *"Persona que navega por el ciberespacio".*

ISACA (*Information Systems Audit and Control Association*) también nos da una definición de Ciberseguridad. De acuerdo con esta asociación, puede entenderse como:

> "*Protección de activos de información, a través del tratamiento de **amenazas** que ponen en **riesgo** la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados*".

Como una buena práctica a la hora de comenzar un análisis sobre un tema, recurriremos a "Wikipedia". Presentamos en el primer párrafo la definición que nos da la versión inglesa de esta Web:

http://Wikipedia.org:

> *"Computer security, also known as **cybersecurity** or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide."*
>
> Traducción: *"La seguridad informática, también conocida como **ciberseguridad** o seguridad de las tecnologías de la información, es la protección de los sistemas informáticos contra el robo o daño al hardware, software o la información sobre los mismos, así como a la interrupción o la redirección de los servicios que proveen".*

Partimos de la definición en inglés pues esta consulta en la misma Web en versión española, también nos redirige al concepto de "Seguridad Informática", como presentamos a continuación, pero vemos que hay diferencias entre ambos puntos de vista. Por nuestra parte vamos a remarcar en azul algo que nos llama la atención.

http://es.wikipedia.org

> *"La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique **un riesgo** si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.*
>
> *La definición de "seguridad de la información" no debe ser confundida con la de "seguridad informática", ya que esta última solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos."*

A lo largo de este artículo, iremos presentando una serie de conceptos (*como los resaltados en el párrafo anterior*) como tema de debate, sobre los que profundizaremos bastante.

Independientemente de estas diferencias y debates, un dato interesante que sí nos ofrece es.wikipedia.org es que, cuando escribimos "ciberseguridad" nos ofrece un artículo denominado "**Ciberseguridad en la Unión Europea**" sobre el que merece la pena que nos detengamos unos minutos. Uno de los primeros párrafos que nos llaman la atención es el siguiente:

> *"Cómo medio para combatir las actividades ilícitas en internet la Unión Europea ha desarrollado una política de ciberseguridad, un ámbito relativamente reciente, que está basado en la importancia a la protección tanto de los usuarios como de las*

redes de comunicación y los sistemas de información frente a posibles ataques".

"Junto con estos programas, se han desplegado una serie de actuaciones como la creación de la ***Agencia Europea de Seguridad de las redes y de la información*** *(ENISA), la elaboración de una "Estrategia para una sociedad de la información segura" o el "Plan de Ciberseguridad de la Unión Europea". En 2013 se propuso, dentro del Plan mencionado anteriormente, la elaboración de una Directiva de la Comisión Europea sobre la seguridad de las redes y de la información (SRI)."*

Esta estrategia articula la visión de la **UE** sobre la ciberseguridad en torno a cinco prioridades:

- Lograr la **ciberresiliencia.**
- La reducción drástica del Cibercrimen.
- El desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (**PCSD**) (*En inglés: Common Security and Defence Policy,* ***CSDP***).
- El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad.
- El establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

De estas cinco prioridades nos centraremos en la primera de ellas: "**La ciberresiliencia**".

Primero comprendamos bien el concepto de "**Resiliencia**".

En ingeniería, se llama resiliencia de un material a la energía de

deformación (*por unidad de volumen*) que puede ser recuperada de un cuerpo deformado cuando cesa el esfuerzo que causa la deformación. En palabras más sencillas, es su límite elástico. Es decir, una vez superado este límite, el material ya no se puede recuperar y queda "deformado". El ejemplo clásico es un alambre de acero templado u otro de hierro negro, el primero se podrá "flexionar" y retornará a su estado normal, es "elástico"; y el segundo es totalmente maleable (en términos de ingeniería es totalmente "Plástico").

Cuando hablamos de "Resiliencia" de nuestras infraestructuras informáticas, nos estamos refiriendo justamente a esta capacidad de recuperar su estado inicial (capacidad "**elástica**").

Por lo tanto, podríamos definirla como:

> **Capacidad de respuesta y recuperación ante incidentes de seguridad**
>
> (*Para: ciberataques → ciberresiliencia*).

Para este primer postulado de la UE "La ciberresiliencia", esta comisión ha desarrollado una política de "**Network and Information Security**" (**NIS**). Dentro de la misma propone:

- Establecer los requerimientos mínimos comunes para este NIS que obliguen a los estados miembros a:
  - Designar autoridades competentes a nivel Nacional para el NIS.
  - Lanzar y mantener sus propios **CERT** (Computer Emergency Response Team).
  - Adoptar una estrategia y un plan de cooperación nacional sobre el NIS.
- Establecer mecanismos coordinados de prevención, detección, mitigación y respuesta, compartiendo información entre las autoridades nacionales competentes, respecto al NIS. Esta cooperación deberá contemplar planes de respuesta ante

incidentes.

- Mejorar la preparación y el compromiso del sector privado.

Dado que la gran mayoría de los sistemas de red y de información son de propiedad y operados por la industria privada, es crucial mejorar la participación con este sector para fomentar la ciberseguridad. El sector privado debería desarrollar, a nivel técnico, sus propias capacidades de resiliencia cibernética y compartir las mejores prácticas en todos los sectores. Las herramientas desarrolladas por la industria para responder a incidentes, identificar causas y realizar investigaciones forenses también deberían beneficiar al sector público.

Sin embargo, los actores privados aún carecen de incentivos efectivos para proporcionar datos confiables sobre la existencia o el impacto de los incidentes de NIS, adoptar una cultura de gestión de riesgos o invertir en soluciones de seguridad. Por lo tanto, la propuesta de ley tiene por objeto **garantizar** que los actores de una serie de ámbitos clave (***energía, transporte, banca, bolsas de valores y facilitadores de servicios clave de Internet, así como las administraciones públicas***) evalúen los riesgos de seguridad cibernética que enfrentan, garanticen que sus sistemas de información son fiables y resistentes a través de una gestión apropiada de los riesgos y compartan la información identificada con las autoridades nacionales competentes de este NIS. La adopción de una cultura de la seguridad cibernética podría mejorar las oportunidades de negocio y la competitividad en el sector privado.

Otro aspecto fundamental que trata este punto es la "Sensibilización": Asegurar la ciberseguridad es una responsabilidad común. Los usuarios finales desempeñan un papel crucial para garantizar la seguridad de las redes y los sistemas de información: necesitan ser conscientes de los riesgos que enfrentan en línea y estar facultados para tomar medidas sencillas para protegerse contra ellos.

A nivel Nacional, Volvemos al punto clave:

> "La propuesta de ley tiene por objeto **garantizar** que los actores de una serie de ámbitos clave (*energía, transporte,*

banca, bolsas de valores y facilitadores de servicios clave de Internet, así como las administraciones públicas)".

A nivel Estado hace cientos de años que el concepto de Defensa es uno de sus pilares básicos pues hace a la soberanía de todo País y a lo largo de la historia de guerras convencionales se ha demostrado su necesidad. Desde principios de este siglo, las guerras ya no son tan convencionales, el armamento y las técnicas van cambiando, hubo escaramuzas cada vez más tecnológicas, pero aún no se ha desatado ninguna operación bélica abierta o encubierta de escala en el ámbito de la red…. Es sólo cuestión de tiempo.

La dependencia tecnológica está llegando a una masa crítica que, cuando se explote adecuadamente, podrá llegar a dejar fuera de combate a una población o territorio al completo. Hoy en día sería imposible reaccionar a cualquiera de las grandes potencias mundiales si no contaran con satélites, sistemas de telecomunicaciones, energía eléctrica, abastecimiento de combustible, sistemas médicos avanzados, radares, visores nocturnos, sistemas teleguiados, sistemas de detección temprana, sistemas electrónicos de defensa, electrónica en sus aeronaves o barcos, internet, etc. Quedaría totalmente fuera de combate.

Por supuesto ya existen excepciones, pero dentro del mundo occidental a nuestro alcance, aún no parece que se estén destinado recursos suficientes al concepto de "**Ciberdefensa**". Recordemos que la analogía actual es lo que se destina, por ejemplo, a la compra de cualquier elemento bélico (*tanque, avión caza, barco, misil, etc.)* cuyos costes unitarios oscilan en los siete ceros como mínimo. ¿Estamos hablando de tantos ceros para la "**ciber**" defensa?

Más allá del enfoque monetario, lo que más nos llama la atención es la implementación de un área dedicada exclusivamente a esta actividad al máximo nivel. Tal cual existen Ministerios de Defensa en todo estado, ya debería existir en los diferentes Países, a ese mismo nivel o formar parte de las máximas jerarquías de esos Ministerios el área de "ciberdefensa", no pareciera que haya un alto nivel de madurez en este sentido o que se encuentren emplazados en lo más alto de los

organigramas.

Los primeros indicadores de esta actividad "sí o sí" deben partir de un análisis de niveles:

- Estratégico.
- Táctico.
- Operacional.

3.2. Situación

Este enfoque de niveles de Ciberseguridad lo desarrollaremos en profundidad a lo largo de este ciclo de charlas, por ahora lo dejamos planteado para dar inicio al concepto, pero seguiremos adelante con el objetivo del presente texto y analicemos la situación en que se encuentran las grandes empresas frente a las ciberamenazas vigentes.

Durante todo este ciclo, trataremos el problema de Ciberseguridad desde una visión amplia del tema. No podemos detenernos en incidentes menores, debemos evaluar el tema con la envergadura que merece, hoy no hablamos de personas aisladas sino de "**Organizaciones mafiosas**". El problema de Ciberseguridad a nivel mundial es un tema de "crimen organizado", como lo son los Cárteles de droga, o lo fueron las mafias de los años sesenta (*Incluyendo en este campo, políticas de algunos Gobiernos que buscan el caos*). Esta organización es celular y segregada en funciones:

- Búsqueda y obtención de usuarios y contraseñas.
- Búsqueda y obtención de tarjetas de crédito y cuentas bancarias (*carding*).
- Búsqueda de vulnerabilidades.
- Búsqueda y obtención de sistemas vulnerables (*botnets*).
- Venta/re-venta de: listados, productos, servicios y zombies.
- Ofuscación u ocultamiento de rastro/información
- Oferta de productos (de dudoso empleo).
- Infección de hosts.

- Diseñadores de malware (Punto de partida de secuencia: *Código primario, ajuste/personalización, implementación, explotación*).
- Analistas de reversing (ingeniería inversa).
- Diseñadores de exploits.
- Analizadores de target e impacto/beneficio.
- Ejecutores de herramientas.
- Control, supervisión y blanqueo de dinero obtenido.
- Muleros/transportistas (eslabón final).

Cuando cada una de estas actividades se "realizan adecuadamente", es justamente **cuando no nos enteramos**. Si salen a la luz es porque algo falló en su organización, ya se ha rentabilizado lo suficiente, son producto de poca "expertiz", o de alguien paralelo (o ajeno) a estas organizaciones.

LO REALMENTE DAÑINO ESTÁ OCULTO

Cualquier persona que desee comprender como operan estas mafias, debe primero analizar sus métodos de operación, técnicas, jerarquías, procedimientos, su día a día; y esto es lo que iremos desarrollando en este ciclo, pero no perdamos de mira la magnitud de lo que nos vamos a enfrentar, no nos quedemos con un concepto de "hacker", este tal vez sea de los últimos eslabones de esta cadena, la cabeza de este fenómeno mundial son "**Mafias organizadas**" que cuando necesitan mano de obra contratan estos perfiles para el área de actividad que les haga falta. Y no olvidemos que cuando aparecen en los medios de difusión es porque ya no les genera tanto beneficio.

3.3. La visión de Cisco

Para seguir en la línea de pensamiento sobre la "Magnitud" a la que nos enfrentamos, iniciaremos este punto sobre la base del "**Informe anual de seguridad Cisco 2016"** *(empresa que, en lo personal, no deja de admirarme por lo bien que difunde su información y el nivel de detalle técnico que siempre podemos encontrar en sus papers).*

Lo podemos descargar en la siguiente URL:

http://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/annual_security_report_2016_es-xl.pdf

Este informe que contó con la colaboración de "**Level 3**" (*el mayor carrier mundial*) y la cooperación del proveedor de alojamiento "**Limestone Network**", comienza hablando del kit de ataque **Angler** como uno de los más grandes y eficaces del mercado. *"afectaba a 90.000 víctimas por día y generaba decenas de millones de dólares al año. Se lo ha vinculado con diversas campañas de ransomware y publicidad maliciosa de alto perfil*".

> *"Como se explica en el Informe semestral de seguridad 2015 de Cisco, las criptomonedas como **bitcoin** y las redes de anonimato como **Tor** permiten que los atacantes ingresen en el mercado de malware de manera fácil y comiencen a generar ingresos rápidamente*".

Para que podamos ir "*abriendo la mente*" sobre la envergadura del problema, me he permitido a continuación citar textualmente algunos de los párrafos de este informe:

> *"Las empresas habían estado lidiando con excesivas cancelaciones de pagos con tarjeta de crédito todos los meses porque los atacantes usaban nombres y tarjetas de crédito fraudulentas para comprar lotes aleatorios de sus servidores valuados en miles de dólares".*
>
> *"Para investigar esta actividad, Cisco obtuvo ayuda de **Level 3 Threat Research Labs** y de **OpenDNS**, una empresa de Cisco. Level 3 Threat Research Labs pudo brindar una mayor perspectiva global de la amenaza, lo que proporcionó a Cisco la capacidad de ver en mayor profundidad el alcance y la trascendencia de esta en su punto máximo. Por su parte, OpenDNS proporcionó una mirada única de la actividad del dominio asociada con la amenaza, lo que brindó a Cisco una comprensión más exhaustiva de cómo los atacantes estaban incorporando técnicas como domain shadowing (camuflaje de*

dominio)".

"Los investigadores detectaron que los usuarios eran redirigidos al kit de ataque Angler a través de publicidad maliciosa incluida en sitios web populares. Los anuncios falsos eran colocados en cientos de sitios importantes de noticias, bienes raíces y cultura popular. Estos tipos de sitio comúnmente se conocen en la comunidad de seguridad como sitios "buenos conocidos"".

*"Encontramos más de **15.000** sitios únicos que redirigían a las personas al kit de ataque Angler, de los cuales el 99,8% se usaba **menos de 10 veces**".*

"Cisco también descubrió que, en realidad, los servidores a los que los usuarios estaban conectados no alojaban ninguna de las actividades maliciosas de Angler. Servían como conductos".

"La colaboración en el sector fue un componente fundamental en la capacidad de Cisco para investigar la actividad del kit de ataque Angler. En última instancia, permitió detener los redireccionamientos a los servidores proxy con Angler en un proveedor de servicios estadounidense y concientizar acerca de una operación de delito cibernético altamente sofisticada que estaba afectando a miles de usuarios todos los días".

Resumen de estos puntos:

- Sale a la luz por el análisis y apoyo grandes empresas (*pues sería imposible analizarlo de otra forma*).
- Manejos financieros con Bitcoins, tarjetas de crédito grandes sumas.
- Redes ocultas (*Tor*) y cambios permanentes de hosts para borrar huellas.
- Miles de pasarelas de hosts infectados.
- Sofisticadas técnicas.
- Diseño, complejidad y ajuste de software.
- Decenas de millones de dólares al año.

Hasta aquí el factor que más deseábamos destacar de este informe, es decir nuestra postura de "Organizaciones mafiosas" pues sería imposible haber realizado todo esto con individuos aislados, y por otro lado, si prestamos atención, esto sale a la luz a través de una investigación de muy alto nivel empresarial.

Si seguimos analizando este mismo reporte (*pido disculpas por hacer tan extenso el análisis de este informe, pero a mi juicio es excelente*), también nos ofrece una perspectiva de ciberseguridad que es útil a tener en cuenta por las empresas.

Cisco ha detectado un incremento en el uso de Bitcoins, del protocolo TLS y de la red Tor que, tal cual acabamos de presentar, que permiten la comunicación anónima a través de la web.

> *"El malware cifrado **HTTPS** (Hiper Text Transfer Protocol Secure) utilizado, creció un 300% entre diciembre de 2015 y marzo de 2016. Tengamos en cuenta que el malware cifrado facilita aún más la capacidad de los adversarios para ocultar su actividad web y ampliar su tiempo de operación".*
>
> *"Herramientas como: Angler, Ransomware, SSHPsychos (también conocido como Group 93 para DDoS), en forma conjunta, Bedep, Gamarue y Miuref (otro troyano) representaron más del 65% de la actividad de comando y control mediante botnets en la base de usuarios que analizamos".*
>
> *El análisis de malware validado como "malo conocido" de Cisco determinó que la mayor parte del malware (91,3%) usa el servicio de nombre de dominio de una de estas tres formas":*
>
> - *Para obtener comando y control*
> - *Para exfiltrar datos*
> - *Para redireccionar el tráfico*

Cifrado:

El cifrado también plantea problemas de seguridad para las organizaciones, incluida una falsa sensación de seguridad. Las organizaciones mejoraron mucho el cifrado de datos cuando estos se transmiten entre entidades, pero los datos almacenados a menudo quedan desprotegidos.

A medida que el nivel de tráfico de Internet cifrado continúe aumentando, será cada vez más importante que las organizaciones adopten una ***arquitectura de defensa ante amenazas integrada****. Las soluciones puntuales no son eficaces para identificar posibles amenazas en el tráfico cifrado. Las plataformas de seguridad integrada proporcionan a los equipos de seguridad mayor visibilidad con respecto a lo que sucede en los dispositivos o las redes. Gracias a esto, pueden identificar más fácilmente los patrones sospechosos de actividad.*

Infraestructura obsoleta: un problema con de 10 anos de gestación

Todas las empresas de hoy son empresas de TI en cierta medida, porque dependen de su infraestructura de TI y TO (tecnología operativa) para estar conectadas, digitalizadas y tener éxito. Esto significa que necesitan dar prioridad a la seguridad de TI. Sin embargo, muchas organizaciones se basan en infraestructuras de red creadas a partir de componentes obsoletos, desactualizados, que ejecutan sistemas operativos vulnerables y no tienen capacidad de recuperación informática (ciberresiliencia).

Otro problema geopolítico importante que las organizaciones deben supervisar se relaciona con las vulnerabilidades y los ataques. Algunos gobiernos expresan estar realmente preocupados por el surgimiento de un mercado de vulnerabilidades sin corrección, denominadas ***"software como arma****". Las herramientas de este tipo son vitales para la comunidad de investigación sobre seguridad, ya que busca maneras de proteger las redes en todo el mundo. Sin*

embargo, en las manos incorrectas, particularmente en las de regímenes represivos, esta tecnología, diseñada para tareas útiles, podría usarse para cometer delitos financieros, robar secretos nacionales y comerciales, eliminar el disenso político o alterar la infraestructura critica.

La infraestructura obsoleta está creciendo y deja a las organizaciones cada vez más vulnerables al riesgo.

Analizamos 115.000 dispositivos de Cisco en Internet y descubrimos que ***el 92%*** *de los dispositivos de la muestra estaba ejecutando software con vulnerabilidades conocidas.*

La ciberseguridad: Una preocupación para los ejecutivos

Obviamente, una seguridad integral puede ayudar a las empresas a evitar violaciones y ataques catastróficos. Sin embargo... ¿puede ayudar a mejorar las oportunidades de éxito de una empresa? Según un estudio realizado por Cisco en octubre de 2015 en el que participaron ejecutivos financieros y de la línea de negocios con el objeto de analizar el rol de la ciberseguridad en la estrategia digital y comercial, los ejecutivos empresariales comprenden que proteger el negocio de amenazas puede determinar su posible éxito o fracaso.

A medida que las organizaciones se digitalizan cada vez más, el crecimiento dependerá de la capacidad de proteger la plataforma digital.

Los líderes empresariales también prevén que ***los inversores y organismos reguladores harán preguntas más rigurosas acerca de los procesos de seguridad****, del mismo modo en que interrogan sobre otras funciones empresariales. El 92% de los encuestados estuvo de acuerdo en que los inversores y organismos reguladores esperarán que las empresas proporcionen más información sobre la exposición a riesgos de ciberseguridad en el futuro.*

Los seis principios de una defensa ante amenazas integrada

Los expertos en seguridad de Cisco afirmaron que la necesidad de soluciones adaptables e integradas dará lugar a cambios importantes en el sector de seguridad en los próximos cinco años. Los resultados serán la consolidación del sector y un movimiento unificado hacia una arquitectura de defensa ante amenazas escalable e integrada. Una arquitectura de este tipo proporcionará visibilidad, control, inteligencia y contexto a través de varias soluciones.

1. *Se necesita una **arquitectura de red y seguridad más eficiente**.*
2. *Contar con **la mejor tecnología de su clase no alcanza** para hacer frente al panorama de amenazas actual o futuro; simplemente aumenta la complejidad del entorno de red.*
3. *Para un **mayor tráfico cifrado**, se necesitará una defensa ante amenazas integrada capaz de reunir la actividad maliciosa cifrada que hace que determinados productos puntuales se vuelvan ineficientes.*
4. ***Las API abiertas** son fundamentales para una arquitectura de defensa ante amenazas integrada.*
5. *Una **arquitectura de defensa ante amenazas integrada** requiere menos equipos y software para instalar y administrar.*
6. *Los aspectos de **automatización y coordinación de una defensa ante amenazas integrada** ayudan a reducir el tiempo de detección, contención y corrección.*

3.4. La visión de Fortinet

En el blog de Fortinet cuyo enlace figura a continuación, esta otra gran empresa líder en el mercado de seguridad, también nos presenta una serie de predicciones para el 2017.

https://blog.fortinet.com/2016/11/21/fortinet-2017-cybersecurity-predictions-accountability-takes-the-stage

Presenta este artículo de la siguiente forma:

> *"Con el crecimiento y la omnipresencia de los dispositivos en línea y las herramientas digitales, alcanzamos un punto crítico en 2016. La necesidad de rendir cuentas a múltiples niveles es urgente y real y nos afecta a todos. Si algo no se hace, existe el riesgo **real** de interrumpir la emergente Economía Digital".*

Este enfoque de Fortinet se centra en las conclusiones:

1. *De **smart a smarter**: los ataques automatizados emulando al ser humano requerirán una defensa más inteligente, el nuevo malware diseñado "emulando al ser humano" con capacidad de adaptación y de aprendizaje, para mejorar el impacto y la eficacia de los ataques.*
2. *Los fabricantes de dispositivos IoT serán responsables de las brechas de seguridad.*

   Si estos fabricantes fallan a la hora de proteger mejor sus dispositivos, el impacto en la economía digital podría ser devastador.
3. ***20.000 millones** de dispositivos IoT, el eslabón más débil para atacar la nube.*

   El eslabón más débil de la seguridad en la nube no se encuentra en su arquitectura en sí, sino en los millones de dispositivos remotos con acceso a los recursos albergados en la misma.
4. *La smart city en su punto de mira.*

   El incremento esperado para el próximo año en el número de sistemas de automatización y gestión de edificios, les convierte en objetivo de los hackers.
5. *El ransomware era solo el malware de entrada.*

   Se espera que se produzcan más ataques dirigidos contra perfiles

de alto nivel, como celebrities, políticos o grandes empresas.

6. *La tecnología tendrá que compensar la falta de conocimiento en ciberseguridad.*

*La **actual escasez de profesionales en ciberseguridad** implica que muchas organizaciones y países que desean participar de la economía digital global, asumirán un gran riesgo.*

3.5. De quién nos defendemos

Hemos estado viendo aspectos clave de Ciberseguridad: Malware sofisticado, pasarelas que ocultan rastros, criptografía que engaña nuestros sistemas de detección, redes ocultas paralelas (Tor), fraude con tarjetas y medios de pago…. organizaciones mafiosas…. Pero el tema no queda aquí.

En la actualidad la potencia de las herramientas informáticas y su fácil acceso, nos enfrentan a todo tipo de ataques, desde los más sofisticados que acabamos de presentar, hasta un niño que descarga un explota de Internet y sin tener mayor conocimiento de lo que hace, lo ejecuta contra nuestra empresa pudiendo ocasionar un daño tremendo si no estamos preparados para defendernos adecuadamente.

Bajo mi punto de vista (y es una apreciación totalmente personal), creo que merece la pena diferenciar un poco la idea de "**mafias organizadas**" que existen, son reales y su objetivo es millonario, con **este tipo de perfiles o delincuentes**.

En realidad, cuando hago mención a "**Ciberseguridad**", por mi parte trato de tener presente esta gran escala de "**ataques organizados o mafiosos**" pues al igual que con la droga actual o el alcohol de la ley seca de los EEUU el siglo pasado, existen mafias, y también delincuentes menores que consiguen la droga por su medios, la revenden, arman sus pequeñas redes de distribución, etc… Pero la raíz del problema son las grandes organizaciones delictivas, ese es el fondo de la cuestión y son los que pueden crear caos, problemas mundiales y hasta como lo enuncia Fortinet: "*Si algo no se hace,*

*existe el riesgo **real** de interrumpir la emergente Economía Digital*". No nos confundamos, **interrumpir la actual economía digital implica**: no pagar con tarjetas, no poder hacer movimientos bancarios en la red, no cobrar nuestros haberes telemáticamente, no poder comprar nada en Internet, no poder hacer "telemediciones de nuestros servicios", no tener alarmas de hogar, no tener cerraduras electrónicas, no automatizar NADA de un coche, no reservar hoteles, pasajes, tickets….. es decir, NADA de lo que mueve nuestro dinero en la Red, es decir un verdadero caos mundial.

Pero más allá de esta cuestión conceptual (que considero importante remarcar), la realidad hace que nuestra empresa, peligre tanto de estas mafias organizadas como de un chico de quince años que opera al margen de cualquiera de ellas, y el impacto que me puede ocasionar a mi empresa en concreto es tal vez el mismo.

Por esta razón es que también debemos tener en cuenta que existen muchos tipos y niveles de intrusos, desde los más iniciados "Newbies o Lamers" que son millones, hasta personas con muy alto nivel de conocimientos que llegan a controlar en detalle los protocolos de comunicaciones o lo que se denomina "Pila y/o buffer" que es el verdadero cerebro desde donde se ejecutan cada uno de los programas en un ordenador como una mera secuencia de pasos en lenguaje binario. Cada una de estas personas me gusta presentarlas como una pirámide de conocimientos con varios "Niveles", donde podemos encontrar en su base a los más nuevos y en su cumbre a menos de un 1% de estas personas que son el máximo peligro de cualquier organización.

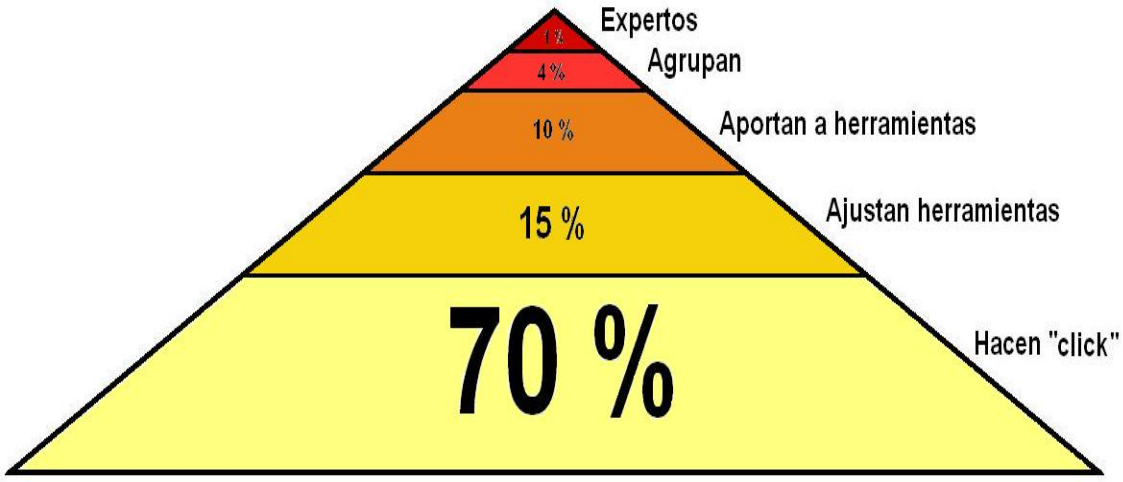


Imagen "Pirámide de expertiz de un intruso"

Lo asombroso de esta pirámide es que todos los niveles están en capacidad de hacer daño y muy significativo a los sistemas informáticos de las organizaciones, aunque la gran masa de usuarios sean inexpertos son tantos millones que producen el fenómeno "**CROWD**" (*multitudes*) que hoy se está estudiando seriamente en Internet (*no solo por seguridad, sino por marketing, tendencias, I+D, etc.*) y a su vez están potenciados por herramientas o software muy poderoso que está disponible con total facilidad en la red.

La clasificación de esta pirámide es una visión personal que hace tiempo que expongo y representa que:

- **Un 70 % Hacen "Click":** Es decir, curiosean por las distintas Webs y foros de hacking y cuando encuentran un software que muchas veces ni siquiera saben para qué sirve, hacen "click" y lo ejecutan, generalmente apuntándola a alguna Web novedosa, conocida, de su centro de estudios, o importante, etc.
- **Un 15 % Ajustan herramientas**: Ese software que hemos mencionado, lo estudian con más detalle y comienzan a configurarlo con más precisión: Engañan sus orígenes, acotan los ataques, ajustan los tiempos y puertos de acceso, etc.
- **Un 10 % Aportan a herramientas**: Van avanzando y a medida que conocen una o varias herramientas, descubren mejores prestaciones, módulos nuevos, optimizan su código, introducen

nuevos o proponen módulos. Este nivel en general participa activamente en foros, Webs y blogs específicos donde se debaten estos temas.

- **Un 4 % Se agrupa**: Es un nivel de más difícil acceso y en el cual se trabaja bajo cierto tipo de organización. Sus ataque y metodologías podríamos decir que son decididamente delictivas y peligrosas. Agrupan también diferentes tipos de herramientas entre sí, potenciando su ataque.
- **Un 1 % Expertos**: Algunos de ellos hoy son famosos. Son "creadores" de código, están en capacidad de llegar a lo más profundo del lenguaje binario y evaluar al detalle todos los niveles del funcionamiento del Software y hardware de los sistemas.

3.6. Análisis de situación desde un punto de vista militar

Luego de esta presentación, pasemos a hacer un ejercicio de "*visualización*". Para los que hemos formado parte del mundillo militar, tal vez nos resulte más sencillo, pero también cualquiera que lea este artículo es porque algún interés por la "Defensa" debe tener y no dudo que al menos habrá visto alguna de esas películas de guerra en las cuáles se encuentra reunido el "Estado Mayor" de esa Fuerza militar y está planificando la estrategia de una defensa. Nuestro ejercicio será (*si queréis, hasta cerrando los ojos*):

Situación a visualizar: Se encuentra reunido el Estado Mayor en una tienda de campaña con una gran mesa en la cual está desplegada una carta topográfica ampliada, sobre ella dibujos y líneas que representan diferentes posiciones del despliegue de sus fuerzas, pareciera ser que están planificando una defensa. Hay varias personas alrededor de la mesa y se destaca claramente la figura del comandante, el mismo se dirige directamente al Oficial que está frente a él que es el "**J2**" (*Oficial de Inteligencia*) y le pregunta:

- ¿Cuál es la situación del enemigo?

El "J2" despliega un gran folio sobre la pizarra que está a un costado de la mesa y en la misma se puede leer lo siguiente:

- Composición: Desconocida
- Disposición: Desconocida
- Magnitud: Desconocida
- Cantidad: Desconocida
- Capacidades: Desconocidas
- Experiencia: Desconocida
- Armamento: Desconocido
- Localización: En todo el mundo
- Movimiento: Desconocido
- Potencia conocida: Desconocida
- Identificación: Ninguna
- Objetivo: Desconocido
- Impresión: Total Desconcierto

Si queréis podéis continuar la visualización imaginando la cara o reacción del comandante, pero por ahora me interesaría destacar:

¿Cómo se organizaría una defensa militar en esta situación?

Si volvemos a la realidad, concretamente esta es la situación que se vive (*con sus más y sus menos*) en cualquier organización que tenga sus ordenadores en red y conectados a Internet.

Así de crudo, duro y concreto... **¿De quién nos defendemos?**

La incertidumbre es total. Si los responsables de informática de nuestra organización son eficientes, cuentan con un conjunto muy sólido de herramientas, procedimientos y medidas de protección que llevan años ajustándose y mejorando, lo que nos permite un nivel de protección aceptable, pero el tema crítico no está aquí sino en la "**Estrategia**" de seguridad de la organización.

Volviendo al mundo militar, una cosa es la "Estrategia", otra la "Táctica", y otro el nivel "Operacional", son tres niveles diferentes. En el mundo empresarial, también es así, una cosa es el nivel "Directivo", otro el "Gerencial" y otro el de "Ejecución".

Si un directivo se contenta únicamente con las herramientas y medidas de ejecución de sus sistemas informáticos, se está equivocando de nivel. Así como el administrador de sus sistemas informáticos se debe encargar de implantar medidas, soluciones, reaccionar ante situación, el director no está para eso. Él está para definir la "Estrategia", él está acostumbrado a moverse ante situaciones de incertidumbre y tomar decisiones trascendentes para la organización.

Si un directivo le preguntara a su administrador de sistemas ¿De quién nos defendemos? Obtendría la misma respuesta que la de nuestro "J2". Ante esta situación un directivo debe situarse en su nivel: "Estratégico".

Todo Internet se regula por una serie de recomendaciones llamadas "**RFC**" (Request for Comments), estos documentos ya superan los ocho mil, y establecen las "pautas" (o mejores prácticas) a seguir. Una de ellas es la **RFC – 1244** (Política de seguridad), si bien ya existe una más actualizada, esta, en el punto el 2.5. propone dos estrategias de seguridad:

- **Proteger y proceder.**
- **Seguir y perseguir.**

Este será el tema de la siguiente charla, pero a título de presentación podemos decir que resumidamente, la primera de ellas propone que, ante un incidente de seguridad, su reacción es apagar equipos, cortar vínculos de comunicaciones, cerrar áreas, etc. es decir "Proteger y proceder". El gran problema reside en que una vez que se decida restablecer todo, las debilidades o los intrusos siguen allí, y volverán a hacer lo mismo, pues "Desconozco casi todo de ellos" tal cual venimos tratando en todo el texto. Os proponemos participar de la segunda charla, en la cual profundizaremos sobre ambas Estrategias.

3.7. Reflexión final

Hemos ido desarrollando conceptos, definiciones, ideas, opiniones de empresas líderes del mercado, analizando niveles de intrusos,

predicciones para este año, etc… Luego hemos visto dos tipos de Estrategias posibles. De todo esto quisiera cerrar esta primera charla volviendo a uno de los primeros conceptos que desarrollamos:

"Resiliencia"

Esta desearía que sea nuestra reflexión final. En primer lugar, seamos conscientes que nos estamos enfrentando a organizaciones poderosas (*y no hemos hablado aún de Ciberterrorismo…*), a herramientas muy potentes, a un nivel tecnológico voraz y cambiante que nos abre nuevos desafíos (debilidades y problemas) a diario, a un grado de exposición que crece de forma exponencial (*tanto en la empresa como en lo personal: IoT*) a una interconexión mundial que no tiene límites ni fronteras. Es muy similar a lo que hemos "*visualizado*" como análisis de situación militar.

Todo esto nos presenta una realidad sobre la que no nos podemos sentir seguros 100%, sería muy audaz creer que mi fortaleza es inexpugnable (así pensaron en Alcatraz o en las murallas de Sagunto hace 2000 años).

Si no tenemos mayores capacidades, deberíamos "Proceder y Proteger", pero con ello no erradicaremos la causa. Si deseamos "seguir y Perseguir" nuestra Estrategia nos conducirá hoy en día sobre nuestras redes y sistemas orientándolas hacia la "**Resiliencia**", es decir que, si sufrimos cualquier tipo de incidente de seguridad, podamos garantizar que:

- En primer lugar: **lo resistimos**.
- En segundo lugar: Estamos en capacidad de **Volver a su estado inicial** (*en un período de tiempo aceptable*).

Si nuestras infraestructuras, superan estos dos hechos, podremos sentirnos más que satisfechos de nuestro trabajo.

3.8. Tareas para el hogar (deberes).

Es mi intención, que este texto sea de utilidad, con el objetivo de ser más eficientes capítulo a capítulo y que, en definitiva, todos estos párrafos hagan mella en nuestra forma de encarar el gran problema actual y enrome que se nos viene encima de la Ciberseguridad.

Propongo que en el capítulo que viene, cada uno de los lectores haya avanzado en la medida de lo posible, al menos un escalón más de lo que nos encontramos en el día de hoy.

Para ello y al mejor estilo "colegio secundario", os propongo a todos los lectores, que no nos quedemos con lo tratado aquí, sino que lo "curremos" (como se dice en España).

A continuación, os propongo una serie de líneas de acción o pensamientos para que dentro de un tiempo los hayamos "masticado" en la medida que cada uno pueda y comencemos el siguiente capítulo con una mejor posición de cada uno de nosotros en Ciberseguridad.

Os propongo las siguientes "**tareas para el hogar"**:

1. ¿De quién nos defendemos?
2. Tratamiento de amenazas: ¿Tenemos claras cuáles son?
3. ¿Cuáles son nuestros riesgos?
4. ¿Qué impacto me producirían?
5. una serie de estándares, protocolos, métodos, reglas, herramientas y leyes. ¿Buscamos, analizamos algunas de ellas?
6. Unión Europea ha desarrollado una política de ciberseguridad…..Por Sudamérica ¿Cómo estamos?
7. Ciberresiliencia ¿Cuál es nuestra situación?
8. ¿Tenemos presente un plan global de unión de Países en Ciberseguridad?
9. ¿Estamos dispuestos, o lanzamos iniciativas conjuntas con la industria privada para afrontar el problema de la

Ciberseguridad?

10. ¿Estamos trabajando seriamente en la sensibilización sobre Ciberseguridad?
11. ¿Nuestros actores clave (energía, transporte, banca, bolsas de valores y facilitadores de servicios clave de Internet, así como las administraciones públicas) están trabajando en conjunto?¿Garantizamos su participación?

4. Estrategias de Ciberseguridad en grandes redes *(Seguir y perseguir - proteger y proceder)*

Resumen del tema

Para hacer frente al Ciberriesgo es necesario adoptar medidas que permitan minimizarlo o mitigarlo en la mejor medida posible. Este conjunto de acciones debe responder a planes a medio y largo plazo (*la improvisación es el primer factor de riesgo en estos temas*).
Desde el punto de vista militar, en toda operación se planifican "**cursos de acción**" y sobre los mismos en la relación coste/beneficio se selecciona el definitivo (*en un proceso de toma de decisiones*). Una vez adoptado este último, se diseña e implementa la "Estrategia a seguir".
Mezclando estos **conceptos militares con metodologías de Internet, existen algunas RFCs** que nos proponen dos posibles métodos) o líneas de acción):

- **Seguir y perseguir**
- **Proteger y proceder**

Sobre la base del nivel de seguridad alcanzado, la experiencia, los recursos, la capacidad de reacción, etc… deberemos inclinarnos por uno o por otro y la decisión final será la clave.

Esta charla es novedosa, justamente por presentar este "mix" entre operaciones militares y seguridad en Internet.

4.1. Planteo inicial

Al analizar el estado de una antigua política de seguridad que presentaba la **RFC–1244**, en su punto el 2.5. vemos que la misma propone dos estrategias:

- Proteger y proceder.
- Seguir y perseguir.

Si prestamos atención al detalle de ambas estrategias, esta misma RFC nos presenta en qué situación puedo optar por una u otra:

"Protect and Proceed

1. *If assets are not well protected.*
2. *If continued penetration could result in great financial risk.*
3. *If the possibility or willingness to prosecute is not present.*
4. *If user base is unknown.*
5. *If users are unsophisticated and their work is vulnerable.*
6. *If the site is vulnerable to lawsuits from users, e.g., if their resources are undermined.*

Pursue and Prosecute

1. *If assets and systems are well protected.*
2. *If good backups are available.*
3. *If the risk to the assets is outweighed by the disruption caused by the present and possibly future penetrations.*
4. *If this is a concentrated attack occurring with great frequency and intensity.*
5. *If the site has a natural attraction to intruders, and consequently regularly attracts intruders.*
6. *If the site is willing to incur the financial (or other) risk to assets by allowing the penetrator continue.*

7. *If intruder access can be controlled.*
8. *If the monitoring tools are sufficiently well-developed to make the pursuit worthwhile.*
9. *If the support staff is sufficiently clever and knowledgable about the operating system, related utilities, and systems to make the pursuit worthwhile.*
10. *If there is willingness on the part of management to prosecute.*
11. *If the system adminitrators know in general what kind of evidence would lead to prosecution.*
12. *If there is established contact with knowledgeable law enforcement.*
13. *If there is a site representative versed in the relevant legal issues.*
14. *If the site is prepared for possible legal action from its own users if their data or systems become compromised during the pursuit."*

Basado en estas dos estrategias básicas podemos evaluar cómo enfrentar un incidente de seguridad. Resumiendo, un poco los párrafos de esta RFC:

a. Proteger y proceder: La premisa de esta es la preservación de los componentes del sistema. El gran problema es que, si el intruso no pudo ser identificado, este podrá regresar por la misma puerta o por algún otra.
¿Qué premisas se deben tener en cuenta para implementar esta estrategia?

- Si los recursos no están bien protegidos.
- Si existe un riesgo económico de magnitud al continuar la intrusión.
- Si no existe la posibilidad de perseguir al intruso.
- Si los usuarios no poseen conciencia (o experiencia) de seguridad y

sus recursos peligran.

- Si no poseemos capacidad de procesar evidencias robustas y contundentes ante una acción judicial.
- Si los recursos no están claramente establecidos o identificados.

b. Seguir y perseguir: Se permite al intruso continuar sus actividades hasta identificarlo y evidenciar las vulnerabilidades del sistema que fueron aprovechadas. Se requiere aquí conocimiento en el manejo de incidentes y herramientas adecuadas pues se está arriesgando demasiado. La gran ventaja de este proceder es que es la única forma eficiente de llegar a las causas del problema para que este no vuelva a repetirse.
¿Qué premisas se deben tener en cuenta para implementar esta estrategia?

- Si los recursos y sistemas están bien protegidos.
- Si se dispone de buenos backup.
- Si la frecuencia de ataques es considerable y lo sabemos identificar.
- Si el acceso de intrusos puede ser controlado.
- Si se posee la capacitación suficiente para enfrentar un ataque.
- Si existen contactos con otros organismos que puedan prestar apoyo ante ataques.
- Si existe soporte legal en la organización para responder ante estos casos.

La primera de ellas es un curso de acción bajo el cual, ante una intrusión, inmediatamente se procede a desconectar sistemas, apagar servidores, negar accesos, etc. Es decir, se soluciona el problema actual pero no se puede llegar al fondo del mismo, no permite determinar las causas, ante lo cual cuando se vuelva a su régimen normal, existe una gran posibilidad que la intrusión se produzca nuevamente. Las ventajas que ofrece son que el intruso en ese momento no podrá avanzar más, y la información y recursos serán

protegidos. Es una buena metodología a tener en cuenta si no se posee un alto grado de capacitación, soporte especializado ni recursos suficientes.

La segunda metodología es más audaz, permitiendo llegar al origen de la vulnerabilidad, determinar las causas, los pasos que siguió el intruso, obtener toda la información probatoria, e inclusive hasta generar ataques inversos. Lo que es evidente aquí es que se está "Jugando con fuego", es decir se debe tener mucho nivel de conocimientos, herramientas adecuadas, especialistas en apoyo y hasta soporte legal y de difusión de noticias.

Este es el punto clave para el desarrollo de esta charla, pues no se aprecia que las estrategias actuales permitan llevar a cabo la actividad de "Seguimiento de intrusiones" con un cierto grado de efectividad, por lo tanto, se debe plantear una nueva línea de pensamiento para la planificación e implementación de los sistemas informáticos que oriente paso a paso al administrador de los mismos.

Lo realmente crítico que posee este hecho es, tal cual presentamos en la primera charla, el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades. Si a este hecho se suma la necesidad, u obligación actual de exponer información al público en general y a sus socios de negocios, fuente de ingresos de una empresa; y a su vez se tiene en cuenta que esta información día a día va aumentando como una estrategia competitiva de presencia en la red y de rapidez en las negociaciones, esto provoca un mayor grado de exposición y por lo tanto de vulnerabilidades.

En el análisis de vulnerabilidades comienza el *primer desbalance* de fuerzas, pues si se ajusta a los datos de la realidad (*y no a lo hipotético o teórico*), no existe una sola empresa real que pueda contar con suficiente personal dedicado a las actualizaciones e investigación de seguridad como para no dejar brechas abiertas en un momento dado. Muy por el contrario, existen millones de personas en

el mundo de Internet cuya principal preocupación es descubrir vulnerabilidades en sistemas. Este es el primer factor a tener en cuenta.

El *segundo aspecto* a analizar es estadístico, y se trata de las operaciones defensivas o de seguridad a lo largo de la historia. **No se tienen antecedentes de una fortaleza invulnerable**. Siempre en estas operaciones, se demoró más o menos tiempo, con armas conocidas o nuevas, esperando el momento adecuado, especulando con los imprevistos, aprovechando las actividades que se transforman en rutinarias, generando pánico, negando recursos, produciendo desconcierto, etc... Pero la muralla cayó, el enemigo se infiltró, se pudo escapar, el robo se produjo, se abrió la brecha,

..... "SIEMPRE EL TEMA SE CENTRÓ EN SABER OBSERVAR".

Teniendo en cuenta por el momento solamente estos dos conceptos, ¿Por qué no se puede partir de las premisas de reconocer que se es vulnerable y se cuenta con un adversario superior en cantidad y calidad, al cual se debe enfrentar?

Luego de estas ideas es estrictamente natural recurrir al análisis de ¿Cómo han hecho los militares a lo largo de la historia en estos casos?

4.2. Las Operaciones Militares

Los estudios de las operaciones militares clasifican el uso de la Fuerza en tres tipos de operaciones:

- Ofensivas.
- Defensivas.
- Retrógradas.

La primera de ellas, es claro, que lo que refleja es una actitud de

avance, ataque o agresiva. En esta charla, no es motivo de interés.

La segunda y la tercera sí pueden llamar la atención como algo afín a un sistema informático que busca protección ante un enemigo externo.

Lo que marca la gran diferencia entre estas últimas es la actitud **pasiva** de una defensa (*si bien puede tener ciertos aspectos de movimiento*), contra la enorme **dinámica** que caracteriza a las operaciones retrógradas.

Las Operaciones Retrógradas a su vez pueden también ser clasificadas, acorde a las distintas doctrinas en **Repliegue**, **Retirada** y **Acción Retardante**.

Desde ya que aquí no se trata de abandonar partes del sistema informático (*Repliegue*), tampoco es intención de este estudio proponer una huida de la red (*Retirada*), pero sí se va a continuar analizando de qué se trata la "**Acción Retardante".**

> NOTA: Se deja claro que en virtud del resumen aquí expuesto se va a obviar el desarrollo del resto de las operaciones, para centrarse en esta última.

A continuación, se citan conceptos textuales de la doctrina militar para despertar la atención en cuanto a las analogías que se presentan con la realidad informática. Se trata de un muy breve resumen de la enorme cantidad de doctrina al respecto, pero se aprecia necesario incluirla para continuar el tema.

El reglamento de **EMPLEO DE LA FUERZA TERRESTRE** (DO1 – 001) de **OTAN** menciona en el punto 14.5.

> *"LA OPERACIÓN DE RETARDO:*
>
> *En la operación de retardo la fuerza, bajo presión enemiga, cambia espacio por tiempo, conservando su flexibilidad y libertad de acción.*

En esta cesión voluntaria de terreno permite a la fuerza de retardo:

- *Ralentizar el impulso de ataque enemigo, llegando incluso a frenarle.*
- *Canalizar y dirigir el avance enemigo hacia zonas en las que resulte vulnerable a un ataque o contraataque por las propias fuerzas.*
- *Descubrir el esfuerzo principal del enemigo.*
- *Combinar las acciones anteriores y desgastar al adversario.*

Estos efectos se logran con un volumen de fuerzas sensiblemente inferior al que requeriría una operación defensiva, proporcionando la consiguiente economía de medios, siempre deseable".

El Reglamento **DO2 – 002 DOCTRINA OPERACIONES** (también de la OTAN) hace las siguientes referencias:

"LAS OPERACIONES RETRÓGRADAS.

Son parte de un esquema más amplio de maniobra para recuperar la iniciativa y derrotar al enemigo. Con ella se consigue mejorar la situación actual o evitar que empeore.

Las finalidades que pueden atribuirse a este tipo de operaciones son:

- *Ganar tiempo.*
- *Maniobrar situando al enemigo en posición desfavorable.*

.....

Operación de retardo: En ella las unidades ceden terreno para ganar

tiempo. Conservando el mando, su flexibilidad y libertad de acción.

Los objetivos a alcanzar con una operación de este tipo podrán ser:

- *Retardar el avance enemigo ocasionándole bajas que reduzcan su capacidad ofensiva con el fin de ganar tiempo para operaciones*
- *posteriores.*
- *Canalizar al enemigo hacia zonas en las que sea vulnerable a los ataques y contraataques y recuperar de esta forma la iniciativa.*
- *Evitar el combate en condiciones no deseadas.*
- *Determinar el esfuerzo principal del enemigo.*

Enemigo:

Será normalmente superior. De su estudio, aparte de valorar su flexibilidad, articulación y procedimientos será preciso conocer:

- *Tipos de Unidades a retardar.*
- *Constitución de sus vanguardias y plazos de intervención de sus gruesos.*
- *Procedimientos ofensivos.*
- *Posibilidades de sus medios ante nuestras acciones de contra movilidad.*
- *....."*

NOTA: para no extendernos tanto en el cuerpo de este documento, hemos incluido una ANEXO que amplía un poco más este último reglamente que merece la pena prestarle atención en otra oportunidad, lo dejamos a criterio del lector.

Hoy se trata de otro combate, pero al comenzar a leer lo que propone

la documentación militar, aparece el primer indicio que es el punto de partida de esta charla.

> Proteger y proceder = OPERACIÓN DEFENSIVA = **ESTATICA**.
> Seguir y perseguir = OPERACIÓN RETROGRADA = **DINAMICA**.

A lo largo de la charla de hoy proponemos una nueva metodología de planeamiento y ejecución de la defensa de un sistema informático, pero bajo esta nueva estrategia. Es decir, **cambiar** la política actual al más alto nivel, dejando de lado el concepto defensivo medieval de "murallas", por el enfoque moderno bajo el cual se debe ser plenamente consciente que se deberá ceder información y terreno ante un enemigo inmensamente superior y desconocido, para poder asegurar los recursos que son verdaderamente valiosos, en detrimento de los que no lo son.

Para que esta estrategia tenga éxito, se aprecia inicialmente que se deberá tener especialmente en cuenta lo siguiente:

- Determinar los distintos grados de calificación de los recursos, con especial atención en cuáles se podrán intercambiar o interactuar, y cuáles definitivamente no (críticos).
- Delimitar líneas de retardo (*zonas de red*) donde se deberán estudiar los sistemas de alarma y la estrategia en ellas.
- Planificar los cursos de acción ante presencia de intrusiones en cada línea, sus probables líneas de aproximación y evaluación de probables metodologías.
- Planificar y llevar a cabo Operaciones complementarias de velo y engaño, seguridad, e información como proponen los reglamentos militares.
- Definir una línea de retardo final o línea a no ceder, dentro de la

cual deberán encontrarse los recursos críticos y excluirse todo aquel que no pueda garantizarse su fiabilidad.

- Definir zonas de sacrificio y contraataques (*Honey Pots*), para quebrar el avance de intrusos (*IDSs y/o IPSs: Intrusion Detection/Prevention System*).

El planteamiento inicial se podría representar bajo el siguiente esquema:

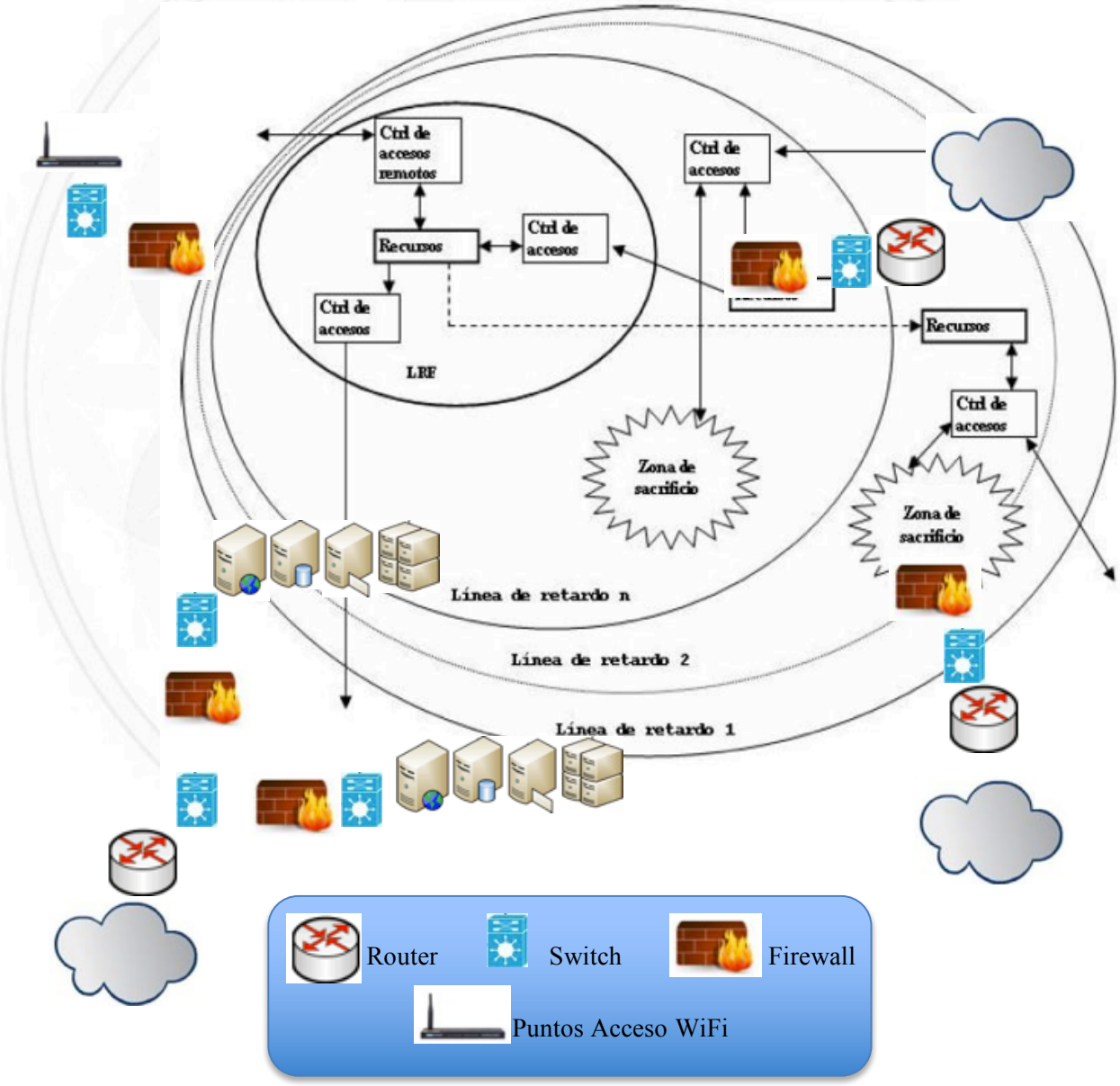


Imagen de zonas de red

En la imagen anterior representamos diferentes zonas (*concepto ya muy difundido en redes como "Defensa en Profundidad"*), cada una de las cuáles tiene diferentes medidas de seguridad, y en las que ubicaremos nuestros dispositivos teniendo en cuenta los perfiles y grupos que pueden o no pueden acceder a los mismos e implantamos las infraestructuras o plataformas de seguridad, monitorización, supervisión y gestión necesarias. Con las flechas de la imagen, presentamos un ejemplo de cómo también podemos definir los "flujos de conexión" entre las zonas, considerando el sentido en el cual puede establecerse o no las diferentes sesiones o diálogos de acceso.

Lo novedoso de este punto de vista, es que **no** propone mantener al intruso fuera del propio sistema informático (*como lo intentan hacer hoy todos los planes y políticas de seguridad actuales*), sino dejarlo ingresar poco a poco, para cumplir el primer y fundamental parámetro de decisión estratégica "**SEGUIR Y PERSEGUIR**" y realizar una verdadera dinámica de la defensa. Por supuesto que no cualquier intruso logrará superar cada línea defensiva, sino que será acorde a las capacidades del mismo, lo que sí reiteramos que debe quedar claro, es que actualmente existen enemigos altamente capacitados (*Organizaciones mafiosas como presentamos en la primera charla*), que sin lugar a duda pueden vencer las tradicionales defensas informáticas (Routers, Proxies y Firewalls). La única forma que actualmente existe para detenerlos **es observar** su proceder, para poder hacer que estas medidas tradicionales y/o contramedidas sean eficaces y detenerlos en el momento oportuno.

Toda esta estrategia propone la "Observación e interacción" hasta este "momento oportuno" denominado justamente línea a no ceder o **LRF** (Línea de Retardo Final)**.**

Para poder asociar los conceptos militares e informáticos es por lo que se presentó brevemente un análisis de la doctrina militar, particularizando los aspectos de la acción retardante, los que pueden dar origen a esta línea de pensamiento informática. Al realizar este

paso, surgen las ideas de asociación de conceptos que se siguen a lo largo de la charla para poder aplicar tácticas militares a la informática, dando como resultado los siguientes puntos para el desarrollo de la presentación.

4.3. Defensa Informática por Acción Retardante

En toda operación militar, y como veremos también de forma muy similar en el mundo empresarial, se debe tener en cuenta el nivel sobre el que estamos tratando el tema. Estos niveles suelen definirse como:

- **Estratégico** (Empresa: Directivo)
- **Táctico** (Empresa: Gerencial)
- **Operacional** Cómo: ejecución de la maniobra (Empresa: ejecutor, administrador)

El nivel **Estratégico** debe involucrarse todo lo posible en "Ciberseguridad", tal cual lo hemos presentado en el primer capítulo sobre la base de los estudios presentados.

Es el punto de partida para determinar las infraestructuras críticas de la de la empresa y definir las prioridades o líneas generales, también para realizar lo que en seguridad informática se conoce como "Análisis de Riesgo". Para el análisis ya existen numerosas herramientas de mercado y hasta estándares internacionales. Básicamente se inicia con la identificación de los activos (*en este caso centrándose en infraestructuras críticas*), su valoración, la relación que poseen entre ellos, el riesgo particular, global y el impacto que puede causar sus anomalías. Sobre todo ello se plantean diferentes "cursos de acción" para la mitigación del riesgo, actividad que tal vez sea la más difícil pues puede ir desde la inversión millonaria, pasando por ideas

creativas, implantación de medidas, hasta la asunción del riesgo al completo. Lo más importante a nivel Estratégico, es que a través de esta gestión del riesgo se pueden estimar costes, preparar presupuestos y luego dimensionar y asignar los recursos necesarios para el medio y largo plazo. La responsabilidad primaria de este nivel pasa por el equilibrio justo entre los riesgos asumidos y las estrategias de mitigación.

El nivel estratégico NO es quien realizará el Análisis de riesgo, sino quien definirá sus líneas generales y luego decidirá sobre el mejor "curso de acción" cuando el análisis esté finalizado.

Como se viene definiendo desde hace tiempo en el ámbito informático, todas las actividades relacionadas a seguridad deben formar parte de un ciclo de vida continuo (**SGSI**: *Sistema de Gestión de la Seguridad de la Información*), de nada sirve haber llegado a un umbral máximo de seguridad, si esto no se mantiene y mejora. Por ello es que el paso final de este primer ciclo de vida a nivel Estratégico debe ser la definición de un Plan de Continuidad de Negocio (**PCN**), pues de todo lo evaluado se debe realizar el esfuerzo final de "imaginar" todas las potenciales situaciones que pueden causar imponderables sobre estos activos, tratando de considerar las mejores opciones para recuperar en la medida de lo posible su capacidad operativa en un plazo acorde a la relación coste/beneficio de cada uno de ellos. Puede sonar fácil, pero no lo es en absoluto.

En nuestro caso, el ámbito estratégico, deberá estar suficientemente involucrado en temas de ciberseguridad y debería estar definido como "**Defensa informática por Acción Retardante**". Para ello, el nivel dirección de la empresa es quien deberá definir plazos, recursos y grandes objetivos a cumplir.

El nivel **Táctico** (o gerencial) es el responsable de dos actividades fundamentales:

- Planeamiento de la Seguridad
- Gobierno de la Seguridad

El **Planeamiento** debe definir el ciclo de vida de la seguridad (**SGSI**) y diseñar la implementación de las medidas técnicas a aplicar para la mitigación de los riesgos que definió el nivel Estratégico, adecuándolos a los cursos de acción seleccionados y con los recursos que se asignen a cada uno de ellos.

Una de las actividades más importantes de planeamiento es toda la ingeniería de infraestructuras (*creación de planta, gestión de cambios, gestión de configuraciones e inventario, etc.*) y los procesos que mantienen "viva" la seguridad (*Gestión de incidencias, gestión de accesos, gestión de backups, gestión de Logs, supervisión y monitorización, etc*).

El **Gobierno** es la actividad que mantiene vivo el estado de seguridad. Supervisa, audita y diseña las acciones de mejora necesarias para mantener el ciclo. Tampoco merece la pena entrar en detalle sobre esta actividad, pues hoy contamos con la familia **ISO-27000** cuyo nombre es justamente el ya mencionado SGSI, que nos describe con máxima profundidad cómo llevar adelante esta actividad de Gobierno continuo de la seguridad.

Cuáles son las líneas de acción que debe involucrarse el nivel **Táctico** para aplicación de una defensa informática por Acción Retardante

1) Realizar un "análisis de riesgo" lo más detallado posible, respetando los pasos clásicos de esta actividad: identificación de recursos, interacción entre ellos, cuantificación, amenazas, riesgo e impacto. Medidas mitigatorias.

2) Diseñar o definir cada uno de estos recursos, pensando en "**Resiliencia**", tal cual hablamos el mes pasado. Es decir, definir backups, RTO y RPO (***RPO**: Recovery Point Objective o Punto de Recuperación, **RTO** Recovery Time Objective o Tiempo de Recuperación*), procedimientos de recuperación, planes de pruebas, redundancias, alta disponibilidad, generación de registros y alarmas, protocolos de monitorización y supervisión, capacitación

(y redundancia) de operadores y administradores, etc.

3) Diseñar la seguridad informática por capas: Estas capas son las que le darán profundidad a la defensa (defensa en profundidad) para asociarlo con las líneas de retardo, dentro de cada una de las cuales se realizará diferentes actividades tendientes a desgastar y obtener información del adversario.
   Esto en términos técnicos es aplicar una robusta política de "Segmentación de redes" basada en zonas.

4) Organizar las capas por niveles de seguridad, hasta llegar a una última capa de máxima seguridad (Core de una empresa) o (Línea de Retardo Final: **LRF**). Los niveles de seguridad son los que definen que tipo de información se puede o no ceder, y van directamente asociados a la capacidad del adversario, pues cuanto más eficiente sea, más profundo llegará. El tema crucial es la definición de esta última capa, la cual no puede ser superada.

   En esta zona final es donde ubicaremos todos los elementos que se han identificado como "críticos" para la organización.

   NOTA: Este punto y el anterior, lo desarrollaremos con más detalle en el **capítulo 5. Ciberdefensa en profundidad y en altura** (la conquista de las cumbres).

5) Implantar robustos procedimientos que regulen toda la actividad que se desarrolle en cada zona.

   NOTA: Este punto y el anterior, lo desarrollaremos con más detalle en el **capítulo 6. "Ciberseguridad: La importancia de los procesos".**

6) Implantar mecanismos para obtener información del adversario: En cada una de las líneas, uno de los principales objetivos es la detección del mismo para poder tener "Alertas tempranas" y poder obrar en consecuencia.

7) Definir medidas para intercambiar tiempo por recursos. Una parte

muy importante de la acción retardante son las "Operaciones de Velo y engaño (también denominadas de decepción)" y "Las operaciones de información".

8) Poder evaluar permanentemente el balance de fuerzas y el debilitamiento sufrido en cada enfrentamiento: Desde el inicio mismo de la operación militar y durante cada enfrentamiento, es necesario mantener el "Estado de Situación", que como se presenta en la Orden de Operaciones militares, es el primer punto y es tratado con sumo detalle. En el caso de la Acción Retardante, como se trata de un enfrentamiento en desigualdad de condiciones, este aspecto cobra aún mayor importancia. Para la actividad informática, el estado de las debilidades se debe mantener también lo más actualizado posible. Si se desea profundizar un poco más sobre este tema hace unos años he publicado un artículo que propone una metodología muy dinámica que da por resultado la "**Matriz de estado de seguridad**" que es el nombre de esta publicación y puede encontrarse con cualquier buscador en Internet, (o descargarse de la Web: http://www.darFe.es).

   NOTA: (Los puntos 6, 7 y 8, los desarrollaremos con más detalle en el **capítulo 7. Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red.**

9) Asegurar esta LRF o Línea a no ceder: La victoria de una Operación de Acción Retardante está dada por negar el acceso al adversario a una cierta línea denominada LRF o Línea a no ceder. Lo novedoso de este trabajo, es que no propone mantener al intruso fuera del propio sistema informático (como lo intentan hacer hoy todos los planes y políticas de seguridad actuales), sino dejarlo ingresar poco a poco, para cumplir el primer y fundamental parámetro de decisión estratégica "SEGUIR Y PERSEGUIR" y realizar una verdadera dinámica de la defensa. Por supuesto que no cualquier intruso logrará superar cada línea defensiva, sino que será acorde a las capacidades del mismo, lo que sí es claro es que actualmente existen enemigos altamente capacitados, que sin lugar a duda pueden vencer las tradicionales defensas informáticas (Routers,

Proxies y Firewalls). La única forma que actualmente existe para detenerlos es observar su proceder, para poder hacer que estas medidas tradicionales y/o contramedidas sean eficaces y detenerlos en el momento oportuno.

10) Toda esta estrategia propone la "Observación e interacción" hasta este "momento oportuno" denominado justamente línea a no ceder o LRF. La máxima seguridad que se aprecia hoy en esta última capa está dada por el empleo de Redes Privadas Virtuales (VPN), túneles y en particular **IPSec** en el tráfico y acceso a la misma y bastionado de elementos.

Por último, el nivel **Operacional** es el "Cómo" de toda la operación.

Este nivel es el que opera el día a día. Para un Operación de Ciberdefensa bajo un concepto de "acción retardante", no existen improvisaciones, ni despliegues que no cuenten con un marco sólido a nivel internacional.

Las herramientas básicas para poder "**Seguir y Perseguir**" que deben operarse, al menos son:

- Herramientas de Gobierno, Riesgo y Cumplimiento legal tipo *SandaasGRC*
- Herramientas de mitigación de ataques DDoS tipo TMS/Peak Flow de Arbor
- Herramientas de centralización y correlación de Logs (SIEM: *Security Information and Event Management*) del tipo:
  - ArcSight de HP
  - RSA Security Analytics
  - Splunk (*Puede discutirse si es o no un SIEM…)*
- Firewalls. En el mercado existen cientos
- Herramientas de gestión de Firewalls del tipo:

- Algosec
- Tufin
- Firemon

- Herramientas de detección y prevención de intrusiones del tipo:
  - Snort
  - Check Point Intrusion Prevention System
  - Cisco Next Generation IPS
  - McAfee Network Security Platform
  - Se pueden considerar aquí los FWs de nueva generación de Palo Alto
- Herramientas de monitorización y supervisión de red. Dentro de este rubro existen cientos de herramientas, en general fuertemente orientadas a líneas de productos, pero lo que debe interesarnos aquí es que las que se seleccionen debe operar con protocolos estandarizados dentro de las familias de **snmp, syslog, mrtg**, etc.
- Herramientas de gestión de ticketing (también existen varias). Este punto, aunque parezca trivial no lo es, ya que todo el control de infraestructuras, dispositivos, redes, etc. Debe responder a una metodología estricta y segura de seguimiento, desde que se da de alta un elemento, se realiza cualquier cambio, se sufre una incidencia, se solicita soporte técnico, se crea o modifica una regla en un FW o IDS, etc. Para cualquiera de estas tareas, es fundamental poseer todo su ciclo de vida (o histórico) pues la actividad de "forense" y la "trazabilidad" serán uno de los pilares de una infraestructura de Ciberdefensa.
- Herramientas de control de acceso, tipo:
  - ACS de Cisco
  - Series SRC de Juniper
  - NAKINA
  - Access Control de Fortinet

- HPNA
- CITRIX
- Máquinas de salto

- Herramientas para "Honey Pots" (ver proyecto Honey net).
- Empleo de "sondas" para la captura, interceptación y generación de tráfico.
- Metodología estricta de sincronización de tiempos basada en el protocolo **ntp** (Network Time Protocol).
- **NOC** (Network Operation Center) 24x7
- **SOC** (Security Operation Center) 24x7
- Infraestructura de telecomunicaciones eficiente y flexible.

  Este punto es de vital importancia pues el verdadero control de la operación pasa por estos cables o fibras ópticas.

4.4. Resumen final

La idea fuerza del primer capítulo fue: **Resiliencia**.

La idea fuerza del segundo capítulo es estrategia de "**Acción Retardante**" bajo el principio de "**Seguir y perseguir**" intrusiones, que nos hablaba la RFC-1244.

Esta estrategia debe plantearse aprovechando la experiencia y doctrina militar para llevarla al terreno de la informática, bajo un enfoque DINÁMICO de la defensa.

- Ralentizar el impulso de ataque enemigo, llegando incluso a frenarle.
- Canalizar y dirigir el avance enemigo hacia zonas en las que resulte vulnerable a un ataque o contraataque por las propias fuerzas.
- Descubrir el esfuerzo principal del enemigo.

- Combinar las acciones anteriores y desgastar al adversario.
- Estos efectos se logran con un volumen de fuerzas sensiblemente inferior.
- Ganar tiempo.
- Maniobrar situando al enemigo en posición desfavorable.

Esta nueva estrategia debe desarrollarse a todos los niveles de nuestra empresa:

- **Estratégico** (Empresa: Directivo)
  - Estrategia de Seguridad, lineamiento análisis riesgo, recursos, selección del "plan de acción", participación - involucramiento.
- **Táctico** (Empresa: Gerencial)
  - Planeamiento de la Seguridad
    - Desarrollo del Análisis de Riesgo.
    - Diseño de la Estrategia (Acción retardante – capas o zonas – contramedidas).
    - Diseño del SGSI.
    - Ingeniería de seguridad.
  - Gobierno de la Seguridad
    - Implantación SGSI (Cuerpo y controles)
- **Operacional** Cómo: ejecución de la maniobra (Empresa: ejecutor, operador, administrador)
  - Operación de la Seguridad (Cómo)

    Empleo de herramientas de:
    - Gobierno, Riesgo y Cumplimiento.

- Gestión de la seguridad.
- Monitorización y supervisión.
- Filtrado.
- Detección, análisis, intercepción y generación de tráfico.
- Ticketing.
- SOC y NOC.

4.5. Tareas para el hogar (deberes).

Manteniendo esta didáctica al mejor estilo colegio secundario, en este segundo capítulo una vez más os propongo llevarnos a casa algunas actividades o líneas de reflexión para que comencemos el siguiente capítulo con un poco más de "expertiz".

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cuáles son mis recursos críticos?
2. ¿Me encuentro en condiciones de lanzar un análisis de riesgo?, ¿Qué necesito para ello?
3. ¿Qué aspectos, medidas o herramientas de mis redes en la actualidad puedo emplear para darle "Dinámica" a mis infraestructuras?
4. ¿Cuáles herramientas considero importantes para incluir en mis infraestructuras?
5. ¿Puedo rediseñar (*o ya tengo*) mis redes bajo al menos tres capas defensivas?
6. ¿Cuento en la actualidad, o puedo contar en el corto plazo con una visión: Estratégica, Táctica y Operacional de la Seguridad?
7. Uno de los puntos clave para enfrentar la estrategia de "Seguir y

Perseguir" es: Si se posee la capacitación suficiente para enfrentar un ataque. ¿Cuento con ese nivel de capacitación?, ¿Qué aspectos necesito reforzar?, ¿Cuáles deberían ser los focos principales de capacitación?

ANEXO de este capítulo: Breve ampliación de los conceptos del "Reglamento DO2 – 002 DOCTRINA OPERACIONES"

FACTORES CONDICIONANTES

La operación de retardo se plantea teniendo en cuenta los siguientes factores:

14.5.a.(1). Inteligencia

Es vital el flujo permanente de inteligencia precisa, oportuna y fiables sobre las intenciones, capacidades y puntos débiles del enemigo durante toda la operación.
.....

14.5.a.(3). Terreno

Si es posible se seleccionará un terreno que:

- *Disponga de barreras naturales u obstáculos que se puedan mejorar fácilmente y puedan emplearse para canalizar el movimiento enemigo.*
- *Permita la rápida ruptura del contacto.*

14.5.a.(4). Tiempo

El mando que decida ejecutar una acción de este tipo

deberá precisar, en función del terreno y los medios disponibles:

- Tiempo disponible para que las propias fuerzas preparen sus posiciones.

- Duración del retardo a imponer. Este retardo se expondrá claramente en la misión asignada.

14.5.a.(5). Mantenimiento de la libertad de acción

El jefe de la fuerza de retardo debe organizar adecuadamente sus medios de forma que se puedan afrontar situaciones imprevistas. Debe aprovechar cualquier oportunidad para llevar a cabo acciones ofensivas, siempre que se pueda infligir bajas o daños al enemigo.

14.5.a.(6). Seguridad y protección

Son esenciales para evitar que las fuerzas de retardo sean sorprendidas y se produzca un combate decisivo no deseado. Esto supone no sólo el máximo empleo de medidas de ocultación, enmascaramiento, decepción, seguridad de comunicaciones, guerra electrónica y todas las de contrainteligencia, sino también de protección de puntos críticos necesarios para el desplazamiento.

14.5.b. CONDUCCION

El desarrollo de la operación supondrá realizar el movimiento retrógrado sobre posiciones de forma sucesiva o alternada, llevando a cabo acciones de ataque, defensa y retardo entre posiciones.

.....

Se aprovechará toda ocasión propicia a la emboscada y a

lograr la sorpresa, a su vez se debe evitar la acción recíproca".

5. *Ciberdefensa en profundidad y en altura (la conquista de las cumbres).*

Resumen del tema

Como ya habréis visto, una de las cosas que considero importante en la seguridad informática es aprovechar la experiencia milenaria del empleo de las operaciones militares y buscar analogías con las tecnologías actuales de defensa de redes y sistemas.

Todo empezó con un artículo a comienzos de este siglo que se llamó "**Sentencia de muerte a los Firewalls**, la idea era intentar desterrar el des concepto que únicamente poniendo barreras ganábamos el combate, no es así, debe existir todo un planeamiento y "Dinámica" en una defensa y aprovechar al máximo cada uno de los elementos que "desarman" las tramas de información. Los Firewalls han sido "apoyados" por varios elementos y aplicaciones más, no son una única muralla.

Luego en otros artículos hablamos de los conceptos de "**defensa por capas"** y esta estrategia en terminología informática tuvo más consenso bajo el nombre de Defensa en profundidad.

Unos años después, con motivo del doctorado, presenté la tesis con el nombre de "**Estrategia de seguridad informática por capas, aplicando el concepto de Operación Militar por Acción Retardante**", esta vez sí ya hablaba de una necesaria "Dinámica de la defensa" intercambiando espacio por tiempo, desgastando a un enemigo desconocido e inmensamente superior, etc... Esta operación hoy en día es lo que hacemos con los IDS (Intrusion Detection Systems), IPSs (Intrusion Prevention System), DPI (Deep Packet Inspection) con los honey pots y/o honey nets, correladores de Logs, etc...

La "Acción Retardante" fue el foco del capítulo anterior.

Hasta ahora entonces, venimos hablando de varios conceptos militares que ya se están aplicando en la defensa de sistemas, primero el destierro de las murallas, luego la profundidad (o capas), más adelante la dinámica de la defensa, pero hace muy poco, propuse la idea de "**defensa en altura**". Es un parámetro fundamental en las operaciones militares, quien domina las cumbres tiene una ventaja enorme. Es otra de las preciosas paradojas de este mundo tecnológico en el que nos creemos que la ciencia y el avance domina el mundo, este es uno más de los ejemplos en que no es así. Todas las fuerzas militares del mundo tienen elementos de montaña y de alta montaña, en esas zonas domina el ser humano, allí en muchísimos casos y condiciones meteorológicas no llegan los vehículos, las motos de nieve, los helicópteros, los aviones…. sólo el hombre, los perros, mulas y trineos…. Volvemos a nuestros orígenes ¿Qué paradoja no?

5.1. Planteo inicial

En la charla anterior comenzamos a tener en cuenta la "profundidad de la defensa, las diferentes zonas y sembramos la idea de plantearnos una "dinámica de la defensa" a través de esta estrategia de "Acción Retardante". En el día de hoy vamos a desarrollar otra línea más de análisis por medio de confrontación de conceptos militares y el estudio de los niveles (o alturas) que debemos considerar en nuestras infraestructuras.

Cuando las fuerzas militares dominan las cumbres y cierran los pasos de montaña la cosa se pone muy difícil para el enemigo, el dominio de las alturas siempre es una ventaja en toda operación militar.

En nuestro caso el ascenso y el dominio de las alturas, no serán ni más ni menos que prestar atención a cada uno de los escalones o niveles que nos propone el modelo de capas, basándonos en el modelo o pila TCP/IP, en cada una de ellas existen aspectos que cuando son bien tratados, se puede llegar a la cumbre que es donde están los datos o información y en definitiva constituyen el corazón (Core) de nuestra empresa. Tal cuál se hace en una operación militar, esa zona o altura

se deberá aprovechar individualmente al máximo para que cada punto dominante del terreno sea un objetivo a ser abordado si se desea cumplir con la finalidad. Como iremos viendo, cada cumbre se evalúa para el control de los "**Valles**" que, en nuestra analogía, serán las zonas de red que estaremos protegiendo.

Toda operación militar antes de ser ejecutada responde a una serie de actividades o pasos perfectamente ajustados con los siglos, llamados "**Secuencia de planeamiento**" y concluyen con lo que se denomina "**Orden de Operaciones**" (para cada tipo de operación), esta orden también tiene un formato digamos que "estandarizado", el punto "2" de la misma se denomina "**Misión**" e inexorablemente debe responder a los cinco interrogantes básicos y colaborar a un fin mayor:

- Quién.
- Qué.
- Cuándo.
- Dónde.
- Para qué.
- CON LA FINALIDAD DE.

Ejemplo sencillo: La tercera compañía de infantería (*Quién*) defenderá *(Qué)* desde el día 25may2017 *(Cuándo)* la altura 57 (*Dónde*) para retardar el avance enemigo (*Para qué*) con la finalidad de facilitar el contraataque del regimiento 3 desde el flanco izquierdo.

Para ir cerrando esta introducción, lo verdaderamente importante en toda operación militar es la "FINALIDAD" que es el objetivo a cumplir por la totalidad de las fuerzas. En la idea que se propone aquí, cada una de las "cumbres" que se defiendan (*es decir cada una de las capas a las que presta función un "host"*) deben analizarse al detalle "**nivel a nivel**" adoptando todas las medidas posibles en cada uno de ellos hasta su máxima capa (*Ejemplo, Switch: nivel 2, Router: nivel 3, FW: Consideremos nivel 4, servidor de correo: nivel 5*).

Cada dispositivo estará protegiendo esos "valles" y "vías de comunicación" que son las zonas en que está colocado, aprovechando todas las posibilidades que en cada una de sus capas tiene a

disposición. Si cada uno de ellos lo hace bien, se logrará cumplir con la "**finalidad**" de la misión, que es donde estarán los recursos más valiosos. Esta zona en la profundidad de nuestra defensa informática será donde están los servidores críticos de la empresa y la información de mayor impacto, la cual, como buena información que es, se aloja en los niveles más "altos": BBDD, almacenamiento de correos, Servicios de directorio, de archivos, configuraciones de elementos, almacenamientos de Logs, etc.… y que en la charla anterior definimos como "Línea a no ceder" o "Línea de Retardo Final".

También presentaremos un aspecto en cuanto "corte transversal" de nuestras redes, para poder segmentar muy claramente:

- Red de Gestión.
- Red de Servicio.

Por lo tanto, el tema de hoy estará dividido en dos líneas de avance:

1) **Planos de altura (niveles TCP/IP)**
2) **Planos de Segmentación en redes de: Gestión y Servicio.**

5.2. Conceptos militares

En este punto, vamos a centrarnos en el **Reglamento "El combate en montaña"** del Estado Mayor del Ejército de España (**R-0-4-36**). Por supuesto que no lo desarrollaremos en detalle pues se trata de un documento de 154 páginas. Del mismo, a continuación, citaremos textualmente los párrafos sobre los que centraremos la atención, y al final de esta sección haremos el análisis de los mismos.

Punto 2.1.5. Extraordinario valor de las vías de comunicación.

Normalmente, la ocupación de una zona de montaña no constituirá por sí misma el fin de una operación, ya que no existirán en ella objetivos de carácter estratégico decisivo.

*La red de comunicaciones, dará lugar a la existencia de **zonas clave**. La importancia de esas zonas estará determinada por el número de comunicaciones que sobre ella confluyen. Constituirán los objetivos naturales de la maniobra ofensiva y, consecuentemente, las áreas que en defensiva habrá que conservar a toda costa, por influir de una manera decisiva en el desarrollo de las operaciones.*

*Los **valles** constituyen las líneas naturales de esfuerzo; y el valor de las alturas que los dominan dependerá de la posibilidad de ejercer acciones por el fuego o movimiento sobre ellos y sobre los puntos de paso obligado.*

2.2. La Maniobra.

La montaña no suele constituir por sí misma el objetivo de una campaña, pues normalmente no existirán en ella objetivos de carácter estratégico.

En definitiva, la lucha en la montaña no tendrá otra finalidad que impedir, o intentar impedir, el paso a través de ella hacia objetivos políticos o estratégicos, que serán el fin último de las operaciones.

*La **sorpresa** es el factor esencial del éxito en toda maniobra en montaña. Durante la ejecución de cualquier maniobra, ha de ser una preocupación constante del mando tanto buscarla como adoptar medidas adecuadas de seguridad para precaverse contra ella, dado que en montaña es más fácil que se produzca.*

En montaña puede ser más decisiva la sorpresa que la fuerza.

Capítulo 3 - La seguridad en montaña

3.1. Generalidades

El mando necesita:

- *Poseer, con extensión y detalle variables, información previa sobre el enemigo y el terreno, para adoptar su decisión.*
- *Disponer de un espacio que le permita desplegar con seguridad sus fuerzas.*

Sus finalidades son:

- *Proporcionar tiempo y espacio al Mando para decidir y preparar su maniobra, y a las unidades para que puedan concentrarse, desplegar, maniobrar y combatir, a pesar de la voluntad y propósitos del enemigo.*
- *Proteger las tropas contra la sorpresa.*

3.2. Factores de la seguridad

- *La información.*
- *El despliegue, y las medidas de protección de las tropas.*
- *El secreto.*

Capítulo 4 - El combate ofensivo en montaña.

4.1. Generalidades

El dominio de los valles será finalmente el objetivo a conseguir, pues por ellos transcurren las vías de comunicación indispensables para la progresión de Grandes Unidades, pero el ataque a lo largo de ellos chocará contra las defensas más fuertes y caerá bajo la acción de los fuegos y contraataques de las fuerzas enemigas que se encuentren en las laderas y alturas que los dominan.

Capítulo 5 - EL combate defensivo en montaña

5.1. Generalidades

El combate defensivo en montaña, al igual que en el llano, se propone esencialmente anular la capacidad ofensiva del enemigo.

Deberá pretenderse en todo momento ampliar en el mayor grado posible la libertad de acción mediante:

- *La elección de la zona de terreno más favorable a la defensa.*
- *El meditado estudio, aplicación y desarrollo de un acertado plan defensivo.*
- *El aprovechamiento oportuno y eficaz de cualquier síntoma de debilidad o error enemigo.*

En la defensiva en montaña ha de tratarse de conseguir la sorpresa táctica mediante un acertado plan de obstrucciones.

*Dado el extraordinario valor que para un atacante tiene la posesión de las **vías de comunicación**, el defensor tendrá que montar su defensa a caballo de ellas para cerrarlas.*

5.2. Ventajas e inconvenientes de la defensiva.

La defensiva en montaña presenta las siguientes ventajas:

- *Aumento de la capacidad de resistencia del defensor por la existencia de pendientes y obstáculos naturales que dificultan la progresión del atacante.*
- *Posibilidad de cubrir, con los mismos medios, frentes más amplios que en terreno llano, resultado de la solidez del terreno, que puede considerarse naturalmente fortificado. En consecuencia, economía de medios.*
- *Facilidad de mayor observación lejana y extensa desde puntos dominantes.*
- *Gran valor del obstáculo.*

5.3. Tipos de defensiva.

- *Sin línea de retroceso.*

- *En profundidad.*

5.3.1.1. Posición defensiva.

Es la zona de terreno donde se desarrolla y decide la batalla defensiva y, por consiguiente, constituye la parte más importante del conjunto del área de defensa.

Se tenderá a que la posición defensiva reúna las condiciones precisas que permitan:

- *Cerrar vías de comunicación.*
- *Disponer de comunicaciones a retaguardia, tanto longitudinales como transversales.*
- *Dominar, por la observación y los fuegos, la mayor profundidad posible del terreno.*

De modo general se puede considerar que existen dos tipos de posiciones: las de arreamiento del os valles seguidos por las vías de comunicación, y las situadas en zonas dominantes.

- *De Barreamiento de los valles. Se establecerán con preferencia en los estrechamientos que forme la montaña, tales como desfiladeros o puntos de paso obligado; se organizará la defensa en el fondo del valle y en las pendientes que desde las alturas laterales caigan sobre él.*
- *En zonas dominantes. Son posiciones establecidas en alturas que dominan un valle y que ofrecen grandes ventajas por la fortaleza que proporcionan las fuertes pendientes, por el dominio de vistas con que cuentan por la necesidad que tendrá el enemigo, si no se decide a atacarlas frontalmente, a realizar largos y difíciles movimientos para tratar de envolverlas, en lo que invertirá mucho tiempo y someterá a sus tropas a grandes fatigas.*

5.3.1.1.3. Ejecución de la maniobra defensiva en la posición defensiva.

En la montaña, la maniobra defensiva se basa fundamentalmente en la determinación de zonas clave dentro del sector asignado. En consecuencia, la maniobra se montará inicialmente a caballo de las vías de comunicación, ocupando posiciones que controlen los accesos más importantes a dichas zonas clave y vigilando el resto.

El defensor se opondrá, asimismo, a las penetraciones enemigas, mediante contraataques y ocupando, de acuerdo al desarrollo del combate, posiciones eventuales preestablecidas.

Cuando no se pueden eliminar las penetraciones enemigas, se tratará de contenerlas llevando a cabo una defensa a toda costa de zonas clave, en espera de la actuación de las reservas del escalón superior.

5.3.2. La defensiva en profundidad.

El desarrollo de una maniobra en profundidad en su concepto estricto no será normal en montaña.

La propia fortaleza del terreno no aconseja el abandono deliberado de zonas importantes cuya reconquista sería muy dificultosa. La defensa en profundidad en montaña, debe entenderse como una serie de posiciones en profundidad a defender sin idea de retroceso.

Ello no excluye, naturalmente, el que puedan tener lugar acciones localizadas de desgaste y retardo a cargo de fracciones elementales, llevadas a cabo entre dos posiciones defensivas consecutivas dentro de la dinámica general de la defensa en montaña. En tal caso, estas acciones se verán favorecidas por la presencia de numerosos puntos de paso obligado sobre los que en un reducido número de efectivos tendrán capacidad para detener un tiempo importante a las columnas enemigas.

Análisis de estos párrafos:

Como en todo análisis o confrontación de conceptos, lo importante es obtener resultados, reflexiones o aspectos de esta visión militar que nos permitan ser aplicados en nuestras infraestructuras para mejorar nuestra seguridad.

Durante el cursado del doctorado, tuve de profesor a "José (Pepe) Mañas". Este docente es el creador de la metodología MAGERIT de análisis de Riesgo. Independientemente de las virtudes y defectos que cada uno puede poner de manifiesto en toda metodología, bajo mi punto de visto (*y es una opinión estrictamente personal*), la maravillosa virtud que tiene MAGERIT, es cómo secuencialmente nos lleva una y otra vez a mirar cada aspecto desde diferentes puntos de vista (*dando vueltas y vueltas sobre un análisis*), hasta lograr agotar cada aspecto pues lo hemos evaluado con todo detalle desde diferentes ángulos.

Cuando hablamos de seguridad, cuanto más detalle pongamos en su evaluación, menos "sorpresas" nos encontraremos, y más robusta será nuestra infraestructura.

Esta nueva propuesta de "**Combate en montaña**" tiene esta finalidad, encontrar nuevos puntos de vista que nos aporten mayor detalle en nuestro análisis de seguridad, por ello lo que os propongo es quedarnos al menos con los siguientes conceptos:

a. Las vías de comunicación (Accesos más importantes).

El avance hacia la profundidad de nuestras redes, no es posible por cualquier camino o ruta. Existen definidos dispositivos, protocolos, rutas, direcciones, puertos y aplicaciones que son las verdaderas "vías de comunicación".

Reveamos el concepto militar:

Extraordinario valor de las vías de comunicación.

*La red de comunicaciones, dará lugar a la existencia de **zonas clave**. La importancia de esas zonas estará determinada por el número de comunicaciones que sobre ella confluyen.*

Es decir, tenemos en nuestras manos un factor fundamental en la clasificación de zonas clave de nuestras redes: Número de comunicaciones que sobre ella confluyen. ¿Hemos analizado alguna vez desde este punto de vista?

*Dado el extraordinario valor que para un atacante tiene la posesión de las **vías de comunicación**, el defensor tendrá que montar su defensa a caballo de ellas para cerrarlas.*

b. Dominio de los valles.

*Los **valle**s constituyen las líneas naturales de esfuerzo.*

El dominio de los valles será finalmente el objetivo a conseguir, pues por ellos transcurren las vías de comunicación

Para nosotros "los valles" son el interior de cada una de las zonas a las que estas "cumbres" están conectadas. Es decir, si poseo un dispositivo sobre el que puedo configurar ciertas medidas de seguridad, el mismo debo enfocarlo haca los "valles" (o zonas) a las que está conectado. No me sirve de nada plantear medidas de seguridad que no apliquen sobre estos "valles", nuestro foco de atención debe estar aquí.

Veremos en la sección siguiente que cada "altura" (nivel) se debe analizar de forma diferente, en virtud de los "valles" (zonas de red) a los que esté conectado.

c. Alturas dominantes.

Facilidad de mayor observación lejana y extensa desde puntos dominantes.

Son posiciones establecidas en alturas que dominan un valle y que ofrecen grandes ventajas

Debemos ser capaces de identificar cuáles son las alturas dominantes de cada una de nuestras zonas de red, y trabajar sobre ellas las medidas de seguridad oportunas. No tiene sentido centrarnos en la seguridad sobre dispositivos que no son "dominantes" de esa zona.

Veremos a continuación que, en determinadas zonas de red, hay alturas (niveles) que tienen mayor importancia que otros.

d. Zonas clave.

En la montaña, la maniobra defensiva se basa fundamentalmente en la determinación de zonas clave.

Ocupando posiciones que controlen los accesos más importantes

Acabamos de ver un concepto fundamental sobre la concentración de vías de comunicación para determinar zonas clave. Por supuesto que existen también zonas clave que por su "importancia estratégica" debemos tener en cuenta (Información crítica, dispositivos críticos de red, servicios de alta disponibilidad, etc.). La definición y análisis de cada una de estas "zonas clave" deberá ser un trabajo básico de seguridad.

e. Sorpresa táctica.

*La **sorpresa** es el factor esencial del éxito en toda maniobra en montaña.*

En montaña puede ser más decisiva la sorpresa que la fuerza.

En la defensiva en montaña ha de tratarse de conseguir la sorpresa táctica mediante un acertado plan de obstrucciones.

Este es un punto de vista novedoso que nos ofrece la visión militar, la "sorpresa" como medida de seguridad. Esta medida puede ser implementada desde diferentes actividades, pero siempre tendiente a evitar que el intruso sea consciente de nuestras medidas o contramedidas de seguridad.

f. Observación lejana y extensa.

Esto es un hecho más que conocido, cuánto más alto estoy, más lejos puedo ver. Por lo tanto, jamás dejemos de adoptar medidas de seguridad al máximo nivel (*en todo sentido*).

5.3. Planos de altura (niveles TCP/IP).

La profundidad de la defensa informática estará dada por cada una de las zonas en las que dividamos los sistemas de nuestra organización. Las puertas de acceso y los caminos entre ellas lo proporcionan los diferentes elementos de red (switchs, puntos de acceso inalámbricos, routes, firewalls, etc.) y la interconexión entre ellos. Estos nodos de red delimitarán y segmentarán las diferentes áreas en las que deseemos instalar los servidores y hosts. Las zonas mínimas que debemos contemplar son:

- Redes externas.
- DMZs (Zonas desmilitarizadas).
- MZs (Zonas Militarizadas).
- Core (Zona de máxima seguridad).

Por supuesto que puede haber más de una de cada, como también en redes menores pueden agruparse o minimizar este concepto, lo importante es tomar esta idea como un modelo de referencia a cumplir.

Este tema está bastante desarrollado en el libro "**Seguridad por Niveles**" (*que puede descargarse gratuitamente en:* http://www.darFe.es), por lo tanto, no se profundizará sobre estos aspectos para avanzar sobre el concepto de "Altura".

5.3.1. El primer nivel (Físico).

El primer punto a desarrollar será nuestra frontera física, como su nombre lo indica abarca temas de seguridad en los locales, medidas contra incendio, humo, partículas, humedad, accesos de personas, video vigilancia, continuidad eléctrica, cableado estructurado, etc. Este tema está desarrollado en detalle en el ANEXO 2 (Consideraciones a tener en cuenta en un CPD) del libro "**Seguridad por Niveles**", así que nuevamente, remitiros a este para ampliar la idea.

Un aspecto que está cobrando mucha importancia son los accesos WiFi y 4G (*por medio de Small Cell*). En ambos casos hay aspectos de seguridad física que deben ser tenidos en cuenta, como son: potencia y direccionalidad de irradiación, modulación, codificación, recuperación de errores, interferencias, fallback hacia 3G o 2G, etc.

Hoy en día en cualquier teléfono móvil, se posee un sistema operativo completo y capacidad de almacenamiento similar a cualquier ordenador, por lo tanto, la seguridad física del mismo no puede ser dejada de lado. Lo mismo está sucediendo con dispositivos de almacenamiento externo (*USB, Tarjetas SD; discos externos*) en los que en muchos casos se almacena información sensible, claves, documentos, planos, etc. En los casos de pérdida o robo exponen mucha información o la dejan en manos que pueden ser peligrosas.

5.3.2. La segunda cumbre: el nivel de enlace.

En este nivel se debe centrar la atención en la comunicación con el "**nodo adyacente**", es decir nuestra visión de la seguridad en este nivel, debe centrarse en dispositivos que en realidad se encuentran relativamente "próximos" (*si bien hay que aclarar que, con la potencia informática de hoy, las nuevas técnicas de modulación y las fibras ópticas, esta idea es muy relativa*).

El detalle de este nivel, podemos encontrarlo bastante desarrollado en el capítulo 4: Switching, del libro "**Seguridad en Redes**" (*que también puede descargarse gratuitamente en:* http://www.darFe.es), pero los conceptos fundamentales de seguridad a considerar aquí son:

- Protocolos de la familia **IEEE 802.x**, en particular desde el punto de vista de seguridad:
  - 802.1D: Spanning Tree Protocol
  - 802.1aq: Shortest Path Bridging (SPB)
  - 802.1Q: Virtual Local Area Networks (VLAN)
  - 802.1x: Autenticación de dispositivos conectados a un puerto LAN
  - IEEE 802.11 – Redes inalámbricas WLAN. En particular 802.11i y 802.11w
- MPLS (Multiprotocolo Label Switching).
- Para telefonía móvil, un buen punto de partida es 3GPP y el **TS33.401**.
- Merece la pena hacer mención a un nuevo concepto que está naciendo que es el de "HetNet" (Redes Heterogéneas) que desde el punto de vista de enlace, mezclarán todo tipo de tecnologías de acceso: cable, fibra, WiFi, Wimax, telefonía móvil y fija, etc.

Durante esta charla, desde ya que no tenemos tiempo para

desarrollar cada uno de ellos, pero sí dejamos algunas reflexiones de este nivel:

1) Autenticación y control de acceso: En las zonas de red en las cuáles los usuarios pueden "validarse" con su equipamiento, debe considerarse la implementación de medidas basadas en este tipo nivel, como 802.1x y 802.11i.
2) El parámetro, tal vez más importante, de este nivel es el direccionamiento **MAC** (de seis octetos hexadecimales). A este esquema de direcciones sólo se accede dentro de la red LAN. Es decir, estas direcciones, tal cual se define este nivel, se ven desde "nodos adyacentes". En virtud de esta característica, es que se debe prestar especial atención a los "segmentos LAN" que se evalúan. En particular los siguientes aspectos son especialmente peligrosos:
   - Falsificación de direccionamiento MAC.
   - Envenenamiento de caché ARP (arp poisoning), con esto se implementa el ataque del hombre del medio a nivel MAC.
   - Flappeo de MAC (en switches, fallos o errores de 802.1D u 802.1aq).
3) VLAN Hoping: Lograr saltar entre diferentes VLANs (aplica sobre el protocolo 802.1q)
4) A nivel acceso de telefonía móvil, aún existen varias vulnerabilidades en el cifrado de la interfaz radio de 2G y 3G.

5.3.3. El nivel de red.

El detalle de este nivel, podemos encontrarlo bastante desarrollado en el capítulo 5: Routing, del libro "**Seguridad en Redes**".

Los aspectos a considerar en este nivel son:

- Definir e identificar claramente, los routers críticos, de frontera (*con empresas, proveedores, clientes, internet,*

etc.), de interconexión, de core, de acceso, reflector, routers P y PE.

- Bastionado de routers.
- Auditorías periódicas de estos dispositivos.
- En las zonas de máxima seguridad, de ser posible emplear rutas estáticas.
- Donde sea necesario el empleo de protocolos de enrutamiento dinámico, emplear los que permitan autenticación, integridad y confidencialidad.
- En los dispositivos "frontera" con otras redes, las vías de comunicación pueden ser muchas. En estos casos, el nivel de red es especialmente vulnerable cuando sus direcciones IP son públicas y las Listas de Control de Acceso (ACLs), tienen problemas para ser "ajustadas", es decir: no podemos restringir de forma adecuada (u óptima) los puertos y direcciones origen y destino.
- En los dispositivos interiores, se debe prestar especial atención al empleo de los protocolos de enrutamiento dinámico, en cuanto a autenticación, confidencialidad e integridad y el empleo de protocolos seguros.
- En toda red la "Segmentación" de sus propias redes o subredes será uno de los factores claves de seguridad. El nivel de red es quien puede asegurar las comunicaciones principales, permitiendo o negando rutas donde sea necesario. Jamás olvidéis la "Segmentación" de las zonas de red.
- En los routers "P" y "PE" que empleen MPLS, se debe ser muy riguroso en sus protocolos de enrutamiento interior y en las asociaciones entre VLAN y VRF.
- La Calidad de Servicio (o QoS), estará ligada al nivel de red en la mayoría de los casos, por lo tanto, el control de los bits de "servicios diferenciados" debe ser un aspecto a considerar en aquellas zonas en las cuáles este parámetro

afecte al negocio.

5.3.4. El nivel de transporte.

El nivel de transporte es quien nos abre las "puertas" de las aplicaciones, por lo tanto, tendrá especial impacto en aquellas zonas en las que se ofrezcan "servicios" o sobre los dispositivos que se emplean para "gestión" de las redes.

En cada zona hay puertos que son bien conocidos por sus fortalezas y debilidades, también hay puertos que no tienen ningún sentido en determinados segmentos. Hay puertos que se emplean específicamente para una comunicación "interna" de nuestra empresa, y hay puertos que estaré obligado a dejar abiertos hacia comunicaciones "externas".

El **control de puertos** es una de las tareas más importantes que debemos asociar específicamente a cada zona, dispositivo, servicio y/o aplicación. El principio más importante a considerar es NO dejar ningún puerto abierto que no se use. Por otro lado, tenemos también la ventaja que los puertos TCP poseen "direccionalidad" es decir que pueden ser abiertos en un sentido y/o en otro, por esta razón se deberá considerar este parámetro como fundamental. El protocolo (TCP) también tiene la potencialidad de "**control de sesiones**", característica que puede ser empleada para bien o para mal, debemos evaluarla en detalle.

Otra función primaria del protocolo TCP es el "**control de flujo**" por lo tanto es uno de los responsables de "regular el ancho de banda" por medio de una técnica conocida como "ventana deslizante". Esta función de TCP también debe ser considerada en detalle en todo servicio que se exponga en cada zona pues, sumado al control de sesiones, es una de las formas más sencillas de lanzar ataques de Negación de Servicio.

Otro factor importante que en la actualidad se tiende a implementar con TCP es la "**segmentación y re ensamble**" (*que implica también el concepto de "**entrega ordenada**", ambas funciones también se pueden realizar por medio del protocolo IP, pero se está generalizando hacerlo por TCP*). Esta función, cuando se generan errores (intencionales o no), puede tirar abajo toda la red. Por seguridad, deben ser muy bien dimensionados, monitorizados y evaluados permanentemente estos parámetros.

5.3.5. El nivel de aplicación.

Este nivel (que no deja de ser otra cumbre más y que también depende de la zona o valle que esté conectado o protegiendo) no lo desarrollaremos en esta charla por tratarse de los diferentes servicios que se ofrecen hacia los usuarios, y el foco principal de este ciclo de Ciberseguridad está orientado a "redes".

5.4. Planos de segmentación de las redes de: Gestión y Servicio

En toda infraestructura de red se debe hacer un importante esfuerzo por poder "**aislar**" la red de gestión del resto de las redes, y en particular, de la que presta servicios.

La **red de Gestión** debe ser accesible únicamente por el personal responsable de los dispositivos y a su vez, que cada uno de ellos sólo puede acceder a los elementos de su responsabilidad (*y a ningún otro*). Tengamos en cuenta que desde esta red se accede a las plataformas, direcciones y puertos que abren juego hacia el "control total" de los elementos.

A una "Red de Gestión" puede accederse mediante dos metodologías:

- Ubicaciones o Centros de Gestión: Son locales, o edificios que tienen conexión con los dispositivos y, únicamente estando

físicamente en esas salas, se alcanzan las direcciones y puertos específicos de gestión de dispositivos.

- Plataformas de acceso a redes de Gestión: A través de dispositivos de control de acceso o máquinas de salto, las personas autorizadas, se validan en ellos, y desde estos dispositivos tienen acceso a los elementos que se desean gestionar.

En ambos casos, los dispositivos a gestionar deben tener al menos dos interfaces de red (*si bien esto podría hacerse con una sola interfaz física con "alias" o más de una dirección IP, no se recomienda hacerlo de esta forma*). Una de ellas es la que deberá pertenecer al rango de direccionamiento de la "Red de Gestión". Este rango no debería estar enrutado hacia, ni desde ninguna otra red, por lo tanto, los routers que lleguen a esta red no tendrán Gateway por defecto, ni encaminamientos de rutas que permitan que se alcance la misma. Para que la red de gestión sea intrínsecamente segura, es necesario también que en **todo** dispositivo que posea una interfaz conectada a la misma, se configuren al menos tres medidas:

- Reglas de Firewall locales para que solo acepte conexiones desde el/los dispositivos de control de acceso, máquinas de salto o segmento asignado al Centro de Gestión. Esta medida, si bien puede ser comprometido un dispositivo desde otra red, no permitirá que desde el mismo se pueda saltar a ningún otro
- Limitación de los comandos de gestión, monitorización y troubleshooting (telnet, ssh, ftp, icmp, finger, snmp, etc..) únicamente al usuario root.
- Sistema de Logs que registre cualquier acción no permitida y de ser posible los envíen a un servidor externo.

Si se mantienen los conceptos de los párrafos anteriores, sólo existen dos formas de llegar a esta red. Teniendo bocas de red cableadas en este rango (*Ubicaciones o áreas de gestión*), o instalando dispositivos de acceso (*dispositivos de control de acceso o máquinas de salto*) que también posean una interfaz conectada a este segmento de gestión.

Desde la red de Servicio, no debería haber ningún tipo de

"**visibilidad**" hacia estos rangos de red. La red de servicio en sí debería estar segmentada de forma tal que ofrezca sus funciones únicamente a los usuarios que preste servicio y nadie más. Este aspecto también es importante a considerar pues, por ejemplo, a un servidor de ficheros del área de I+D, sólo debería ingresar el personal de esa área o quien haya sido autorizado, ninguna otra área de la empresa y mucho menos alguien ajeno a la misma. Independientemente que luego ese servidor en sí tenga medidas de bastionado, autenticación y control de acceso, la **red** en sí misma, también debería contemplar medidas para que ese servidor no sea alcanzable desde donde no se desee.

Este enfoque también debe ser considerado como planos diferentes, es decir dos alturas que no comparten puntos de conexión.

5.5. Tareas para el hogar (deberes).

Una vez más en este capítulo os propongo llevarnos algunas actividades o líneas de reflexión para que comencemos el capítulo siguiente con otro breve debate sobre los mismos.

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Puedo identificar claramente mis valles o zonas de red?
2. ¿Puedo determinar las potenciales vías de aproximación de cada una de ellas?
3. ¿Qué medidas concretas por nivel o altura puedo adoptar en cada dispositivo de red de cada una de esas zonas?
4. ¿De qué forma puedo analizar, diseñar e implantar medidas para cuidar el factor sorpresa en cada nivel?
5. ¿Merece la pena en mis redes, implantar redes de gestión? ¿cómo sería mejor hacerlo en mi organización?

6. Este nuevo punto de vista, ¿me ha dado una visión más amplia o más lejana del detalle de mis redes?

6. Ciberseguridad: La importancia de los procesos.

Resumen del tema

Los procesos pueden parecer poco interesantes para alguien que desea dedicarse a Ciberseguridad, pero nuestra experiencia al respecto es que juegan un rol fundamental en toda organización de la Seguridad, pues son los que verdaderamente regulan "*qué se puede y que no se puede hacer*"; sin ellos cualquier persona deja librada a su criterio personal y aislado las diferentes medidas, acciones, decisiones, permisos, rutas, reglas, borrados, cambios, procederes, reacciones…… cualquiera de estas palabras suenan a *¡Peligro!* en alguien que se dedique a estos temas.

A lo largo de estos últimos años, hemos tenido la posibilidad de auditar un importante número de redes y también a realizar el seguimiento y retesting de las mismas, lo que más nos llamó la atención es justamente que gracias a haber hecho un fuerte hincapié en estos procesos se ha manifestado un cambio radical en todas ellas. Por esta razón es que si bien somos conscientes que existen muchos más procesos de los que presentamos en este capítulo, hemos seleccionado específicamente **ocho** que creemos son los que cobran una importancia básica en la Seguridad de redes.

Durante el desarrollo de este capítulo presentaremos cada uno de ellos, y desarrollaremos los aspectos principales que deben ser tenidos en cuenta en su contenido.

6.1. Planteo inicial.

Centraremos la atención sobre los aspectos fundamentales que deben tenerse en cuenta a la hora de diseñar, redactar e implementar estos procesos.

Un aspecto muy frecuente que nos hemos encontrado es que existen los mismos, se encuentran muy bien redactados y completos, se mantienen actualizados y con una buena metodología de control de cambios, pero…. En la práctica, no se aplican, las diferentes áreas los desconocen o directamente no los cumplen, por que no quieren o como también sucede en varias oportunidades, no se "han bajado a tierra", es decir, se han contemplado todos los detalles, pero desde la "estratosfera", cuando los mismos se intentar hacer realidad, generan más complicaciones que solución, y cuando acontecen estos hechos, los procesos mueren.

En cualquier caso, nuestra intención a transmitir en este capítulo es que todo esto que escribamos en nuestros procesos:

- Sea aplicable e implementable.
- Se mantengan vigentes.
- Se audite su correcto cumplimiento.

Específicamente, estos ocho son los procesos que cobran una importancia básica en Ciberseguridad desde nuestro punto de vista:

- Entrada en producción
- Gestión de cambios
- Gestión de accesos
- Configuraciones e inventario
- Gestión de Backup
- Gestión de Incidencias
- Supervisión y Monitorización
- Gestión de Logs

6.2. Presentación de los procesos.

El detalle particular de cada proceso puedes verlo en el **capítulo 3** del libro "**Seguridad en Redes"** (*que se puede descargar gratuitamente en: www.darFe.es"*). En esta presentación, sólo nos centraremos en los conceptos clave de cada uno de ellos.

6.2.1. Entrada en producción.

La idea del procedimiento de entrada en producción, es el conjunto de pasos a seguir desde que un dispositivo, plataforma o servicio es "imaginado", pensado o planificado hasta que el mismo entra en producción.

Como cualquier informático sabe, todo lo que no se aplica desde el "diseño" mismo, luego su coste es exponencial. Por lo tanto, los aspectos de **Seguridad** deben ser contemplados **desde el inicio mismo** de este flujo, sino costar mucho más cuando surja a futuro o será imposible de implantar.

Básicamente se deben considerar tres actividades:

a. Análisis técnico.
b. Pruebas de Laboratorio.
c. Pruebas en Red (***FOA**: First Office Application*).

De cada uno de ellas se desencadenarán una serie de "Sub" procesos.

Si todo ha sido correcto los siguientes pasos serán:

a. Autorización de Introducción en planta para Despliegue.
b. Documentación de Despliegue.
c. Informe de Acreditación de Seguridad.
d. Informe de Pruebas FOA.

6.2.2. Gestión de cambios.

Hemos podido verificar que en reiteradas oportunidades las incidencias de alto impacto, se producen por errores, o ausencia de un procedimiento estricto de "control de cambios". Debido a ello, el proveedor o empleado, ha accedido a un dispositivo o plataforma, por ejemplo: en ventanas de tiempo críticas, con escalado de privilegios, con usuarios genéricos, en zonas restringidas, ejecutando comandos que no debía, por accesos –vínculos - enlaces o plataformas no autorizados, sin dejar "Logs" de su actividad, excediendo los permisos que tenía para realizar una determinada actividad, etc. Y con ello se han sufrido caídas de horas (*e inclusive días*) en servicios críticos (*DNSs, Servidores, Switchs y Routers de Core….)*

El principal objetivo del proceso es que paulatinamente se esté intentando, paso a paso, ajustar al máximo estos detalles. Nuestra experiencia es que en general, se trata de un proceso que aún en las grandes redes no se le ha dado la importancia que merece.

Lo ideal es lanzar un plan de acción a medio plazo que permita implantar un proceso de Gestión de cambios e **integrarlo** con:

- Gestión de usuarios.
- Alguna metodología de Identity Manager.
- Workflow de seguimiento.
- Gestión de incidencias.
- Proceso de "autenticación" o "Control de accesos"

6.2.3. Gestión de accesos.

Lo más importante a considerar para la "Gestión de accesos" es tener la capacidad de derivar a cada uno **exactamente** dónde debe acceder.

Ni a más, ni tampoco a menos dispositivos/servicios/redes/ aplicaciones/funciones que las que le corresponde.

La gestión de los dispositivos, es una actividad que debe ofrecer disponibilidad y redundancia máxima para poder llegar y conectarse a los diferentes elementos ante cualquier anomalía o para tareas habituales de administración, pero no por ello desde el punto de vista de la seguridad, debemos emplear "reglas holgadas" para que todo el mundo pueda hacerlo, sino todo lo contrario. No es sencillo, pero sí es muy importante poder garantizar que "**solo accede quien debe hacerlo y con los privilegios que necesita**".

Las ideas fuerza con la que nos deberíamos quedar en cuanto al funcionamiento de esta actividad son:

a. Qué exista y se cumpla un documento "Control de accesos".
b. Deben estar definidos los pasos para la solicitud, administración y anulación de los derechos de acceso.
c. Debe existir el rol de "Gestor de usuarios", y esta persona (*o área*) mantendrá actualizado "registro y gestión de identidades".
d. Debe establecerse y llevarse a la práctica el Ciclo de vida de las cuentas de usuarios.
e. Es importante el empleo de herramientas de workflow para control de accesos para poder tener una trazabilidad completa de los mismos.
f. Debe estar documentado y definido un perfilado de usuarios para los diferentes accesos (*Lectura / Mantenimiento estándar / Mantenimiento avanzado/ Administrador, etc.*)
g. De ser posible debería estar integrado con AD, LDAP, RRHH, etc.
h. Se debe hacer todo el esfuerzo posible para eliminar las cuentas genéricas y locales en los dispositivos.
i. Debe ser riguroso el empleo de diferentes "Privilegios" de acuerdo al nivel de acceso.

j. Se deben emplear siempre "Ventanas de acceso" cuando se realicen actividades que pueden ser críticas para la estabilidad de la red.

k. Se debe incrementar al máximo el concepto de "Granularidad" para el acceso a los diferentes dispositivos. (elemento, red, plataforma, proveedor).

l. Es fundamental implementar "Plataformas de trazabilidad de accesos", que permitan realizar cualquier tipo de análisis sobre el ciclo histórico de accesos.

m. Una de las actividades básicas de cualquier intruso es la evasión de los controles de acceso, por lo tanto, debe ser implementadas "Medidas de control" sobre potencial evasión del control de acceso.

Para la gestión de accesos, es de suma importancia el concepto que tratamos la charla anterior (alturas) sobre "**Segmentación de redes**", en particular "Redes de Gestión". Para poder asegurar que las configuraciones de nuestros elementos de red cumplan con los requisitos de seguridad establecidos, una de las reglas básicas es poder diferenciar bien diferentes zonas desde las cuales la "visibilidad y funciones" de los dispositivos responden de diferente forma.

6.2.4. Configuraciones e inventario.

Cuando hablamos de Ciberseguridad, es imposible adoptar medidas o tomar decisiones si no sabemos qué es lo que se debe asegurar. Ninguna empresa de seguros otorgaría una póliza sin saber qué es lo que está asegurando, ninguna empresa de vigilancia podría prestar servicio si no supiera qué debe vigilar…. en una red es exactamente igual.

Es imposible abrir una regla de Firewall si no se conoce en detalle la comunicación de extremo a extremo que se está habilitando, no se puede lanzar un plan de continuidad de negocio si no se sabe

con qué recursos se cuenta, no se puede crear una VLAN (*Virtual LAN*) si no se sabe cuáles son los elementos que la deben integrar. Podríamos seguir citando cientos de ejemplos más, pero cualquier tipo de análisis de seguridad que se desee realizar necesita contar con el máximo nivel de detalle sobre las configuraciones e inventario sobre el que se va trabajar.

Es cierto que, en una gran red, es muy difícil mantener actualizada la planta y las configuraciones de cada elemento, pues la dinámica actual es muy grande, pero no por ello se deben bajar los brazos.

El inventario de activos debe ser lo más completo posible (*descripción del activo, propietario del activo, encargado del tratamiento del activo, nivel de criticidad, etc.*)."

¿Cuáles son los aspectos más importantes que debemos considerar al respecto?:

a. Procedimiento de configuraciones y gestión de inventario (*redacción, aprobación y existencia del procedimiento*).
b. Alcance del procedimiento (*áreas a las que aplica y las que no*): ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización?
c. Detalle del nivel alcanzado (*Hitos a cumplir, importancia de campos, flujos de alta, modificación y baja de datos, metodología de actualización y mantenimiento, parches y obsolescencia, responsables de los datos, etc.*). Se trata aquí de evaluar la profundidad y el nivel de detalle de este procedimiento. En general suele existir una gran debilidad en cuanto al mantenimiento de los mismos. En pocas redes se poseen herramientas más o menos automatizadas que ayuden a la actualización de los mismos, a su vez se podría afirmar que casi en ninguna existe un inventario centralizado que esté verdaderamente "vivo" y que facilite una información global de los elementos de red de la misma.
d. Integración de este proceso con los de "Entrada en Producción" y "Control de cambios" pues es la única forma de mantener "vivo" el mismo.

Una muy buena práctica que deseamos destacar aquí es la implantación de un mecanismo de control de obsolescencia con los diferentes proveedores, y bajo el cual, periódica y obligatoriamente se va recibiendo la información de las versiones a actualizar, parches a instalar, dispositivos que deberían ser cambiados, módulos, etc. La misma se ingresa al inventario y desde allí se pueden generar reportes, alarmas, acciones, etc.

El último aspecto a considerar también desde el enfoque de seguridad, es el de autenticación y control de accesos a la información de este inventario, pues es un repositorio de información vital para la red, cualquier persona no autorizada que obtenga estos datos ya tendría una importantísima base de conocimiento para poder trabajar en nuestras redes y sistemas.

Confrontación de planos con realidad *(¿Cómo analizar estas diferencias?)*. Este es un "**objetivo de control**" que no puede ser dejado de lado, pues debe ser uno de los indicios más claros del nivel de seguridad alcanzado en una infraestructura. Hemos verificado muchas veces que donde se pone de manifiesto un control estricto de inventarios, se posee un buen nivel de "concienciación en seguridad" pues estos inventarios se los considera como punto de partida de la actividad de esta área.

6.2.5. Gestión de Backup.

En general, se nota una gran diferencia entre el nivel de concienciación que tiene el perfil de personal de TI, respecto a la gente de red. Cabe señalar que los dispositivos de red, poseen mucha más estabilidad que los de TI (*aplicaciones, desarrollos, programas, BBDD, etc.*), también es cierto que existen muchísimos menos virus y troyanos para dispositivos de red que para los de sistemas, se suele hacer evidente que el personal no le presta el mismo grado de atención al resguardo y recuperación de sus configuraciones y Logs, es frecuente escuchar *"… pero es que este*

dispositivo no se ha caído nunca en sus años de servicio….”, en muchos casos es cierto, pero también en muchos otros no. Por esta razón es que creemos que es casi una obligación comenzar a despertar conciencia sobre la importancia de las copias de respaldo y también de sus procesos y pruebas de recuperación.

Otro inconveniente (*serio, real y concreto*) que nos encontraremos aquí es que muchas de estas plataformas y/o dispositivos son muy caros, y por esa razón no se poseen en maqueta o para pruebas, su criticidad tampoco permite hacer pruebas de restauración, pues ante cualquier fallo de estos dispositivos en producción el impacto es alto, esta es una realidad frecuente, ante la cual también tal vez se pueda hacer recapacitar a quien tenga la decisión de adquirir maquetas, o contratar estas pruebas por parte de los proveedores de estos dispositivos que sí poseen esas maquetas, y alquilándolos por el tiempo necesario, hacer las pruebas pertinentes de recuperación, obteniendo todas las conclusiones necesarias.

¿Qué aspectos debemos considerar para esta actividad?:

a. Que exista un procedimiento de respaldo y recuperación. (*Redacción, aprobación y existencia del procedimiento*).
b. El alcance del procedimiento (áreas a las que aplica y las que no). ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización?
c. Análisis de criticidad de elementos de red.

   Para poder realizar un adecuado plan de recuperación en tiempo y coste eficiente, es imprescindible contar con un análisis de detalle sobre cuáles son los dispositivos o plataformas críticas para la estrategia de negocio. En este control se trata de verificar si esta actividad se realiza y el nivel de detalle alcanzado
d. Análisis de criticidad de tiempos de fallo y recuperación.

   Idem anterior, respecto a un análisis de detalle sobre cuáles son los tiempos mínimos y máximos que cada plataforma, área, dispositivo puede soportar.

e. Inventario de soportes.

   ¿se encuentran debidamente identificados estos soportes?, ¿Existe alguna metodología o procedimiento para este inventariado?

f. Plan de pruebas (Desarrollo, hitos fechas y periodicidad, registros de pruebas correctas y erróneas).

   ¿Existe este plan?, ¿se cumple?, ¿hay registros al respecto?

g. Planes de mejora (estudios, propuestas, modificaciones al plan y procedimiento, acciones concretas).

   ¿se verifican acciones de mejora generadas por estas pruebas?

h. Descripción e implantación de mecanismos de: redundancia, rotación, extracción de discos y cintas, registros de entrada, salida y destrucción de soportes.

   ¿Existen estos mecanismos?, ¿se cumplen?, ¿son adecuados?, ¿hay constancias de ello?

i. Nivel de detalle en asignación de roles y responsabilidades.

   Responsables del: elemento, almacenamiento principal y secundario, otros resguardos, plataformas de resguardo y recuperación, acceso a la información, implantación, actualización y difusión del plan, pruebas de ejecución, etc. Verificación del detalle alcanzado.

Dado que el backup es el último recurso en caso de producirse una situación de pérdida de datos es muy importante definir un procedimiento de backup que sea común a todas las unidades de la empresa.

6.2.6. Gestión de Incidencias.

Este procedimiento debe contemplar todas las acciones relacionadas a la notificación, gestión y respuesta a incidentes de seguridad, definiendo claramente las responsabilidades, obligaciones y acciones a realizar en el tratamiento de incidencias.

Uno de los aspectos más importantes en el manejo de incidencias es el de "recopilación y análisis de evidencias", pues será la información de mayor interés a la hora de evaluar el hecho o realizar un análisis forense.

Existen varias RFC (Request For Comments) que regulan o estandarizan metodologías y procedimientos para el manejo de incidencias. Un buen punto de partida es la política de seguridad que propone la **RFC–2196** (Site Security Handbook) y también la anterior **RFC-1244**, de las cuáles recordemos los conceptos planteados en la segunda de nuestras charlas sobre:

- Protect and Proceed (**Proteger y proceder**)
- Pursue and Prosecute (**Seguir y perseguir**)

Este es el punto clave para el desarrollo de este procedimiento ante incidencias pues, tal cual hemos presentado en su momento, sin un riguroso análisis, diseño e implantación de acciones adecuadas es imposible realizar un "Seguimiento de intrusiones" con un cierto grado de efectividad.

En el caso de incidencias que sean generadas por intentos de intrusión, lo realmente crítico que posee este hecho es el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades (*Tema que también desarrollamos con el concepto de "**Acción Retardante**")*.

¿Qué aspectos debemos controlar especialmente con este procedimiento?:

a. Metodología para la notificación, gestión y respuesta a incidentes de seguridad de la información (*Redacción, aprobación y existencia del procedimiento).*
b. Alcance del procedimiento (*áreas a las que aplica y las que no*).

   ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización? Verificación de hasta dónde se cumple o no lo que establece la documentación.
c. Integración con Workflow de la organización.

En caso todas las organizaciones, existen hoy en día flujos de gestión de actividades, tareas, proyectos, etc. Este procedimiento debería estar integrado a estos flujos de forma tal que facilite la asignación de actividades al personal involucrado y permita realizar un seguimiento detallado de las mismas.

d. Nivel de Integración con "Control de cambios".

   Se ha verificado la ocurrencia de muchos incidentes de seguridad que se generan durante acciones de cambio en dispositivos de red, por lo tanto, cuando se está realizando este tipo de tareas, debe tenerse en cuenta un "ticket" o flujo que mantenga alerta a la organización para poder dar rápida respuesta si ocurriera este tipo de incidentes, ¿existe este tipo de integración?

e. Clara distribución de roles, responsables, funciones y cadena de llamadas.

   ¿Se cuenta con este tipo de documentación?,¿está actualizada?, ¿está al alcance de las personas adecuadas?, ¿funciona correctamente?

f. Mecanismos de monitorización, alarmas y escalado de incidencias.

   Una vez ocurrida una incidencia, ¿son correctos estos mecanismos?

g. Informes, estadísticas, acciones de mejora.

   ¿Existen evidencias de informes, o estadísticas sobre incidentes de seguridad?, ¿Se verifican acciones de mejora desencadenadas por estos?

h. Recopilación de evidencias.

   ¿Es factible recopilar evidencias sobre incidentes de seguridad?, ¿es ágil este mecanismo?, ¿funciona adecuadamente?

6.2.7. Supervisión y Monitorización.

Para poder ofrecer un grado de "**Disponibilidad**" mínimo es necesario contar con una infraestructura de "Supervisión y Monitorización". Desde el punto de vista de la Ciberseguridad a su vez, no sólo nos interesa por la disponibilidad, sino también para la detección temprana y la generación de alertas ante cualquier actividad anómala en la misma. Ambas funciones se llevan a cabo a través de:

- **NOC** (*Network Operation Center*).
- **SOC** (*Security Operation Center*).

Desde ya que estas funciones deberán ser acordes al tipo de red y se deberá asignar los recursos adecuados para cada tipología, pero lo importante aquí es ser conscientes de la importancia que revista esta actividad y plantearse SIEMPRE cómo se llevará a cabo, por mínima que sea la infraestructura.

En cuanto a la Supervisión / Monitorización / Alarmas, nuestra experiencia al respecto es muy positiva. En general todas las grandes redes, poseen algún tipo de mecanismos para esta actividad.

Inicialmente debemos diferenciar el concepto de NOC del de SOC, pues este último sí debería abocarse exclusivamente a seguridad, mientras que el primero no.

La aplicación de un procedimiento de este tipo, debería conducirnos a obtener una visión clara sobre:

¿Qué hace este personal si detecta alguna anomalía en la red, cuyos parámetros puedan estar relacionados con un incidente de seguridad?

Ejemplos típicos de ello son:

- Incremento anómalo de ancho de banda.
- Saturación del ancho de banda.
- Caídas secuenciales de dispositivos.
- Propagación abusiva de un determinado patrón de tráfico.

- Modificaciones sensibles del flujo de tráfico de nuestros DNSs.
- Incremento llamativo del volumen de Logs.
- Mensajes anómalos en los Logs de elementos de red.
- Alarmas en bases de datos, procesadores, módulos de memoria.
- Alteración de rutas.
- Fallos en los sistemas de señalización.
- Segmentos de red o dispositivos inalcanzables.
- Pérdidas de accesos de gestión a dispositivos.
- Modificación de contraseñas, cuentas, perfiles, roles, o directorios activos.
- Intentos reiterados de accesos (fallidos o no).
- Escaneos anómalos de red o puertos.
- Etc.

Con este tipo de ocurrencias, se está ante indicios de algo que puede guardar relación con incidentes de seguridad. En principio sobre un procedimiento de gestión de Supervisión / monitorización, podemos indagar acerca de si están o no tipificados estos casos, ¿Existen evidencias de este tipo de anomalías?, en segundo lugar deberíamos analizar si Existe un procedimiento ante estos casos específicos.

Más consideraciones que deben ser tenidas en cuenta para este procedimiento son:

- Situación de los centros de supervisión de red.
- Que se generen los "Registros de auditoría y monitorización".

Se deberían registrar todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias o fallos observables en un sistema de información o red de comunicaciones que puedan estar relacionados con la confidencialidad, integridad o disponibilidad de la información. Especialmente se registrarán la actividad de los administradores y operadores de los sistemas de información.

En cuanto a la supervisión:

a. ¿Se registra especialmente la actividad de los administradores y operadores de los sistemas de información?

b. ¿Se realiza algún tipo de análisis para determinar la profundidad o cantidad de eventos a registrar en un sistema de información o red de comunicaciones?

c. En cualquier caso, ¿se supervisan y monitorizan adecuadamente los eventos de seguridad que se detallan a continuación?:

   - los eventos requeridos por la legislación aplicable.
   - los intentos de autenticación fallidos.
   - los accesos de los usuarios a los dispositivos, tanto autorizados como los intentos no autorizados.
   - los eventos de operación y administración de los sistemas: el uso de cuentas privilegiadas de administración (root, admin, etc.), el uso de programas y utilidades de administración, la parada y arranque de los sistemas, la instalación o desinstalación de dispositivos de almacenamiento o de entrada/salida, etc.
   - los cambios en los parámetros de configuración de los sistemas.
   - los errores de funcionamiento de los sistemas y las redes.
   - los accesos a redes de comunicaciones, tanto autorizados como los intentos no autorizados: acceso remoto a la red interna (por Ras, ADSL, red privada virtual, etc.), accesos a Internet, etc.
   - el tráfico no permitido o rechazado por los cortafuegos y los dispositivos de encaminamiento (al menos de los protocolos más comunes y/o peligrosos).
   - las alertas generadas por los dispositivos de detección/prevención de intrusos (IDS/IPS).
   - los cambios en los privilegios de acceso: alta, baja y modificación de usuarios, cambios en los perfiles, etc.

- los cambios en los sistemas de seguridad, como la activación/desactivación o cambios en la configuración de los antivirus, de los sistemas de control de acceso, etc.
- el acceso al código fuente de los sistemas desarrollados.
- la activación/desactivación o cambios en la configuración de los mecanismos que generan los registros de auditoría.
- las modificaciones o borrado de los ficheros con registros de auditoría.
- el acceso a datos de carácter personal sensibles.

El procedimiento debe establecer claramente que infraestructuras, plataformas, dispositivos, redes y sistemas serán monitorizados y de qué forma se elaborarán y revisarán informes periódicos con los resultados de la monitorización. La periodicidad en la generación y revisión de cada informe estará determinada por el análisis de riesgos del elemento al que aplica.

6.2.8. Gestión de Logs.

El concepto de Logs, muchas veces se relaciona o se denomina como "**Registro de Auditoría**", lo cual sin entrar en debates sobre si es correcto o no, puede resultarnos interesante pues en definitiva un Log es un tipo de registro que se genera desde un dispositivo para dejar constancia de un evento. Un Log (o registro) para un sistema Unix, que fue el punto de partida de estos temas, es de un tipo u otro dependiendo de la aplicación de la que provenga (facilities) y del nivel de "gravedad" del evento que ha logueado (priorities). Una vez presentado el tema, nos centraremos únicamente en el procedimiento de "gestión de Logs".

Una de las acciones sobre las que más interés hemos puesto en los últimos años es justamente la implantación de plataformas de centralización de Logs. Hoy en día debemos referirnos a estas como **SIEM**: Security Information and Event Management.

En realidad, el concepto de SIEM viene de una combinación de dos soluciones (o definiciones) anteriores:

- **SIM**: Security Information Management
- **SEM**: Security Event Management

Al unir ambas ideas aparece, tal vez más robusta, la posibilidad de "correlar" (o correlacionar) eventos de seguridad. Hoy en día estas implementaciones son de uso frecuente, y existen varios proveedores, algunos de ellos son:

- ArcSight de HP
- RSA Security Analytics
- Splunk (Puede discutirse si es o no un SIEM…)

Nuestra experiencia sobre los SIEM y el proceso de Gestión de Logs es que se debe considerar dos aspectos básicos:

a. El nivel de implantación y explotación alcanzado de Logs.
b. El nivel de seguridad en la gestión de la plataforma de centralización y/o correlación.

6.3. *Tareas para el hogar (deberes).*

Una vez más en este capítulo os propongo llevarnos algunas actividades o líneas de reflexión para que comencemos el próximo con más "expertiz".

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cómo está nuestro nivel de procedimientos de seguridad?
2. ¿Se están aplicando adecuadamente?
3. El nivel de cada uno de ellos ¿es el adecuado? (*es decir aplica al área, función o persona idónea para su cumplimiento*).

4. ¿Sobre cuál de ellos debo incrementar la atención?
5. ¿Creo necesario incluir alguno más?, ¿Cuál?
6. ¿Qué tipo de herramientas o aplicaciones puedo emplear para dar cumplimiento a estos procedimientos?

7. Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red

Resumen del tema

Hasta ahora hemos venido desarrollando conceptos, definiciones, y procesos. En este capítulo presentamos una serie de despliegues que son de utilidad en el trabajo de Ciberseguridad de nuestras redes. Muchos de estos despliegues pueden ser considerados como plataformas, infraestructuras, appliances, desarrollos de software e inclusive como un conjunto de medidas de seguridad. Nuestra intención de presentarlas en este capítulo es que una vez que ya hemos comprendido los niveles más importantes de una red (Enlace, red y transporte) ahora podamos aplicar diferentes productos u ofertas del mercado para ampliar nuestro trabajo de Ciberseguridad, por esa razón es que los hemos incluido en este texto.

Aunque es cierto que algunos de ellos no respondan estrictamente al título de "Plataforma" o "Infraestructura", presentaremos lo siguiente:

- Control y filtrado de accesos.
- Firewalls.
- ACLs en routers.
- Supervisión / Monitorización / Alarmas.
- Centralización y explotación de Logs.
- Detección / Prevención / Mitigación.
- IDSs/IPSs (Sistemas de Detección / Prevención de intrusiones).
- Plataformas de mitigación/detección.

- Infraestructuras para la resolución de nombres.
- Balanceo de carga.
- Plataformas de sincronización de tiempo.
- Plataformas de Control de Accesos
- Herramientas de gestión de Routers.
- Herramientas de gestión de Firewalls.
- Empleo de máquinas de salto.

7.1. Planteo inicial

Dentro del universo de plataformas e infraestructuras de seguridad, que sería infinito de resumir en estas páginas, en textos anteriores y también en Internet hay varios de estos temas que son bastante conocidos o que podemos encontrar información en abundancia.

En los aspectos de Filtrado (*Firewalls y ACLs en routers*), sabemos bien que lo importante es tener un buen conocimiento de nuestras redes y hosts, en particular sobre sus sistemas operativos (y actualizaciones), su direccionamiento IP y los puertos que nos dan acceso a las aplicaciones.

Si partimos de esta base, es relativamente sencillo abrir o cerrar las reglas necesarias para permitir o negar el ingreso o salida de cada uno de ellos.

No merece la pena detenernos en esta función.

Si hablamos de:

- Gestión y Supervisión

  - Supervisión / Monitorización / Alarmas.
  - Infraestructuras para la resolución de nombres.

- Balanceo de carga.
- Plataformas de sincronización de tiempo.
- Herramientas de gestión de Routers.
- Herramientas de gestión de Firewalls.

Podríamos presentar varios fabricantes de estos productos, sistemas de ticketing, de **OSS** (*Operations Support System*), **BSS** (*Business Support System*), metodologías de empleo del protocolo **NTP** (*Network Time Protocol*) y también qué parámetros nos sirven para determinar cómo puedo repartir el tráfico para que el servicio sea más eficiente.

Otro componente de este rubro que hemos querido destacar es la **resolución de nombres, que en todo Internet se sustenta con el protocolo DNS** (*Domain Name System*), desde el punto de vista de seguridad siempre nos ha traído dolores de cabeza. La realidad es que la masa de los productos comerciales se basan en nuestro viejo y querido **BIND** (*Berkeley Internet Name Domain*) de Unix, que sabiéndolo operar adecuadamente es inmejorable.

Pero como tenemos un par de puntos sobre los que deseamos centrar la atención en estos pocos minutos, también dejaremos de lado estas infraestructuras.

7.2. Unos breves minutos

Sólo nos detendremos unos minutos a tratar el tema de:

- Detección / Prevención / Mitigación.
  - IDSs/IPSs (Sistemas de Detección / Prevención de intrusiones).
  - Plataformas AntiDDoS.

Pues creemos necesario hacer hincapié únicamente en un par de ideas fuerza:

- **IDSs/IPSs** (Sistemas de Detección / Prevención de intrusiones).

  Como punto de partida: "Cuidado" con las medidas de prevención de intrusiones.

  Los IDSs, llevan años en producción. A principios de este milenio, tuve la suerte de poder hacer un trabajo de evaluación de estas nacientes tecnologías. El resultado fue un artículo muy conocido "**Nivel de inmadurez de los NIDS**". En este trabajo, se montó un laboratorio con los cuatro mayores fabricantes de IDS a nivel mundial, generamos todo tipo de tráfico, y lo llamativo de sus resultados fue que cada uno de ellos respondía de forma diferente; algunos detectaban ciertos patrones y protocolos, otros no, los umbrales eran muy diferentes y los falsos positivos y negativos aparecían más que los datos ciertos.

  Hoy, quince años después, el panorama no ha cambiado mucho si intentamos emplear estas herramientas sin un adecuado ajuste o personalización y actualización constante. Los IDSs siguen siendo herramientas que necesitan mucho trabajo y recursos dedicados. Los considero **fundamentales** e **imprescindibles** en toda gran infraestructura de red, pero "**sí, y solo sí**" le dedicamos los recursos suficientes, sino no merece la pena gastar tiempo ni dinero, pues no sirven para nada.

  Es decir, en primer lugar, los IDSs son buenísimos si los tomamos en serio (*es decir con dedicación*), por lo tanto, si pensamos en "prevenir" intrusiones el tiempo de personalización es aún mayor, sino estaremos gastando del doble de tiempo y dinero y, a su vez, incrementando el riesgo de nuestra empresa, pues como siempre me gusta afirmar, por mi parte "apuesto por el humano". Es el ejemplo que pongo siempre del prisionero que mira a su cárcel

durante horas, días, meses, años… hasta que encuentra la vía de escape, la cual, como no existe fortaleza invulnerable, tarde o temprano la hallará.

Con los IPSs es algo similar, si los millones de intrusos comienzan a analizar las respuestas de nuestras redes a sus actividades, poco a poco podrán ver de qué forma "automática" se cierran puertos, conexiones, accesos, etc… y a través de los mismos, ya hemos conocido grandes ataques de negación de servicio que han logrado aislar redes en virtud de la reacción de los IPSs.

Para cerrar este tema, no dejo de insistir en que tenemos a nuestro alcance una herramienta fabulosa como es "**Snort**" (https://www.snort.org) que invito a que la instaléis y pongáis a prueba, seguramente nos enseñará muchísimo y si la ponemos en producción (*y le dedicamos los recursos suficientes*) tendremos un pilar fundamental para nuestra seguridad.

- Plataformas **AntiDDoS**.

Para esta plataforma pondremos por ejemplo la que ofrece **Arbor Networks** y el paquete comprende dos herramientas diferentes:

- **Peakflow**
- **TMS**: Threat Management System

Algunas empresas, sólo poseen PeakFlow como una herramienta de supervisión y monitorización de tráfico, es cierto que desde la misma manualmente se pueden configurar medidas para minimizar ciertos patrones de tráfico, pero el concepto de "Mitigación" efectivo pasa por medio de TMS. Su lógica la podemos describir mejor a través de las imágenes que presentaremos más abajo.

Para entender bien el concepto, debemos considerar que un ataque bien lanzado de DDoS, en general, busca dejar inactivo un servicio concreto, por ejemplo, una página Web, un servidor de correo, una aplicación, etc. Por lo tanto, si se bloquea todo el tráfico hacia el mismo, lo que estamos logrando es exactamente el ejemplo que

acabamos de presentar con los IPSs. Alguien que se dedique a analizar en qué momento se bloquea este tráfico, puede lograr dejar fuera de servicio intencionadamente al mismo. Por lo tanto, no es una medida eficiente el bloqueo de todo el tráfico. Tampoco es sencillo lograr la "granularidad" suficiente como para que en "tiempo real" podamos analizar "en línea" la totalidad del tráfico que pasa por un gran router. Hemos remarcado con comillas estas tres palabras, pues estamos hablando de un tráfico de varios cientos de gigas o hasta tera bits por segundo, este inmenso caudal no es sencillo de procesar, de hecho es uno de los grandes problemas de colocar Firewalls en las interfaces de acceso a Internet por parte de los **ISP** (Internet Service Provider) pues al día de hoy, siguen sin existir FWs en capacidad de desarmar este altísimo volumen de tramas y procesarlas, sin causar una baja de rendimiento considerable.

Para dar solución seria a este problema el protocolo BGP introdujo el concepto de "**BGP flow spec**", que, si bien no desarrollaremos en estas líneas, al menos presentaremos algunas breves ideas.

La BGP flow Spec es una nueva herramienta que puede utilizarse para ayudar en la mitigación de DDOS de una manera dinámica, aprovechando BGP, permitiendo una mayor granularidad para construir instrucciones de ruteo que coincidan con un flujo particular considerando: origen, destino y parámetros de nivel cuatro, como así también especificaciones de paquetes como longitud, fragmento, etc.

A través del empleo de BGP Flow Spec se pueden definir acciones concretas en los rotuers de frontera para:

- Descartar el tráfico
- Inyectarlo en un **vrf** (virtual routing forwarding) diferente para su análisis.
- Permitirlo, pero de acuerdo a una política o tasa de tráfico definida y específica.

Para resumirlo y comprender estos conceptos, presentamos a continuación tres imágenes, que como bien se sabe, valdrán más

que miles de palabras:

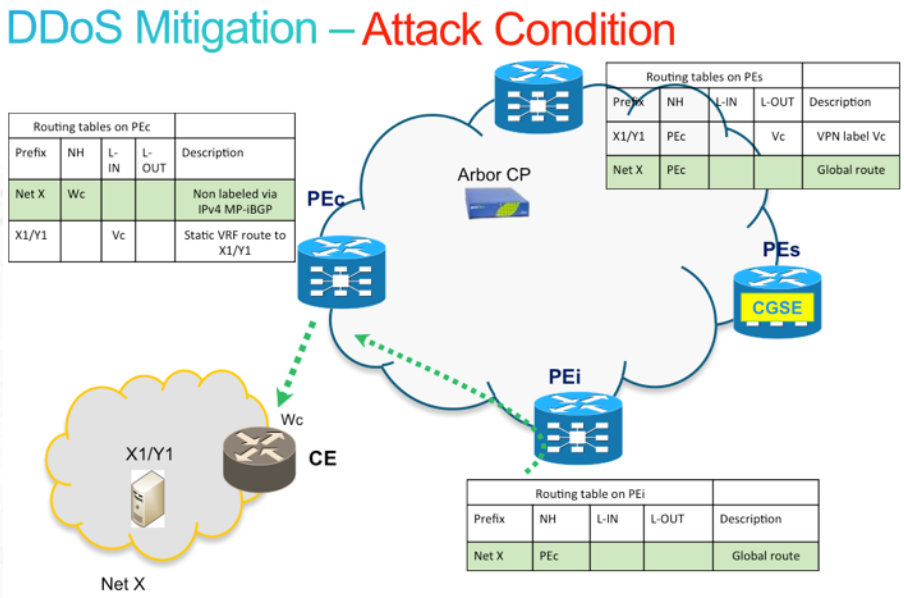


Imagen 1 (tráfico normal – tablas de rutas BGP iniciales)

* **CGSE**:Cisco Carrier Grade Services Engine

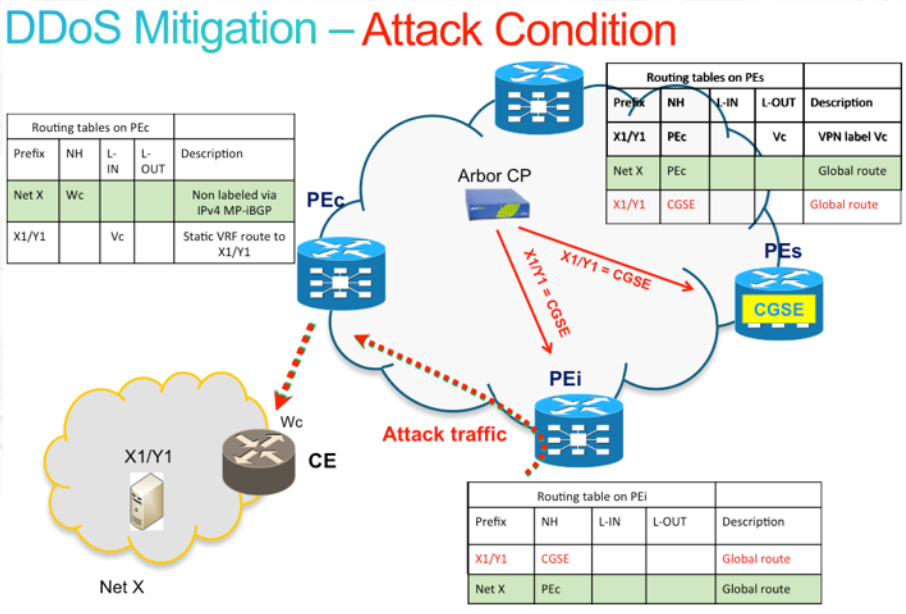


Imagen 2 (ataque – inserción de nuevas rutas BGP)

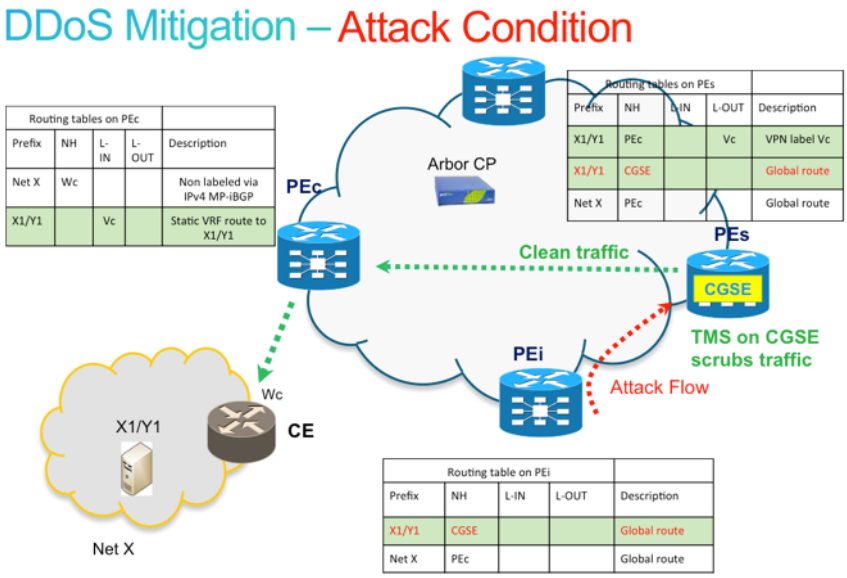


*Imagen 3 (cambio rutas BGP sólo para **X1/Y1** – flujo limpio)*

Hemos intentado resumir este importante concepto en tres imágenes que representan una metodología que creemos, a día de hoy, es la más importante que se puede implementar para hacer frente a ataques de DDoS. Existen otro tipo de soluciones, pero a nuestro juicio, el empleo de Flow Spec, es tal vez la única que permite hacer frente a este problema en gran escala, sin causar afección al resto de los servicios (ni siquiera al atacado), pero desde diferentes direcciones y patrones que los del origen del ataque.

Invitamos a que profundicéis más sobre este tema, pues es uno de los más grandes que se están presentando a nivel ciberseguridad.

7.3. Tema base de hoy

Habiendo desarrollado brevemente los conceptos anteriores, queremos centrarnos un poco más en los temas que siguen, para hacer referencia a algunos estándares y normas que seguramente nos serán de interés en el día de hoy.

Los temas que nos quedan son los siguientes:

- Autenticación y control de Accesos
  - Plataformas de Autenticación
  - Plataformas de Control de Accesos
  - Empleo de máquinas de salto.
  - Centralización y explotación de Logs.
- Virtualización
  - host
  - redes

Teniendo en cuenta que la "movilidad" hoy en día es uno de los aspectos clave de las infraestructuras de red, se hace necesario poder acceder a nuestros servicios y aplicativos desde diferentes ubicaciones y zonas geográficas. Para poder ofrecer esta posibilidad sin dejar de lado la seguridad que nos ofrecen nuestras LANs (Local Área Networks)

En referencia a los mismos, a continuación, vamos a presentar, en primer lugar, los tipos de VPNs:

a. VPNs Basadas en **SSL**
b. VPNs basadas en **IPSec**
c. VPNs basadas en **SSH**

Si los analizamos como modelo de capas TCP/IP, los podemos representar de la siguiente forma:

5	HTTPS (TCP-443)	SMTPS (TCP-465)	LDAPS (TCP-646)	IMAPS (TCP-993)	POP3S (TCP-995)	FTPS (TCP-989 y 990)	...
4	TCP (SSL o TLS)						
3	IP						
2	Enlace *(802.3, 802.11, 802.16, 3GPP,...)*						
1	Físico *(F.O., UTP, Radio enlace, telefonía móvil,...)*						

VPNs Basadas en SSL

5	Cualquier aplicación sobre TCP	...
4	TCP	
3	IPSec	
2	Enlace *(802.3, 802.11, 802.16, 3GPP,...)*	
1	Físico *(F.O., UTP, Radio enlace, telefonía móvil,...)*	

VPNs basadas en IPSec

5	Cualquier aplicación sobre TCP	...
4	SSH (port TCP 22)	
3	IP	
2	Enlace *(802.3, 802.11, 802.16, 3GPP,...)*	
1	Físico *(F.O., UTP, Radio enlace, telefonía móvil,...)*	

VPNs basadas en SSH

a. VPNs Basadas en **SSL** (Secure Sockets Layer)

El protocolo SSL nace como propietario de la empresa Netsacpe y luego se estandariza como **TLS** (Transport Layer Security) que se identifica como SSL v3.1, aunque entre ambos tienen algunas diferencias):

Las características de cualquiera de ellos son:

- Protege una sesión entre cliente y servidor.
- Requiere protocolo de transporte orientado a la conexión (típicamente TCP)
- Autenticación
  - del servidor hacia el cliente
  - opcionalmente, del cliente hacia el servidor. (mediante certificados)

Una comunicación a través de SSL implica tres fases:

- Establecimiento de la conexión y negociación de los algoritmos criptográficos que van a usarse en la comunicación.
- Intercambio de claves.
- Cifrado simétrico del tráfico.

Una opción para poner a prueba esta metodología es **OpenVPN**, que presenta las siguientes características:

- Busca implementar VPNs de forma más sencilla que IPSEC.
- No requiere de la complejidad del protocolo **IKE** (Internet Key Exchange).
- Puede trabajar en modo bridging o en modo routing.
- Utiliza la implementación de **openssl**.
- *www.openvpn.net* (Ver también: *www.openssl.org*)

NOTA: Una recomendación adicional es hacer todas las pruebas que estén a nuestro alcance con **OpenSSL** (generar claves, firmarlas, generar certificados, instalar una Autoridad de certificación, una de revocación, probar el cifrado con certificados, generar conexiones SSH con el empleo de certificados, emplear los certificados para firma electrónica, etc.)

b. VPNs basadas en **IPSec**

Sobre el protocolo IPSec no entraremos en mayores detalles pues lo hemos desarrollado al completo en el libro "Seguridad por Niveles", sólo mencionamos a continuación los requerimientos que hacen falta para implementar estas VPNs:

Se basan en el empleo de los protocolos: AH (Authentication Header), ESP (Encapsulation Security Payload) e IKE (Internet Key Exchange).

Para el empleo de **IKE** puede hacerse por medio de:

- Preshared-keys
- Pares de claves (firma digital)
- Certificados Digitales.

AH: ofrece verificación de la fuente, integridad de paquetes y anti-replay, **ESP** ofrece Confidencialidad.

c. VPNs basadas en **SSH** (Secure SHell)

Esta tecnología se basa en empleo de túneles SSH y la redirección de puertos (Port forwarding) que ofrece este protocolo. Este protocolo es nativo en todos los sistemas Unix/Linux, por lo que no requiere ningún tipo de configuración previa y recursos adicionales. Con ProxySocks se pueden emplear túneles dinámicos que nos permiten acceder a diferentes direcciones IP.

Para profundizar en estos túneles, puede verse el Webinar "**SSH Forwarding**" en la siguiente URL:

https://www.youtube.com/watch?v=dYK1blKK3xc&t=82s

También pueden consultarse una serie de ejercicios que están en el punto 9.3. del libro "**Seguridad en Redes**".

El empleo de este tipo de VPNs es de suma utilidad en la implantación de "máquinas de salto", pues es una solución muy sencilla y práctica y eficiente de crear accesos seguros a redes o segmentos de red sobre los que se desea tener un control más estricto.

Por último, debemos mencionar que dentro de nuestras propias LANs, también podemos virtualizar redes. Esto ya lo hemos comentado en charlas previas, pero sobre la base de la familia de protocolos IEEE-802.x, existe uno en particular que es 802.1Q, que justamente introduce el concepto de VLAN (Virtual LAN) y que lo podemos emplear para diferenciar el tráfico de las áreas de nuestra LAN, creando para cada una de ellas su propia VLAN. Esta configuración se realiza en cada uno de los switchs y en grandes líneas lo que se realiza es un encabezado adicional en el campo "Ethertype" del protocolo Ethernet que, cuando contiene el valor **81-00** identifica que se trata de una VLAN específica y en ese nuevo encabezado se incluye toda la información de la misma.

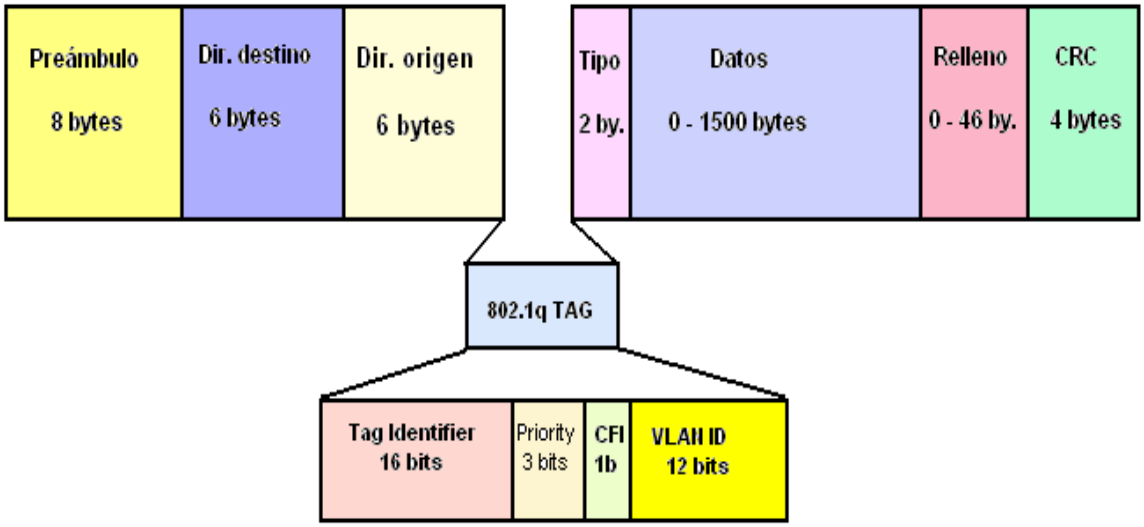


Imagen 4 (Formato de una trama 802.1q)

Todo el detalle sobre este protocolo, podemos encontrarlo en el punto 4.2.3. 802.1Q (Virtual LAN), del libro "**Seguridad en Redes**".

Un punto adicional que dejo como tarea de estudio (y merece la pena comenzar a evaluar) es el protocolo **802.1ae** Media Access Control (MAC) Security, publicado en 2006 y cuya última enmienda es del 2013: **802.1AEbw**)

Conocido como **MACSec** ofrece confidencialidad, integridad y autenticación de origen. Introduce nuevos campos a la trama Ethernet (SecTag, ICV)

Asociaciones seguras de conectividad (grupos de estaciones conectadas por medio de canales seguros con su propia llave SAK).

Al igual que 802.1Q, en este protocolo también se agrega un nuevo encabezado a la trama Ethernet, cuando el campo Ethertype posee el valor Ethertype: **88-E5**. A continuación, presentamos la imagen que ofrece en el contenido de la norma:

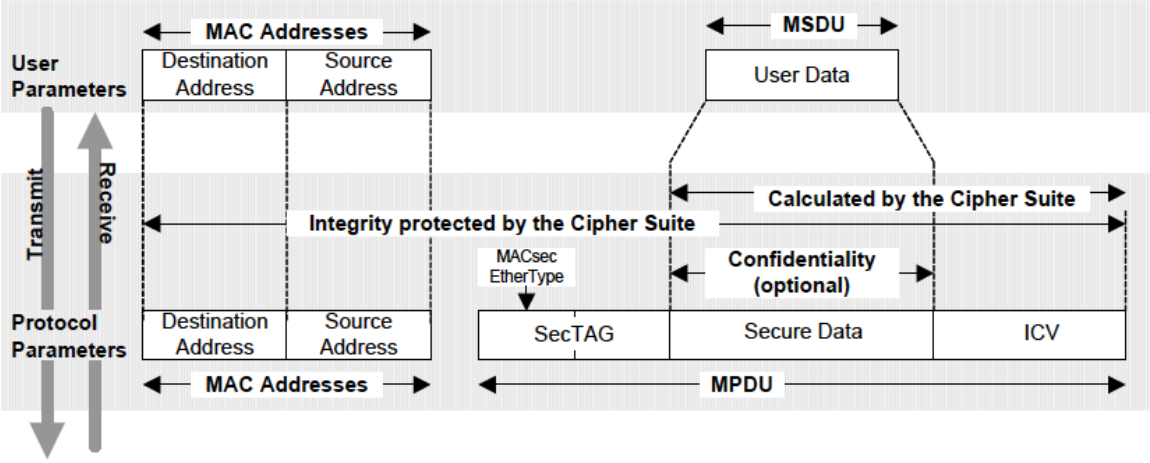


Figure 8-1—MACsec

Imagen 5 (Formato de una trama 802.1ae)

Toda esta información adicional es de suma importancia, ahora que ya estamos comenzando a comprender el tema de Ciberseguridad en su conjunto, pues a medida que vamos incrementando las medidas es cuando nuestras infraestructuras se hacen más sólidas. Por ello como reflexión final, presentamos la secuencia, que en este caso ofrece Cisco, en el que podemos ver cómo se van integrando los diferentes protocolos de capa dos (enlace) para ofrecer un paquete robusto de autenticación y control de acceso basado en esta serie de protocolos de la familia IEEE-802.x que venimos desarrollando desde hace tiempo en nuestros textos.

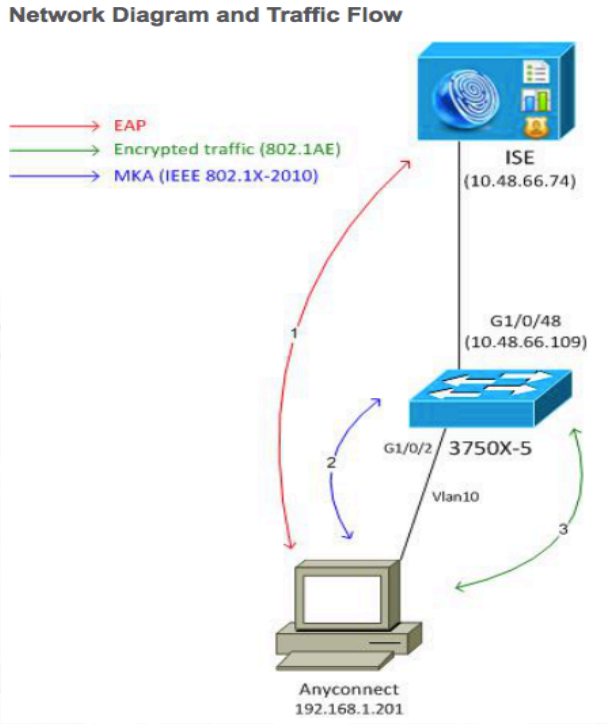


Imagen 6 (Combinación de 802.1x con 802.1ae)

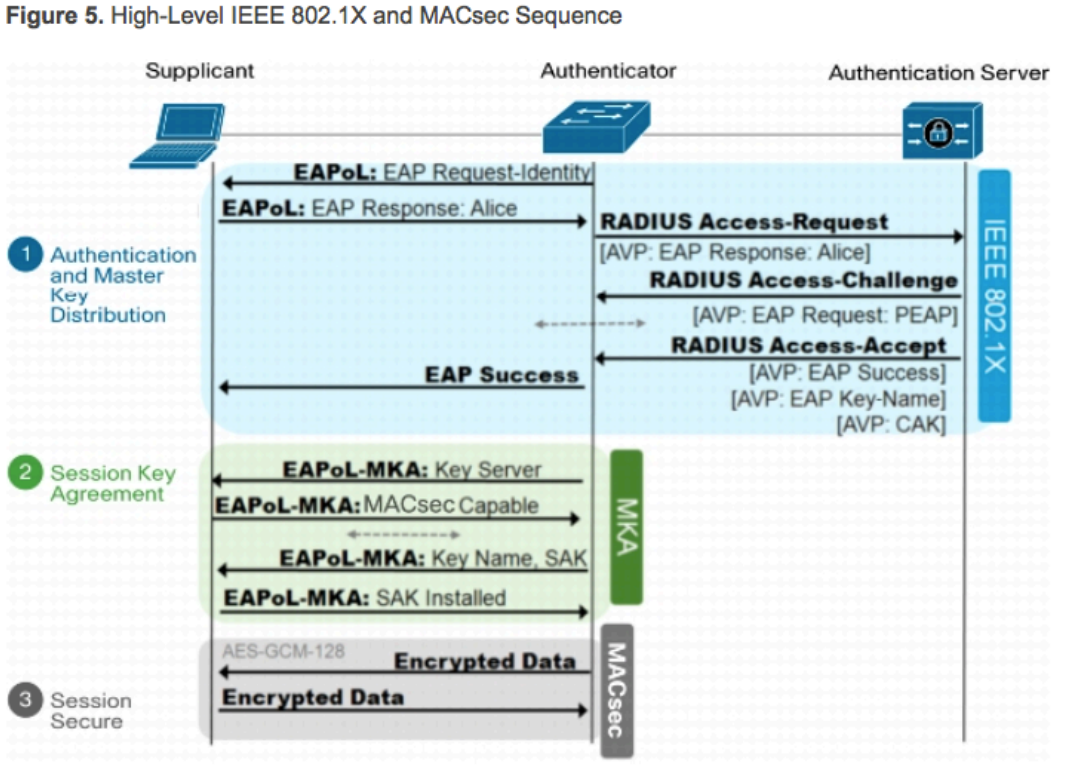


Imagen 7 (Secuencia de 802.1x con 802.1ae)

Ambas figuras están tomadas de:

http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/identity-based-networking-services/deploy_guide_c17-663760.html

7.4. Tareas para el hogar (deberes).

Una vez más os propongo llevarnos a casa algunas actividades o líneas de reflexión para que comencemos el siguiente capítulo con más "expertiz".

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Profundicé con SNORT?, ¿Como funciona su motor?, ¿pude implementas local rules?
2. ¿Necesito implantar sistemas AntiDDoS?
3. ¿Hice pruebas de IPS con respuestas automáticas?
4. Realizar pruebas de túneles SSH y el empleo de redirección de puertos.
5. ¿Pude instalar una máquina de salto?
6. ¿Qué opinión me merece el empleo de IEEE-802.1ae?

8. Ciberseguridad: Cómo son las entrañas de esta gran red mundial

Resumen del tema

En este capítulo, no dedicaremos tiempo a historia de Internet o aspectos conocidos de su evolución, sino a la descripción técnica que nos hace posible hoy en día poder transmitir información por todo el mundo.

Conocemos los diferentes tipos de acceso e infraestructuras básicas que nos permiten conectarnos a la red e inclusive parte de estas zonas, plataformas e infraestructuras que poseen las operadoras nacionales que en definitiva son las que llegan a través de la red fija o móvil hasta cada uno de nosotros, clientes finales. Avancemos ahora más en profundidad sobre los detalles de estas conexiones.

Si comenzamos a analizar esta red de forma jerárquica desde arriba hacia abajo, lo primero que nos encontramos son los grandes "**Carriers**" del mundo, es decir los que interconectan continentes y países de forma bastante piramidal. Existen tres niveles de ellos, conocidos como Tier 1, Tier 2 y Tier 3.

Esta parte profundizará sobre el funcionamiento de estos niveles superiores de Internet que son los que transportan los grandes volúmenes de datos y su ancho de banda son inimaginables. El conocimiento de sus entrañas es lo que posiciona a cualquier atacante en un nivel superior en cuanto a volúmenes de tráfico y conectividad de extremo a extremo, por lo tanto, si lo que deseamos desde el punto de vista de "ciberdefensa" es poder adoptar medidas contra estas acciones delictivas, necesitamos también conocer en detalle el fondo de esta red.

8.1. Planteo inicial

En el día de hoy desarrollaremos cuatro conceptos básicos sobre el corazón de nuestras redes:

- **Tubos**
- **Carriers**
- **Protocolo BGP**
- **Sistema DNS**

Por supuesto que para que todo Internet funcione, existen miles de conceptos, infraestructuras, protocolos, regulaciones, empresas, organizaciones, etc. Que también participan en el día a día de esta red, pero para concentrar la charla de hoy en aspectos fundamentales del tema lo haremos específicamente en estos tres que acabamos de presentar.

8.2. Tubos

El periodista de tecnología **Andrew Blum** acaba de publicar un libro que intenta comprender la realidad física de Internet. "**Tubos, un viaje hacía el centro de Internet**"

El título del libro de Blum se refiere a un comentario de un senador estadounidense, llamado **Ted Stevens**. Hablando en el Senado el 28 de abril del 2006 respecto a una legislación sobre el negocio de proveedores de Internet, Stevens dijo, "Internet no es algo que simplemente montas sobre otra cosa. No es un camión. Es una serie de tubos." Este comentario fue motivo de críticas y risas en su momento.

Comenta Blum:

"He confirmado, con mis propios ojos, que Internet es muchas cosas en muchos lugares. Pero una cosa que sí es, en todos los lugares donde existe, es una serie de tubos. Hay tubos debajo del mar que conectan Londres con Nueva York. Tubos que conectan Google con Facebook. Hay edificios llenos de tubos, y cientos de miles de caminos y vías de trenes que tienen tubos corriendo a sus lados. Todo lo que haces en línea viaja dentro de un tubo. Dentro de esos tubos, en general, hay fibras de vidrio. Y dentro de esas fibras, luz. Y, codificado dentro de esa luz, estamos –cada vez más– nosotros."

"Una de las cosas que me gustó mucho de los administradores de grandes redes sobre los que escribí es que son diferentes de los típicos técnicos de soporte informático. En parte es porque hay una cierta diplomacia necesaria en lo que hacen. No sólo tienen que administrar su propio sistema, sino que también tienen que conectar sus redes a otras redes. Entonces siempre están negociando entre ellos; siempre tienen que tener en cuenta las necesidades de las otras redes además de las de ellos mismos. Eso los lleva a ser muy empáticos.

La segunda cosa que me llamó la atención es que ellos tienen una imaginación bien geográfica y específica. Tienen que tener en cuenta cómo está conectado el mundo real para poder armar redes eficientes".

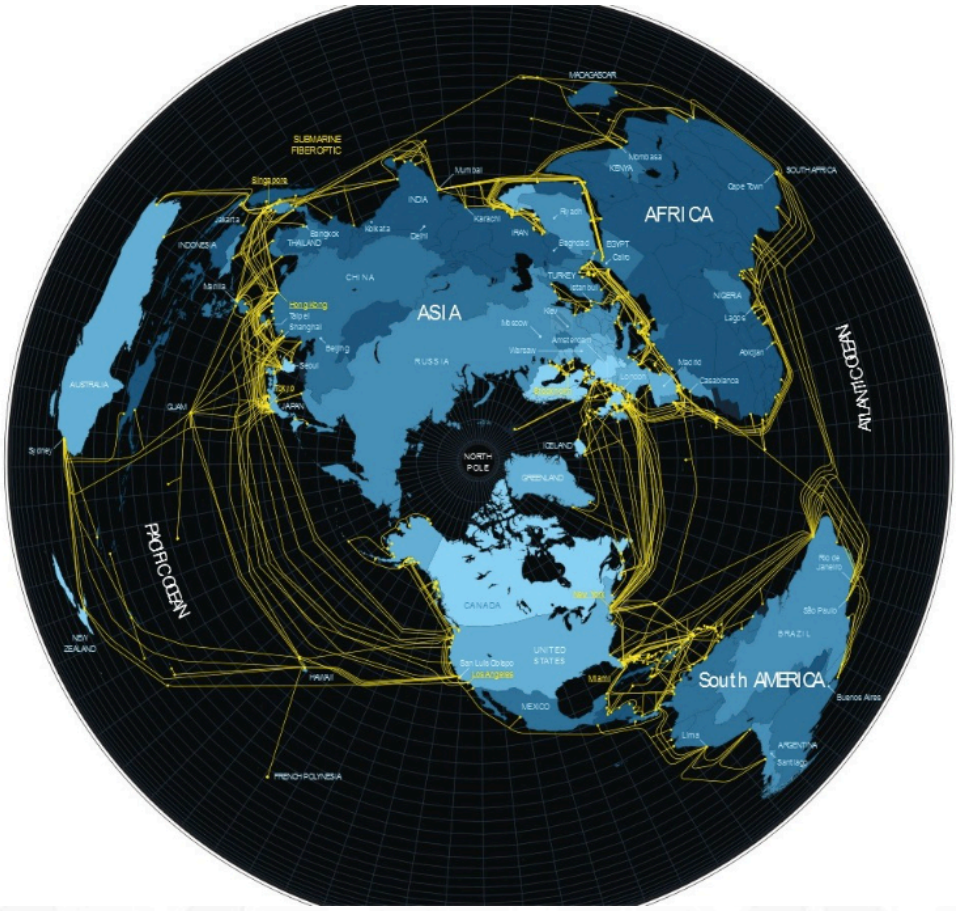


Imagen 8 tomada de: https://norfipc.com/infografia/mapa-mundial-redes-conexion-internet.html

Estos tubos interconectan a nivel físico todos los extremos del planeta, estos "tubos" para establecer las conexiones podemos clasificarlos en tres categorías:

- Fibras ópticas.
- Cables de cobre
- Enlaces de radio

Esto es concretamente lo que denominamos "Medio físico" y es el nivel inferior de nuestro modelo de capas. Los extremos de cada uno de estos medios físicos, se conectan a dispositivos.

Estos dispositivos básicamente los podemos clasificar en dos categorías:

- Conmutadores o Switchs: operan a nivel 2 (enlace) del modelo de capas.
- Routers: operan a nivel 3 (red) del modelo de capas.

Los "tubos" llegan a una boca física de un router o switch, se conectan al mismo y a partir de allí ingresan o parten los "paquetes" de datos encapsulados en el protocolo que corresponda.

Como cualquier sistema de entrega y recepción, es necesario basarse en algún tipo de "Direccionamiento", el cual para el caso de Internet es el protocolo IP, en la actualidad sigue siendo la versión 4 del mismo, pero ya se está implantando la nueva versión 6, que está instalada y funcionando en gran parte de esta arquitectura mundial, si bien no podemos pensarla como que está en "producción" aún.

Todo este esquema de direccionamiento IP se encuentra asignado y regulado a lo largo de nuestro planeta por **IANA** (Internet Assigned Numbers Authority).

REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

(*Imagen 9 tomada de* *http://iana.org*)

IANA tiene delegado sus rangos de asignación IP por regiones geográficas, tal cual podemos ver en la imagen anterior. Estas regiones son denominadas **RIR** (Regional Internet Registry).

Otra de las responsabilidades de asignación de IANA es la que respecta a los Sistemas Autónomos (**AS**: Autonomous Systems), los cuáles se tratan de conjuntos de redes IP y routers que se encuentran bajo el control de una misma entidad (en ocasiones varias) y que poseen una política de encaminamiento similar a Internet.

El concepto de Sistema Autónomo es fundamental para el control de Internet, pues los grandes routers de esta red, sólo conocen de AS.

Este tema es el que presentamos en los puntos siguientes.

8.3. Carriers

Los grandes puntos de interconexión que tratamos en los párrafos anteriores, son gobernados por lo que podemos llamar "**Carriers**". Se trata de grandes corporaciones, que unen el corazón de esta gran red.

Si comenzamos a analizar esta red de forma jerárquica desde arriba hacia abajo, lo primero que nos encontramos son los grandes "Carriers" del mundo, es decir los que interconectan continentes y países de forma bastante piramidal. Existen tres niveles de ellos, conocidos como Tier 1, Tier 2 y Tier 3.

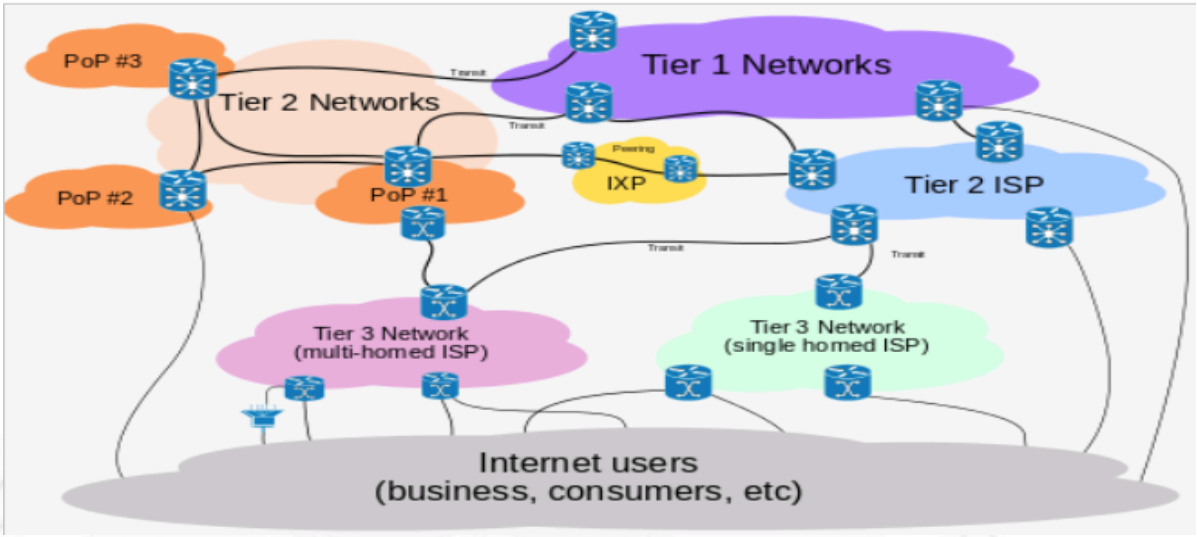


Imagen10 (Tiers de Internet) (Imagen tomada de Wikipedia)

Los **Tier 1** son los grandes operadores globales que tienen tendidos de fibra óptica al menos a nivel continental. Desde la red de un Tier 1 se accede a cualquier punto de Internet, pues todas las redes de Tier 1 deben estar conectadas entre sí. Son backbone, core, núcleo ó troncal de Internet. Si bien se puede llegar a discutir la frontera entre algún Tier 1 específico, los que podemos considerar sin lugar a dudas como Tier 1 son:

Nombre	Sede	Nº as (asN)
Cogent anteriormente PSINet	Estados Unidos	174
Level 3 Communications (Ex Level 3 y Global Crossing)	Estados Unidos	3356 / 3549 / 1
XO Communications	Estados Unidos	2828
AT&T	Estados Unidos	7018
Verizon Business (anteriormente UUnet)	Estados Unidos	701 / 702 / 703
CenturyLink (anteriormente Qwest and Savvis)	Estados Unidos	209 / 3561
Sprint	Estados unidos	1239
Zayo Group anteriormente AboveNet	Estados Unidos	6461
GTT (anteriormente Tinet)	Estados Unidos	3257
NTT Communications (anteriormente Verio)	Japón	2914
Teliasonera International Carrier	Suecia - Finlandia	1299
Tata Communications (adquirió Teleglobe)	India	6453
Deutsche Telekom (Hoy: International Carrier Sales & Solutions)	Alemania	3320
Seabone (Telecom Italia Sparkle)	Italia	6762
Telefónica	España	12956

Independientemente de su magnitud, también deben reunir algunas características como son:

- Deben tener acceso a las tablas completas de routing a través de las relaciones que poseen con sus **peering** (otros Tiers).
- Deben ser propietarios de fibras ópticas transoceánicas y enlaces internacionales.
- Deben poseer redundancia de rutas.

El dato más representativo y actualizado del peso y actividad de cada uno de ellos se puede obtener a través de **CAIDA** (Center for Applied Internet Data Analysis) en:

http://as-rank.caida.org

Un ejemplo cercano de Tier 1 lo tenemos con Telefónica, a través de su empresa **TIWS** (Telefónica International Whole Sales) o actualmente con su nuevo nombre TBS (Telefónica Bussiness Solutions), desde su página Web podemos apreciar el mapa que se presenta a continuación donde se presentan todos los vínculos físicos que controla este Tier 1.

Imagen 11 (Red Internacional del Grupo Telefónica) (Imagen tomada de la web: http://www.internationalservices.telefonica.com)

Las diferentes operadoras de telefonía e Internet de cada país, enrutan su tráfico de clientes hacia el resto del mundo a través de estos carriers. Para esta tarea tenemos básicamente dos escenarios:

- Interconexión con su "Carrier" (Salida Internacional): En este caso se trata de routers del ISP, que físicamente están conectados a routers de un "Tier 1 o Tier2" y entregan su tráfico para que ellos lo enruten a través de Internet. Este tipo de enlaces suelen ser redundantes y en general hacia al menos dos Carriers diferentes para garantizar su disponibilidad.

- Punto de Intercambio (**IXP**: Internet eXchange Point) o también denominado o Punto Neutro: Se debe considerar que el tráfico de Internet, tiene un alto porcentaje que se mantiene dentro de

las fronteras de cada país (consultas a Web nacionales, correos locales, etc..), este tipo de tráfico no tiene sentido que sea enrutado fuera de estas fronteras pues sobrecargaría las troncales de la red. Para estos casos en muchos países (no todos) se han creado estos IXP, que en definitiva son salas con "Racks" de comunicaciones (básicamente switchs de alta capacidad) donde se interconectan los grandes carriers de ese país. Al organizarse las rutas BGP, es natural que este tipo de enlaces ofrezcan mayor ancho de banda que si siguieran otros caminos, por lo tanto, a la hora de generarse las tablas de ruteo, el "peso" que tienen estos caminos supera cualquier otro, debido a ello se generan rutas locales preferenciales que encaminan el tráfico nacional, sin la necesidad de salir de ese país.

El propósito principal de un punto neutro es permitir que las redes se interconecten directamente, a través de la infraestructura, en lugar de hacerlo a través de una o más redes de terceros. Las ventajas de la interconexión directa son numerosas, pero las razones principales son el costo, la latencia y el ancho de banda.

El tráfico que pasa a través de la infraestructura no suele ser facturado por cualquiera de las partes, a diferencia del tráfico hacia el proveedor de conectividad de un Internet Service Provider (**ISP**).

La técnica y la logística de negocios de intercambio de tráfico entre los Internet Service Provider se rige por los acuerdos de interconexión mutua (**peering**). En virtud de dichos acuerdos, el tráfico a menudo se intercambia sin compensación. Cuando un punto neutro incurre en costos de operación, por lo general éstos son compartidos entre todos sus participantes.

8.4. Protocolo BGP

Siguiendo con la secuencia de estos párrafos, corresponde ahora tratar el tema de Sistemas Autónomos. Ampliando los conceptos anteriores, se define como "un grupo de redes IP que poseen una política de rutas

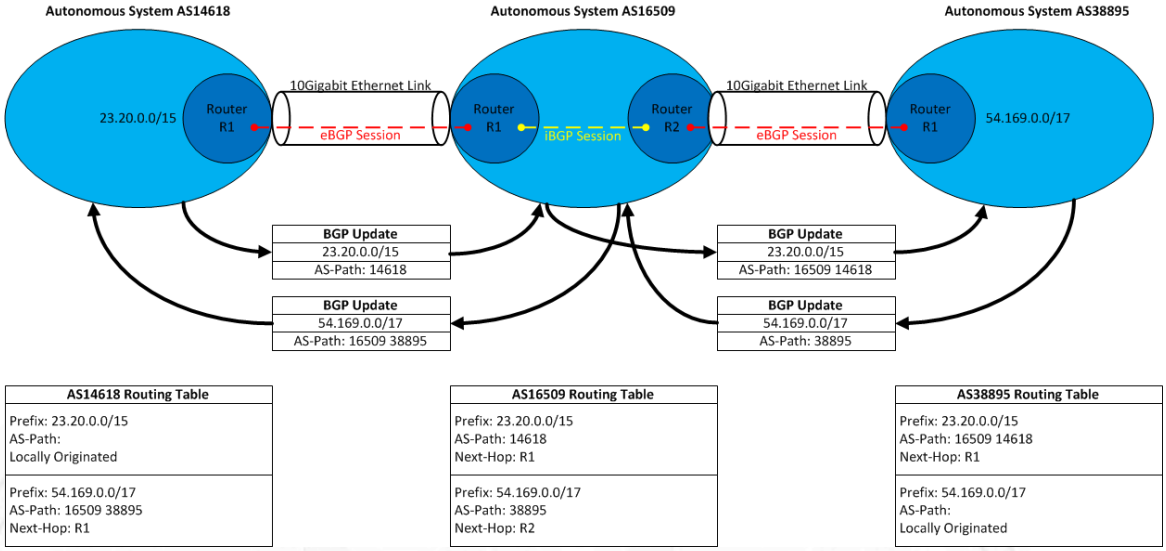
propia e independiente". Esta definición hace referencia a la característica fundamental de un Sistema Autónomo: realiza su propia gestión del tráfico que fluye entre él y los restantes Sistemas Autónomos que forman Internet. A cada uno de ellos, y es el que lo identifica de manera única a sus redes dentro de Internet.

Hasta el año 2007 los números de sistemas autónomos estaban definidos por un número entero de 16 bits lo que permitía un número máximo de 65536 asignaciones de sistemas autónomos. Debido a la demanda, se hizo necesario aumentar la posibilidad La **RFC 4893** introduce los sistemas autónomos de 32 bits, que IANA ha comenzado a asignar. Estos números de 32 bits se escriben como un par de enteros en el formato x.y, donde x e y son números de 16 bits. La representación textual de Números de sistemas autónomos está definido en la **RFC 5396**.

Los números de Sistemas Autónomos son asignados en bloques por la Internet Assigned Numbers Authority (**IANA**) a Registros Regionales de Internet (**RIRs**).

Los números de sistemas autónomos asignados por IANA pueden se encontrados en el sitio web de IANA: *http://iana.org*

El protocolo **BGP** (Border Gateway Protocol), es el responsable de enrutar todos los paquetes de Internet a lo largo del mundo. Este protocolo responde a un esquema de direccionamiento dinámico, es decir que sus rutas se van modificando frecuentemente sobre la base de diferentes métricas, que en definitiva son parámetros lógicos que permiten decidir por cuál interfaz debe sacar un determinado router cada uno de los paquetes que le llegan a él. Estas rutas se van creando sobre la base de la información que comparten los dispositivos vecinos (neighbor) que conforman esa comunidad BGP. A continuación, presentamos una imagen que representa este funcionamiento:



(Imagen tomada de: https://www.awsarchitectureblog.com/2014/12/internet-routing.html)

8.5. Sistema DNS (Domain Name System)

El sistema **DNS** es el responsable de asociar las direcciones IP con los Nombres que emplea Internet. Esta actividad se lleva a cabo por un sistema estrictamente jerárquico cuya raíz (**root**), son exactamente 13 Sites (donde cada una de ellas por supuesto está compuesta por más de un servidor con redundancia y balanceo de carga). Esta jerarquía como concepto de máximo nivel emplea el nombre de la forma **FQDN** (Fully Qualified Domain Name o Nombre de dominio completo) que se obtiene a partir del árbol, construyendo el dominio desde abajo hasta arriba, incluido el punto final y como máximo tiene 256 caracteres.

Como mencionamos, actualmente existen estos 13 servidores raíz, con los nombres de la forma **letra.root-servers.net**, donde letra va desde la **A** a la **M**. A continuación, presentamos la plantilla que está en Wikipedia con el detalle de cada uno de ellos:

Letra	Direc. IPv4	Direc. IPv6	Nro. AS	Nombre antiguo	Operador	Ubicación #sitios (global/local)	Soft ware
A	198.41.0.4	2001:503:ba3e::2:30	AS26415	ns.internic.net	Verisign	distribuido (anycast) 4/0	BIND
B	192.228.79.201	2001:478:65::53	AS4	ns1.isi.edu	USC-ISI	Marina Del Rey, California, U.S.	BIND
C	192.33.4.12	2001:500:2::c	AS2149	c.psi.net	Cogent Communications	distribuido (anycast) 8/0	BIND
D	199.7.91.13	2001:500:2d::d	AS27	terp.umd.edu	Universidad de Maryland	College Park, Maryland, U.S. 1/0	BIND
E	192.203.230.10	2001:500:a8::e	AS297	ns.nasa.gov	NASA	Mountain View, California, U.S. 1/11	BIND
F	192.5.5.241	2001:500:2f::f	AS3557	ns.isc.org	Internet Systems Consortium	distribuido (anycast) 4/51	BIND 9
G	192.112.36.4	2001:500:12::d0d	AS5927	ns.nic.ddn.mil	Defense Information Systems Agency	distribuido (anycast) 6/0	BIND
H	128.63.2.53	2001:500:1::803f:235	AS13	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, U.S. 2/0	NSD
I	192.36.148.17	2001:7fe::53	AS29216	nic.nordu.net	Netnod (antes Autonómica)	distribuido (anycast) 41/0	BIND
J	192.58.128.30	2001:503:c27::2:30	AS26415		Verisign	distribuido (anycast) 62/13	BIND
K	193.0.14.129	2001:7fd::1	AS25152		RIPE NCC	distribuido (anycast) 5/12	NSD
L	199.7.83.42	2001:500:3::42	AS20144		ICANN	distribuido (anycast) 130/0	NSD
M	202.12.27.33	2001:dc3::35	AS7500		Proyecto WIDE	distribuido (anycast) 4/1	BIND

Estos dispositivos, fueron, son y serán blanco de todo tipo de ataques, pues sin ellos sería prácticamente imposible navegar por Internet, y quizás tampoco por la red de cualquier gran empresa.

La historia de estos dispositivos, podríamos presentarla como que nace de la mano del desarrollo Open Source "**Bind**", que aún mantiene una posición respetable (*Como podemos ver en el cuadro anterior, lo emplean TODOS los root*), si bien hay que admitir que la competencia privada ha dedicado un esfuerzo admirable y hoy en día está ofreciendo productos de la forma de "Appliance" con los que es difícil competir desde el mero software, lo que sí es cierto es que casi todos ellos tienen parte del motor de Bind. El detrimento innegable de Bind es que es un hecho que su administración sigue siendo muy "estricta" en cuanto al empleo de línea de comandos y muy poca gente conoce al detalle sus pormenores, causa por la cual es muy raro encontrarlo actualizado y bien configurado.

Seguridad en **DNSs** y **DNSSec** (Domain Name System Security Extensions)

La organización jerárquica del Sistema de Nombres de Dominio y su trabajo clave en Internet, como ya mencionamos, lo posicionan como uno de los mayores blancos de ataque.

La funcionalidad del sistema DNS es resolver nombres ← → direcciones IP. (*sin esto es imposible navegar*).

Desde su nacimiento en los años 80 hasta hoy, sus mayores debilidades (*y continúan siéndolo*) son los engaños sobre esta asociación, pues son su única función. Hoy también presentan problemas con los llamados "ataques de amplificación" que han sido objeto hace pocos años-

Esta infraestructura inexorablemente debe entrar en contacto con cualquier usuario de Internet dejando el puerto 53 (TCP y UDP) abierto. Su única protección pasa por:

1. Bastionar robustamente cada host (hardening) de esta infraestructura.

2. Mantener siempre actualizados sus versiones de SSOO y aplicaciones.
3. Monitorizar su actividad y configuración permanentemente.
4. Colocar las barreras en los elementos que no necesariamente estén visibles.
5. asegurar la integridad de sus registros de información (y este es el punto clave).

El diseño original del Domain Name System (DNS) no incluía la seguridad, sino que fue diseñado para ser un sistema distribuido escalable. Las Extensiones de seguridad para el Sistema de Nombres de Dominio (DNSSec) intentan aumentar la seguridad, y al mismo tiempo mantener la compatibilidad con lo más antiguo.

La **RFC 3833** es la primera que intenta documentar algunas amenazas conocidas en el DNS y cómo DNSSec puede responder a las mismas.

Luego de esta RFC y desde principios del 2000 empezó a presentarse este conjunto de especificaciones que conforman **DNSSec**, pero recién en 2008, se consolidó con la aparición de la **RFC 5155** "Hashed Authenticated Denial of Existence" conocida como DNSSec3.

También se deben considerar las especificaciones llamadas DNSSec-bis, que describen el actual protocolo DNSSec con más detalle. Ellas son **RFC 4033**, **RFC 4034** y **RFC 4035**.

El registro DNSKEY correcto se autentica a través de una cadena de confianza, que comienza en un conjunto de claves públicas de la zona raíz del DNS, que es la tercera parte de confianza.

El punto clave de toda esta propuesta pasa por la implementación de "firmas" de zonas a través del empleo de certificados digitales.

Con esta estrategia, se asegura la "Integridad" de las zonas de todos los servidores y a su vez las respuestas que se ofrecen a las solicitudes, solucionando con ello el problema más crítico de este servicio.

Servidores de agujero negro.

La **RFC 1918** reserva tres rangos de direcciones de red para su uso en redes privadas en IPv4:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Este tráfico debe ser filtrado por todo ISP en su conexión hacia Internet, pero a pesar de ello, no es raro que este tipo de tráfico se filtre y aparezca de todos modos.

Para hacer frente a este problema, **IANA** ha puesto en marcha inicialmente tres servidores DNS especiales llamados "**servidores de agujeros negros**". En sus inicios los servidores de agujeros negros fueron los siguientes:

- Blackhole-1.iana.org
- Blackhole-2.iana.org
- prisoner.iana.org

Estos servidores están configurados para responder a cualquier consulta con una "dirección inexistente" como respuesta. Esto ayuda a reducir los tiempos de espera ya que la respuesta (negativa) se da de manera inmediata y por lo tanto no se requiere que expire. Además, la respuesta devuelta es también permitida se ser guardada en caché de los servidores DNS recursivos. Esto es especialmente útil debido a una segunda búsqueda para la misma dirección realizada por el mismo nodo, probablemente sería respondida desde la caché local en lugar de consultar a los servidores autorizados de nuevo. Esto ayuda a reducir significativamente la carga de red. Según IANA,

los servidores de agujeros negros reciben miles de consultas por segundo.

En la actualidad funciona el proyecto **AS112** que se trata de un grupo de operadores de servidores de nombres de voluntarios que se unieron en un sistema autónomo. Ellos operan instancias de los servidores de nombres con anycast que responden la búsqueda DNS inversa para direcciones de red privada y de enlace local que hayan sido enviadas a la Internet pública. Estas consultas son ambiguas por su naturaleza y no se pueden responder correctamente. Pero las respuestas negativas se proporcionan de todos modos para reducir la carga sobre la infraestructura DNS pública.

8.6. Tareas para el hogar (deberes).

Una vez más en este capítulo os propongo algunas actividades o líneas de reflexión.

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cómo llevas los conceptos de medio físico?, ¿tienes claro los tipos de cables, fibras y emisiones de radio que existen?
2. Identifica en tu País, quiénes son tus Tier 1, 2 y 3.
3. ¿Empleas BGP en alguno de tus routers?, en ese caso ¿Empleas autenticación de neighborhood?
4. Explora la Web: http://he.net/3d-map/ y analiza sus contenidos.
5. ¿Quiénes son tus DNSs de jerarquía superior?
6. ¿Has avanzado sobre DNSec en tus redes?, ¿Qué conclusiones o comentarios merece?

9. Ciberseguridad: empleo de SOC y NOC

Resumen del tema

Desde el punto de vista de Ciberseguridad, para poder ofrecer un grado mínimo de "Disponibilidad" y "Alarmas tempranas" es necesario contar con una infraestructura de "Supervisión y Monitorización". Desde el punto de vista de la Ciberseguridad a su vez, no sólo nos interesa por la disponibilidad, sino también como hemos mencionado, para la detección temprana y la generación de alertas ante cualquier actividad anómala en la misma. Ambas funciones se llevan a cabo a través de:

- **NOC** (Network Operation Center).
- **SOC** (Security Operation Center).

Desde ya que estas funciones deberán ser acordes al tipo de red y se deberá asignar los recursos adecuados para cada tipología, pero lo importante aquí es ser conscientes de la importancia que revista esta actividad y plantearse SIEMPRE cómo se llevará a cabo, por mínima que sea la infraestructura.

En este capítulo se definirán los aspectos que deben ser tenidos en cuenta, en general se presentan con un "objetivo de máxima", es decir lo ideal que podríamos plantear si tuviéramos un NOC y un SOC 24x7, pero reiteramos, lo importante es no olvidarse de esta actividad y ajustarla a la red que cada uno posea.

En cuanto a la Supervisión / Monitorización / Alarmas, nuestra experiencia al respecto es muy positiva. En general todas las redes, poseen algún tipo de mecanismos para esta actividad.

El aspecto sobre el que vamos comenzar es el "*Flujo y categorización*" de alarmas e *incidentes de seguridad*. Para ello, inicialmente debemos diferenciar el concepto de "**NOC**: Network Operation Center" del de "**SOC**: Security Operation Center", pues este último sí debería abocarse exclusivamente a seguridad,

mientras que el primero no. La cuestión, tal cual planteamos al inicio, está en que no todas las redes poseen SOC (*y tampoco se justifica que lo tengan*), en estos casos, evidentemente algún tipo de tareas relacionadas a seguridad deberían recaer sobre el NOC.

Sea cual fuere la situación (con o sin SOC), nuestro objetivo debería conducirnos a obtener una visión clara sobre:

> **¿Qué hace este personal si detecta alguna anomalía en la red, cuyos parámetros puedan estar relacionados con un incidente de seguridad?**

9.1. NOC (Network Operation Center)

Los **NOC** o también llamados **CCR** (Centro de Control de Red), nacen en los años 60 para obtener información del estado de routers y swithcs. Se trata de ubicaciones físicas hacia donde converge toda la información de supervisión, monitorización y alarmas de la red o infraestructuras que tiene bajo su responsabilidad. Se trata de un conjunto de recursos humanos y materiales que están **24x7** los **365 días** del año y cuyas funciones básicas son:

- Monitorización y detección de eventos
- Clasificar y categorizarlos (Determinar impacto)
- Documentarlos (Sistema de Ticketing)
- Gestión de alarmas
- Gestión de incidentes
- Gestión de peticiones (Control de cambios)
- Gestión de accesos
- Gestión de inventario

Podríamos pensar que la "Monitorización y detección de eventos" es su rol primario, cada evento que llega debe pasar a una segunda instancia "Clasificar y categorizarlos" que permite determinar su impacto y derivarlo a su cadena de escalada correspondiente una vez "documentado", para lo cual una muy buena estrategia es contar con un sólido sistema de "ticketing".

La pregunta natural que nos podemos hacer entonces es ¿Qué es un evento para el NOC?

Ejemplos típicos de ello son:

a. Incremento anómalo de ancho de banda.
b. Saturación del ancho de banda.
c. Caídas o fallos de dispositivos.
d. Caídas o fallos de algún enlace.
e. Propagación abusiva de un determinado patrón de tráfico.
f. Modificaciones sensibles del flujo de tráfico de nuestros DNSs.
g. Incremento llamativo del volumen de Logs.
h. Mensajes anómalos en los Logs de elementos de red.
i. Alarmas en bases de datos, procesadores, módulos de memoria.
j. Alteración de rutas.
k. Fallos en los sistemas de señalización.
l. Segmentos de red o dispositivos inalcanzables.
m. Pérdidas de accesos de gestión a dispositivos.
n. Modificación de contraseñas, cuentas, perfiles, roles, o directorios activos.
o. Intentos reiterados de accesos (fallidos o no).
p. Escaneos anómalos de red o puertos.
q. Etc.

Con este tipo de ocurrencias, se está ante indicios de algo que puede guardar relación con incidentes en los dispositivos o enlaces de la red. En principio un procedimiento de gestión de Supervisión / monitorización, debe contemplar si están o no tipificados estos casos, en el caso de no estarlo, se debe lanzar una secuencia de acciones, por ejemplo:

- ¿Se trata de un evento de red o de seguridad?
- ¿Existe un procedimiento ante estos casos específicos?
- ¿Se conocen o definen los pasos a seguir?
- Dentro del workflow de este centro, ¿está contemplado o tipificado algún "ticket" (o varios tipos de "tickets") para este tipo de eventos?
- ¿Está categorizado este flujo para incidentes de red o de seguridad?
- ¿Se conoce la jerarquía, niveles de escalado o cadena de comunicación para estos casos?
- ¿Cómo se abre, verifica, mantiene y cierran estas incidencias?

Por supuesto, estamos presentando el tema, sobre la base de un NOC que está en producción. Si aún se está planificando o recién se está implantando el mismo, hay más consideraciones que deben ser tenidas en cuenta son:

- Situación de los centros de supervisión de red.

  Que existan en nuestras redes, que posean las herramientas necesarias, que el personal tenga documentadas y comprenda sus funciones, responsabilidades y obligaciones, que los elementos y eventos a monitorizar y supervisar sean acordes al dimensionamiento del centro.

- Que se generen los "Registros de auditoría y monitorización".

  Que se contemple su revisión de forma continua junto a la eficacia y eficiencia de los controles de seguridad establecidos, así como la

detección de las anomalías que puedan afectar a la seguridad de la información y los recursos de la empresa.

Para ello es necesario definir, implantar y/o gestionar:

- los requisitos y tecnologías de generación y almacenamiento de los registros de auditoría.
- los procedimientos y tecnologías de monitorización de los registros de auditoría.

Se deberían registrar todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias o fallos observables en un sistema de información o red de comunicaciones que puedan estar relacionados con la confidencialidad, integridad y/o disponibilidad de la información. Especialmente se registrará la actividad de los administradores y operadores de los sistemas de información.

En cuanto a la supervisión hay consideraciones específicas que deben ser detectados para luego poder enviarlos o no al SOC:

- ¿Se registra especialmente la actividad de los administradores y operadores de los sistemas de información?
- ¿Se realiza algún tipo de análisis para determinar la profundidad o cantidad de eventos a registrar en un sistema de información o red de comunicaciones?
- En cualquier caso, se supervisan y monitorizan adecuadamente los eventos de seguridad que se detallan a continuación?:
  - los eventos requeridos por la legislación aplicable.
  - los intentos de autenticación fallidos.
  - los accesos de los usuarios a los dispositivos, tanto autorizados como los intentos no autorizados.
  - los eventos de operación y administración de los sistemas: el uso de cuentas privilegiadas de administración (*root, admin, etc.*), el uso de programas y utilidades de administración, la parada y arranque de los sistemas, la instalación o desinstalación de dispositivos de almacenamiento o de entrada/salida, etc.

- los cambios en los parámetros de configuración de los sistemas.
- los errores de funcionamiento de los sistemas y las redes.
- los accesos a redes de comunicaciones, tanto autorizados como los intentos no autorizados: acceso remoto a la red interna (*por acceso remto, ADSL, red privada virtual, fuera de banda, etc.),* accesos a Internet, etc.
- el tráfico no permitido o rechazado por los cortafuegos y los dispositivos de encaminamiento (*al menos de los protocolos más comunes y/o peligrosos*).
- las alertas generadas por los dispositivos de detección/prevención de intrusos (IDS/IPS).
- los cambios en los privilegios de acceso: alta, baja y modificación de usuarios, cambios en los perfiles, grupos o roles, etc.
- los cambios en los sistemas de seguridad, como la activación/desactivación o cambios en la configuración de los antivirus, de los sistemas de control de acceso, etc.
- el acceso al código fuente de los sistemas desarrollados.
- la activación/desactivación o cambios en la configuración de los mecanismos que generan los registros de auditoría.
- las modificaciones o borrado de los ficheros con registros de auditoría.
- el acceso a datos de carácter personal sensibles.

Debe existir un procedimiento para establecer claramente que infraestructuras, plataformas, dispositivos, redes y sistemas serán monitorizados y de qué forma se elaborarán y revisarán informes periódicos con los resultados de la monitorización. La periodicidad en la generación y revisión de cada informe estará determinada por el análisis de riesgos del elemento al que aplica.

Se deben considerar también los errores de funcionamiento de los sistemas y redes reportados por los usuarios o generados por las

aplicaciones y cómo deberán ser analizados para identificar los posibles problemas de los sistemas.

Se recomienda dentro de lo posible, el uso de un sistema centralizado para la monitorización y supervisión de red que sea independiente del resto de equipos y aplicaciones. Estos sistemas centralizados permiten la definición de reglas de correlación para la identificación de ataques y modelos de comportamiento.

9.2. SOC (Security Operation Center)

De forma similar al NOC, un **SOC** es también una ubicación física donde se concentran los recursos humanos y materiales cuya responsabilidad es la monitorización, detección, análisis, prevención y seguimiento de los eventos de seguridad en las redes e infraestructuras de la organización. Hemos presentado en primer lugar el concepto de NOC pues ambos deberían trabajar muy "de la mano".

Si se han ajustado adecuadamente los procedimientos, el NOC será una de las principales fuentes de información del SOC, y si se han categorizado correctamente los "eventos de seguridad" el envío fluido de los mismos hacia el SOC será una actividad frecuente.

Es factible implantar un SOC que no opere 24x7 si se puede considerar un servicio de guardia para cualquier incidente crítico cuando se cuenta con sistemas de detección temprana o, justamente un NOC, que ofrezca esta función de alarma y escalada. Otra opción que está creciendo día a día es "managed security service providers", es decir, tercerizar este servicio en otra empresa especializada en seguridad y que cuente con su propio SOC orientado a prestar servicio a empresas externas; en la actualidad hay una amplia oferta al respecto y es fundamental tomarse un buen tiempo para seleccionar la que más se ajuste a nuestra necesidad concreta.

La implementación de un SOC es una decisión estratégica de la

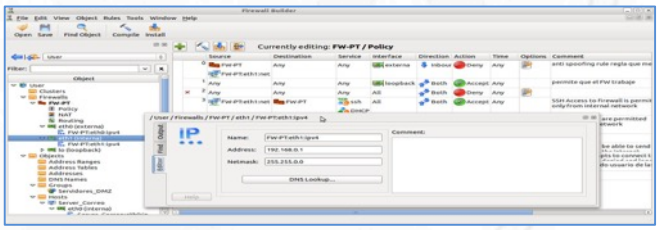
empresa, que tiene un coste considerable, por lo que debe ser analizada en detalle.

Un SOC debería proporcionar al menos los siguientes servicios:

- Monitorización y gestión de la infraestructura de seguridad.
- Gestión de incidentes de seguridad.
- Gestión de vulnerabilidades.
- Auditorías de seguridad.
- Apoyo a cumplimiento regulatorio.
- Investigación de seguridad en Internet.
- Análisis y detección de malware.
- Prevención de la seguridad.
- Cadenas de contactos y escalada en incidentes de seguridad.
- Propuesta y seguimiento de acciones de mejora en seguridad.

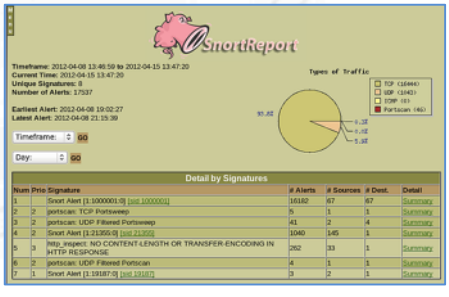
Las herramientas que puede operar un SOC son:

- Firewalls



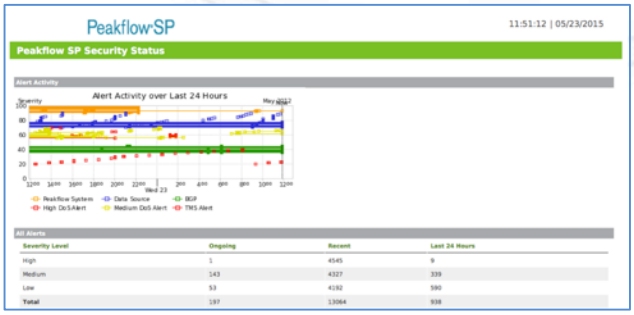
Herramienta FWBuilder

- IDSs/IPSs



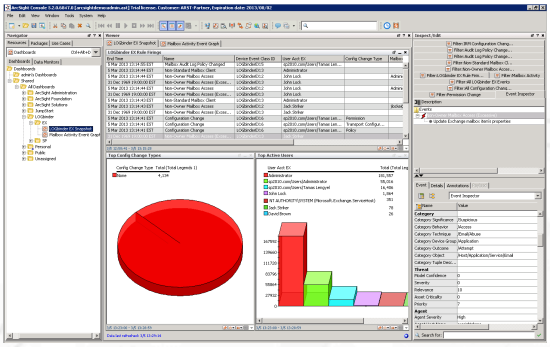
IDS Snort

- Sistemas AntiDDoS



ARBOR Peak Flow

- Plataformas SIEM



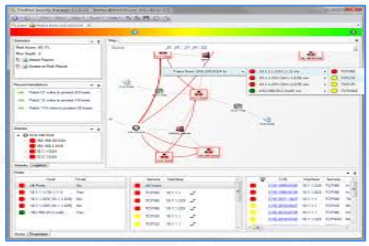
Herramienta HP ArcSight

Herramienta RSA Security Analytics

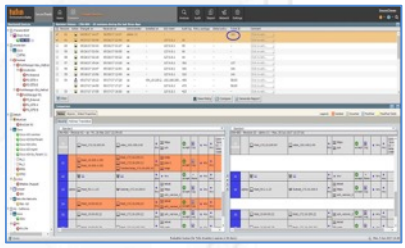
- Honey Pots (Ver proyecto honeynet: https://www.honeynet.org)

- Herramientas de gestión de FWs, Routers, Switchs (*Algosec, Firemon, Tufin, Nipper, OPnet*).

Algosec

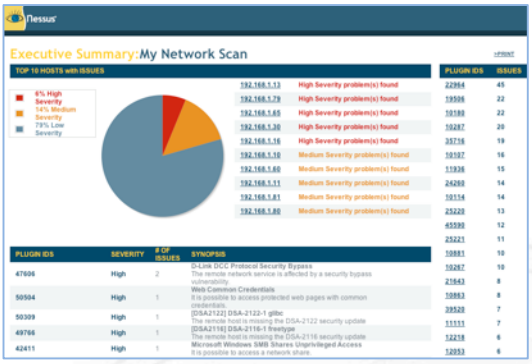


Firemon

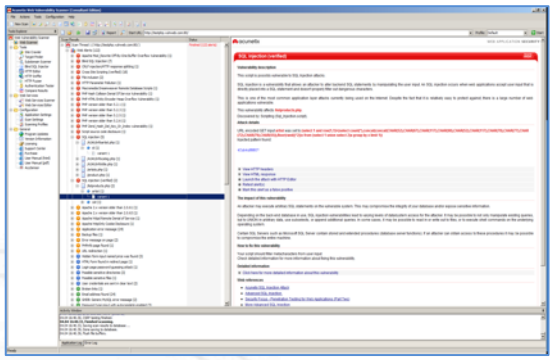


Tufin

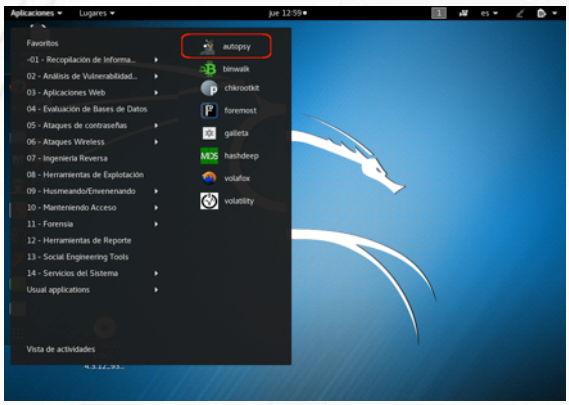
Herramientas de análisis de vulnerabilidades (Nessus, Accunetix, Burp, OSSIM: Open System Security Information Management, nmap, john, Kali, etc).



Herramienta Nessus



Herramienta Accunetix



Sistema Operativo "Kali" (Linux)

Heramienta Nikto

Herramienta OSSIMM

9.3. Tareas para el hogar (deberes).

Una vez más en este capítulo os propongo llevarnos a casa algunas actividades o líneas de reflexión para que comencemos el capítulo que viene con más "expertiz".

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cómo diseñarías un NOC para tu empresa?

2. ¿Qué aspectos consideras más importantes a procedimentar en un NOC?
3. ¿Hay aspectos que crees pueden ser automatizados como respuesta a eventos?
4. ¿Qué eventos concretos son los que deberían ser escalados a un SOC?
5. ¿Cuáles serían para ti las fuentes de información desde las que obtener información y actualizaciones sobre temas de seguridad?
6. ¿Qué pasos seguirías para hacer "inteligencia" en temas de seguridad a través de Internet?

10. Ciberseguridad: la importancia de saber gestionar "Logs"

Resumen del tema

El concepto de Logs, muchas veces se relaciona o se denomina como "Registro de Auditoría", lo cual sin entrar en debates sobre si es correcto o no, puede resultarnos interesante pues en definitiva un Log es un tipo de registro que se genera desde un dispositivo para dejar constancia de un evento. Un Log (o registro) para un sistema Unix, que fue el punto de partida de estos temas, es de un tipo u otro dependiendo de la aplicación de la que provenga (*facilities*) y del nivel de "gravedad" del evento que ha logueado (*priorities*).

El detalle del sistema de Syslog, si bien lo mencionaremos en este capítulo, no lo desarrollaremos en profundidad, nos centraremos más en el procedimiento de "**gestión de Logs**".

Una de las acciones sobre las que más interés hemos puesto en los últimos años es justamente la implantación de plataformas de centralización de Logs. Hoy en día debemos referirnos a estas como **SIEM**: Security Information and Event Management.

En realidad, el concepto de SIEM viene de una combinación de dos soluciones (o definiciones) anteriores:

- **SIM**: Security Information Management
- **SEM**: Security Event Management

Al unir ambas ideas aparece, tal vez más robusta, la posibilidad de "correlar" (*o correlacionar*) eventos de seguridad, tema sobre lo que sí se hará hincapié en esta última charla.

10.1. Presentación.

Los "Logs" o también llamados "registros" son las huellas que todo sistema de telecomunicaciones puede ir dejando a lo largo de su ciclo de vida. Como todo proceso informático, estos Logs son generados por procesos del sistema, los cuáles pueden ser perfectamente parametrizados para que justamente nos dejen huellas de la actividad que haga falta. Una vez generados, se debe considerar que hacer con ellos: categorizarlos, priorizarlos, guardarlos, enviarlos, volver a procesarlos, descartarlos, etc.

Desde el punto de vista de la Ciberseguridad son fundamentales, ellos nos dirán justamente qué es lo que se ha hecho o dejado de hacer, por esa razón es que debemos darle la importancia que merecen.

> **Anécdota**: No puedo dar mucha información sobre la empresa, pero sí deseo poner de manifiesto que en una de las redes que he trabajado, había un servidor verdaderamente crítico. Su importancia era tal que, para la gestión de sus logs, independientemente que respondían a una seria política de almacenamiento y envío, a su vez, tenía conectada una impresora de matriz de punto y papel de formulario continuo, en la cual se imprimían en tiempo real TODOS los Logs que generaba este servidor.
>
> Esta decisión respondía a que si cualquier intruso llegaba a acceder al mismo (*cuestión que todo administrador debe ser consciente que puede suceder, por más medidas de seguridad que adopte…*), TODA la actividad que realizara, se imprimía inmediatamente, y una vez impreso, este proceso es irreversible, por más que el intruso logre borrar todos sus rastros electrónicos, el formulario continuo ya habría pasado a la siguiente línea y no vuelve atrás.

Volviendo a uno de los conceptos fundamentales de Ciberseguridad que hemos puesto de manifiesto desde el primer día, la "**Resiliencia**" de un sistema, independientemente de nuestro adecuado sistema de resguardo y recuperación, dependerá en gran medida de cómo hayamos tratado estos Logs, pues a través de ellos podremos analizar detalladamente la gran

mayoría de los incidentes que surjan en nuestras infraestructuras y llegar a las causas raíces de los mismos.

Consideremos que los Logs son fundamentales, por esa razón es que deben ser tratados con sumo cuidado, tanto en su integridad, disponibilidad, como en su confidencialidad. Un intruso será de las primeras cosas que intentará borrar de su actividad, como así también de las primeras que intentará acceder pues les dará toda la información de ese dispositivo, red, infraestructura, sistema, etc.

Los aspectos legales también merecen la pena ser tenidos en cuenta, pues si los Logs deben ser presentados como una prueba jurídica, deberemos ser capaces de demostrar su validez, temporalidad, integridad, buen uso, tratamiento, acceso, etc.

Otro tema, a la hora de trabajar con Logs, es que los dispositivos "fuente" de Logs, es decir todo elemento que genere Logs, debe encontrarse perfectamente "**sincronizado**", pues si los Logs de diferentes dispositivos no responden a una base de tiempo en común, el repositorio al cual son enviados los irá encolando sobre la fecha/hora que su fuente les impuso, por lo tanto si es necesario analizar un rango de información temporal proveniente de diferentes dispositivos, y cada uno de ellos les puso una base de tiempo diferente, sería imposible seguir algún tipo de lógica. Este problema tiene una solución muy sencilla, que es el empleo de una sencilla jerarquía del protocolo "**ntp**" (*Network Time Protocol*), definiendo claramente sus "stratus" (o jerarquía) y los nodos hacia donde debe "apuntar" cada área.

La adecuada gestión y explotación de Logs permite:

- Aprender a ajustar nuestras infraestructuras.
- Detectar amenazas, patrones anómalos, picos de tráfico, actividad sospechosa.
- Prevenir o detectar fugas de información.
- Realizar análisis forense.

- Correlacionar información de diferentes fuentes.
- Dar cobertura legal.
- Detectar altas, bajas o modificaciones de usuarios, aplicaciones, configuraciones, protocolos, etc.
- realizar seguimiento de acciones de mejora o desvíos en as mismas.
- Tareas de supervisión y monitorización de redes y sistemas.
- Detectar y prevenir caídas y fallos en redes y sistemas.
- Configuración de alarmas y umbrales.

He trabajado con syslog desde hace muchos años, pero como análisis detallado del mismo puedo citar una actividad que tiene su comienzo teórico a finales de 2002, cuando a través de los trabajos realizados con IDSs y con la infraestructura de software libre denominada **OSSIM** (*Open Source Security Information Management*) que estaba naciendo en esos años. Comenzamos a comprobar que la "lógica" de operación, para la detección de eventos críticos no era la adecuada. En su momento publicamos un artículo en Internet que se denominó "**Metodología Nessus-Snort**" o también conocida como "**Metodología: Generación de ataques / Detección con NIDS**", que aún sigue vigente en Internet. Más adelante, siguiendo en esta línea de pensamiento, publicamos otro artículo que se llamó "**Matriz de estado de seguridad**", que también hoy se puede encontrar en la red.

Nuestra idea principal era y sigue siendo un punto de partida fundamental:

> *Es imposible hoy en día controlar los miles de Logs o eventos que generan los servidores.*
>
> *No se puede empezar desde lo general a lo particular, sino todo lo contrario.*
>
> *Debemos saber PRIMERO, a qué somos vulnerables, y luego, muy metódicamente, ajustar de forma sencilla, nuestros dispositivos de detección.*

Nuestra filosofía fue radicalmente diferente al resto, y basada en un viejo lema militar: "**Solo lo sencillo promete éxito**", por esta razón partimos de lo sencillo, para ir avanzando en complejidad, hasta donde se desee.

Una realidad con la que nos encontramos frecuentemente en empresas que comienzan a implementar plataformas de centralización de Logs y/o SIEM, es que la primera fase de esta tarea suele ser la configuración de los dispositivos para el envío de estos Logs hacia los repositorios o relés. En esta fase lo más normal es ver que no se realice ningún tipo de análisis sobre qué tipo de Logs deseamos centralizar y por lo tanto se envían de forma masiva la totalidad de los mismos. Como cabe suponer esto satura cualquier tipo de servidor, BBDD o discos, y a su vez dificulta tremendamente la capacidad de análisis pues se nos comienza a hacer imposible detectar lo importante dentro de semejantes volúmenes de información.

10.2. El sistema Syslog de Unix (syslog como estándar).

El sistema de syslog nace en los años 80', pero recién en 2001 es cuando aparece su primer paso a estandarización a través de la **RFC-3164**, hoy obsoleta por la **RFC 5424,** hablaremos de ambas. El mundo de Internet se sustenta hoy en la pila TCP/IP, por lo tanto, el origen de la información de todo protocolo o aspectos considerar deben ser las RFCs. Este conjunto de documentos debería ser tenido en cuenta como punto de partida siempre que se desee estudiar cualquier tema en relación a esta red. En el caso de syslog, una vez más podemos ver que si bien desde el 2001 está bastante claro su funcionamiento, siguen existiendo fabricantes que no lo cumplen estrictamente, ocasionando con ello que cuando se desea centralizar Logs en alguna plataforma específica para ello, uno de los mayores problemas que nos encontramos es la "normalización", es decir, intentar darle un formato único al conjunto de los Logs que se reciben, de los cuáles seguramente varios de ellos no responden justamente a lo que desarrollaremos en este punto.

Presentemos algunos conceptos clave de estas RFCs.

Comencemos con la **RFC-3164**. Syslog emplea el protocolo **UDP** (User datagram Protocolo) a nivel transporte y tiene asignado como puerto destino el **514**, esta RFC RECOMIENDA que también el puerto "fuente" sea el UDP 514 para indicar con total claridad que es un mensaje generado por el sistema syslog.

Cualquier elemento que genera mensajes syslog será llamado "dispositivo"
Una máquina que pueda recibir mensajes syslog y re encaminarlos se llamará "relay"
Una máquina que recibe mensajes y no los encamina se llamará "colector" (*comúnmente llamado también "syslog server").*

Los mensajes syslog tienen tres partes:

- PRI Part
- Header (Encabezado)
- MSG (Mensaje)

La notación que emplea es **ABNF** (*Augmented Bakus-Naur format*) que está estandarizada por la **RFC-5234**. Es un formato que nace en los años 60', como método para expresar gramáticas libres de contexto, se emplea como reglas de formación de la gramática en los lenguajes de programación (*cuyo punto de partida fue ALGOL 58*). Su nombre se debe al primer precursor **John Backus** (*en 1959*) que luego fue simplificada en subconjunto de símbolos por **Peter Naur**. En resumen, se trata de in sistema de reglas del estilo que todo programador conoce

<símbolo> ::= <expresión con símbolos>

La RFC luego define otros conceptos:

- **Facilidad** (*o recurso*): Se trata del tipo de dispositivo, o elemento que ha generado el log.

Los define textualmente como se presentan a continuación:

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

- **Severidad** (*prioridad o nivel*): Indica la "gravedad" del Log

Los define textualmente como se presentan a continuación:

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

El valor del campo PRI (Prioridad) debe calcularse multiplicando en primer lugar la "Facilidad" por 8 y a esta operación sumarle el valor de la "Severidad". Por ejemplo:

Facilidad = 0: kernel messages
Severidad = 0: Emergency

Un mensaje de este tipo tendría una prioridad igual a:

Prioridad = (0x8) + 0 = **0**

Otro ejemplo:

Facilidad = 20: local use 4 (local4)
Severidad = 5: Notice

Un mensaje de este tipo tendría una prioridad igual a:

Prioridad = (20x8) + 5 = **165**

Cuanto menor sea su prioridad, más "prioritario" debería ser.

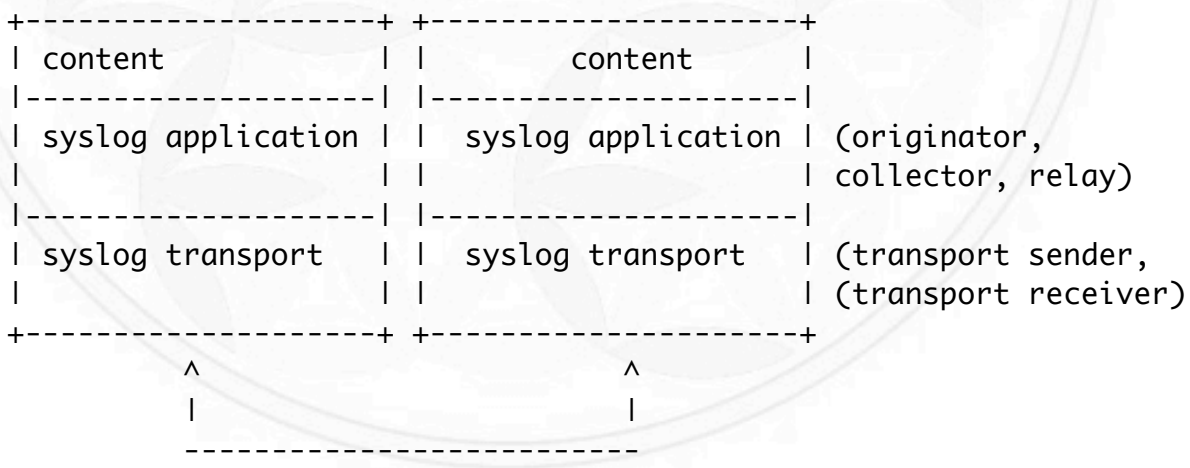
El Header (*encabezado*) contiene el "Timestamp" y el hostname o dirección IP del dispositivo. Según esta primer RFC, ll Timestamp debe ser de formato "Mmm dd hh:mm:ss"

Por último, el campo MSG tiene el TAG y el CONTENT, el TAG se debería corresponder con el nombre del programa o proceso que generó el mensaje y el CONTENT, justamente el detalle del mensaje.

Cuando en marzo de 2009, aparece la RFC-5424 introduce las siguientes modificaciones (resumiremos las más importantes):

Define tres niveles para syslog:

- Syslog content (contenido): Información de gestión de un mensaje
- Syslog application (aplicación): Generación, interpretación, enrutamiento y almacenamiento
- Syslog transport (transporte): Envío y recepción de mensajes



En este diagrama la **RFC-5424** nos muestra las diferentes entidades, separadas por nivel.

Esta nueva RFC, no especifica cómo opera el nivel de transporte. Lo deriva en la **RFC-5426** (*que es consistente con el tradicional transporte*

UDP por el puerto 514), pero sí establece como novedad que toda implementación de esta RFC DEBE soportar transporte basado en **TLS** (*Transport Secure Layer*) y lo deriva en la **RFC-5435**.

Luego describe todo el nuevo formato del mensaje syslog, donde sí encontramos muchas novedades que no merece la pena profundizar en este texto, pero aparecen nuevas longitudes, campos, fechas, nombres, etc. Manteniendo su punto de partida exactamente igual en cuanto al "corazón" de syslog de sus facilidades y severidad. Esta nueva versión de syslog debe se define como **versión 1**.

En cuanto a cómo se ejecuta el sistema de syslog, en los entornos Unix, es por medio de demonios.

El primero de ellos es:

- **Sysklogd**: Es el más básico e histórico. Dentro de este, en realidad se esconden dos: **Syslogd** (*mensajes del sistema*) y **klogd** (*mensajes del kernel*).

A finales de los 90`aparece:

- **Syslog-ng** (*por next generation*) cuyas mayores prestaciones pasan por añadir más filtros y sobre todo la posibilidad de emplear **TCP** (*Transport Control Protocol*) a nivel transporte, dándole más confiabilidad

Y por último tenemos a:

- **Rsysylog** (2004): mejora la fiabilidad sobre TCP, mejora compatibilidad con su precursor (sysklogd) y sobre todo facilita los envíos remotos, soportando también algoritmos de cifrado y marcas de tiempo. Podríamos afirmar que en la actualidad está soportado por todas las distribuciones Unix/Linux

10.3. Plataformas SIEM

Una de las mejores medidas que se pueden tener en cuenta al trabajar con Logs es la implantación de plataformas de centralización de los mismos. Hoy en día debemos referirnos a estas como **SIEM**: Security Information and Event Management.

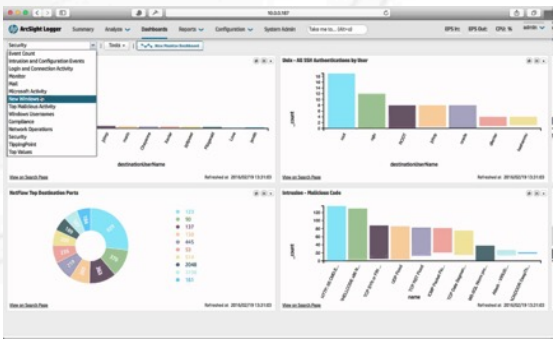
En realidad el concepto de SIEM viene de una combinación de dos soluciones (o definiciones) anteriores:

- **SIM**: Security Information Management
- **SEM**: Security Event Management

Al unir ambas ideas aparece, tal vez más robusta, la posibilidad de "correlar" (*o correlacionar*) eventos de seguridad. Hoy en día estas implementaciones son de uso frecuente, y a nivel grandes empresas se puede poner como ejemplo los siguientes productos:

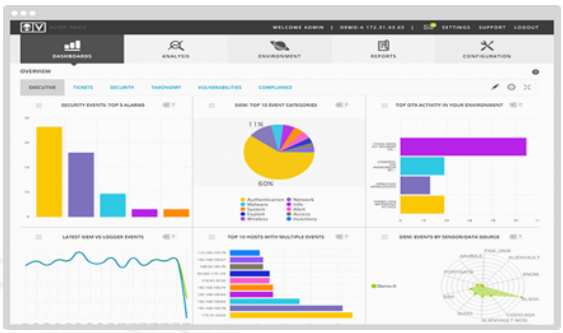
- ArcSight de HP
- RSA Security Analytics
- IBM Security QRadar
- AlienVault Unified Security Management.
- Splunk (Puede discutirse si es o no un SIEM…)
- McAfee Enterprise Security Manager

RSA Security Analytics



ArcSight de HP

IBM Security QRadar



AlienVault Unified Security Management (OSSIMM).

Splunk

McAfee Enterprise Security Manager

Independientemente de las mayores o menores prestaciones que cada una de ellos ofrezca, nuestra experiencia al trabajar con estas plataformas, es que deberíamos considerara dos aspectos fundamentales desde el punto de vista de la seguridad:

1) El nivel de implantación y explotación a alcanzar.
2) El nivel de seguridad en la gestión de la plataforma.

1) El nivel de implantación y explotación a alcanzar.

Los indicadores del estado de implantación podemos medirlos o evaluarlos en base a:

- Tiempo de puesta en producción de la herramienta.
- Recursos dedicados a la misma.

- Análisis de prioridades sobre elementos críticos que deban enviar Los a la plataforma.
- Cantidad de ellos que en la actualidad estén enviando Logs.
- Gestiones en curso para nuevas integraciones de envíos de Logs.
- Desenvoltura, capacidad del administrador en el manejo de la herramienta.
- Tipo de consultas, vistas, informes y estadísticas definidas.
- Informes generados.
- Explotación de la plataforma: descubrimientos, elevación, evolución, seguimiento, acciones de mejora que hayan generado estos informes.

2) El nivel de seguridad en la gestión de la plataforma.

   El acceso a la plataforma debe estar realizándose a través de https hacia la interfaz web de acceso, los usuarios en lo posible deberían validar contra algún LDAP, TACACS o servidores de autenticación externo. Por supuesto no se deben emplear cuentas genéricas o por defecto, como tampoco nombres triviales (y mucho menos contraseñas triviales).

Si estamos evaluando la plataforma, podremos analizar los "login" de usuarios sobre la misma en un período de tiempo, en esta consulta nos interesa observar que no sean excesivos, que no se esté empleando "Administrator", y que no aparezcan Fails más allá del normal error de equivocarse alguna vez en la validación. Un factor clave es qué política de almacenamiento, rotación y borrado emplea para el tratamiento de Logs.

Una actividad importante es implantar de forma segura y "ajustada" el acceso de cada dispositivo que envía Logs hacia aquí. En las grandes redes, lo más frecuente es que no exista una visibilidad directa desde el dispositivo al colector, por lo tanto, deberíamos colocar "relay" en zonas críticas y/o abrir rutas y/o reglas en Firewalls.

En estos casos, se deben tener en cuenta las siguientes medidas:

- El que envía Logs (*la fuente*) es un dispositivo concreto, no un "rango" o segmento de red, por lo tanto, la regla debería ser una sólo IP origen. Las excepciones que pueden presentarse sobre este tema, son por ejemplo que exista un segmento claramente identificado y ajustado el segmento de red donde se encuentran varias fuentes de Logs (Ej: Core de routers críticos).
- El puerto normal de envío de Logs, es el estándar de "Syslog": UDP 514. Sólo debería encontrarse este como destino.
- Existen excepciones de envíos a este puerto, que se denominan "File Reader" en EnVision, por ejemplo, cuando el "Colector" (que es quien debe recolectar los Logs) necesita obtenerlos de sistemas particulares, caso "Microsoft Exchange", en estos casos necesita hacer empleo del protocolo "sftp" a través del puero TCP 22 de forma "bidireccional", por lo tanto pueden ocurrir este tipo de excepciones, siempre y cuando se encuentren debidamente documentadas. Otro tipo de ellas son hacia ODBC (Puertos 1433 y 1434), también hacia sistemas propietarios como el caso de los Firewall Check Point con los puertos 18184 y 18210, el envío y recepción de snmp con puertos UDP 161 y162, en máquinas Windows recientemente se ha habilitado otra alternativa de consultas a eventos por http o https (TCP 80 y 443). En cualquier caso lo que nos interesa es que en ninguno de ellos existe la necesidad que la regla de filtrado sea "generosa u holgada", SIEMPRE podrá (o deberá) ser puntual puerto TCP 22, puerto TCP 1434, TCP 443, etc..

10.4. Herramientas Open Source para el trabajo con Logs.

En este punto, se presentan algunas opciones de herramientas para trabajar con Logs de distribución gratuita.

AWStats

Potente herramienta orientada al análisis de todo tipo de Logs (Web/Mail/FTP, etc.). Trabaja a través de interfaz gráfica o por línea de comandos, ofrece varios tipos de estadísticas. Su URL es:

http://www.awstats.org

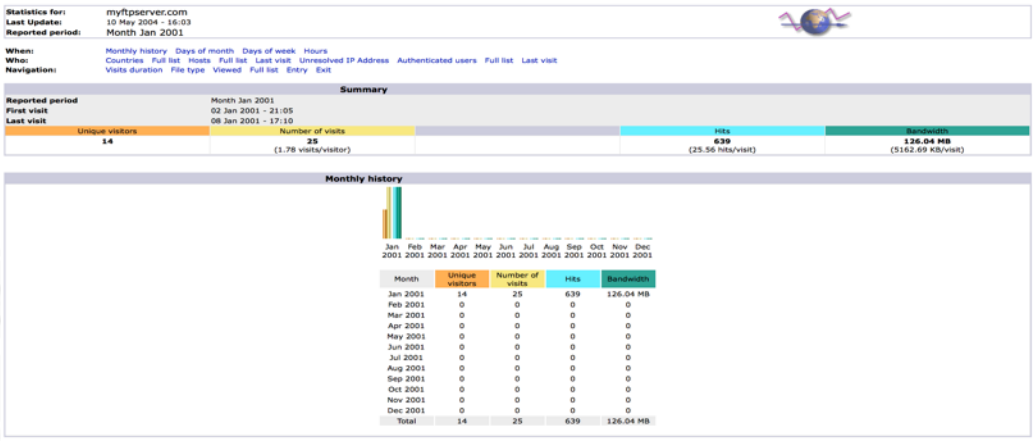


Imagen tomada de http://www.awstats.org/awstats.ftp.html

Goaccess

Herramienta orientada a Logs generados por servidores Web, diseñada en "C" que permite ser empleada con una sencilla instalación y operada por línea de comandos o interfaz gráfica. Su autoría es de **Gerardo Orellana** y se encuentra en:

https://goaccess.io

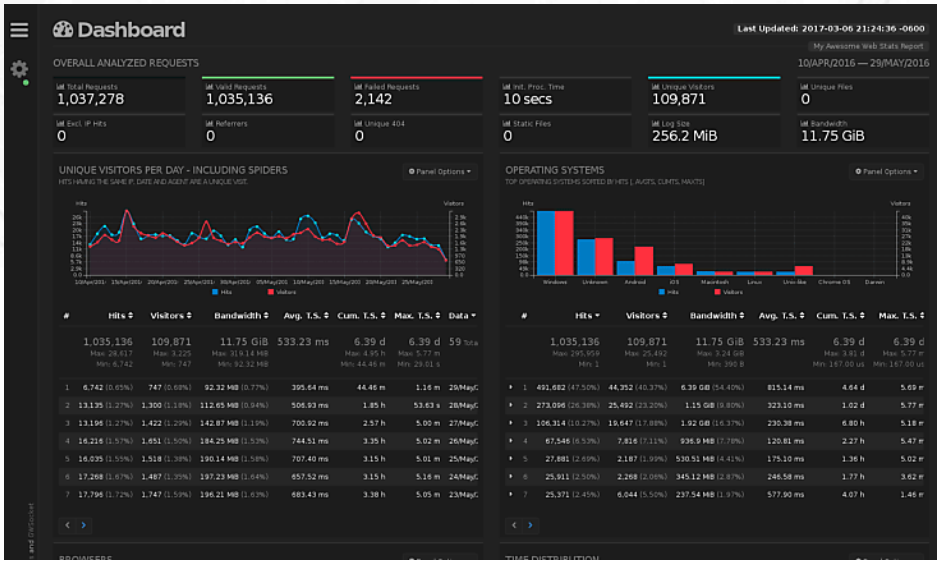


Imagen tomada de https://goaccess.io

Guía de SANS para crear un SIEM

El **SANS Institute** (*SysAdmin Audit, Networking and Security Institute*) es una institución con ánimo de lucro creada en 1989, que ha aportado un sinnúmero de proyectos e iniciativas en temas de Seguridad. En este caso presenta este documento: **Creating Your Own SIEM and Incident Response Toolkit Using Open Source Tools** (*Creación de tu propio SIEM y kit de herramientas para respuesta ante incidentes empleando herramientas de código abierto*), que creemos importante a ser evaluado para cualquiera que se plantee comenzar a trabajar con estas tecnologías.

Esta guía puede descargarse gratuitamente de:

https://www.sans.org/reading-room/whitepapers/incident/creating-siem-incident-response-toolkit-open-source-tools-33689

Webalizer

Webalizer es otra herramienta de análisis de Logs con licencia GNU, basada en interfaz Web de sencilla administración.

Puedes obtener toda la información y descargarla en:

http://www.webalizer.org

W3Perl

W3Perl es otra herramienta Open Source bajo licencia GPL que ofrece una interfaz gráfica amigable para analizar diferentes tipos de formatos de Logs.

Puede encontrarse en:

http://www.w3perl.com

LogAnalyzer

LogAnalyzer es otra herramienta gráfica que para los sistemas Linux es de libre descarga bajo licencia GPL.

Puede descargarse en:

http://loganalyzer.adiscon.com

Logcheck

Logcheck es una herramienta muy potente que opera a nivel línea de comandos, y se puede instalar en cualquier sistema Linux. Como buena herramienta de consola, su simplicidad nos ofrece un alto rendimiento y una muy buena parametrización, con lo que es ideal para quien desee investigar, analizar Logs y sobre todo dedicarle buen tiempo a su ajuste. Al instalarlo trae un conjunto de reglas pre configuradas, que son un gran apoyo inicial, pues descarta varios tipos de Logs que no suelen aportarnos información de interés.

Si se atreven a dedicarle su tiempo es una muy buena elección.

10.5. Tareas para el hogar (deberes).

Una vez más en este capítulo os propongo llevarnos algunas actividades o líneas de reflexión.

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cómo sincronizarías los tiempos de tus Logs?
2. En tus redes y sistemas, ¿has evaluado qué dispositivos NO pueden dejar de enviar Logs hacia un repositorio externo?
3. Los Logs de tu organización ¿Los empleas para supervisión y monitorización?, ¿Les sacas algún provecho en estos temas?
4. ¿Has profundizado en los estándares (RFCs) de syslog?
5. ¿Has podido ajustar facilidades y prioridades en el envío de tus Logs?
6. ¿Has instalado alguna herramienta para trabajar con Logs?
7. ¿Has logrado obtener información a través del cruce de diferentes tipos de Lgs?
8. El trabajo con Logs, ¿te ha reportado alguna acción de mejora en la seguridad de tus infraestructuras?

11. Juegos de Ciberguerra.

Resumen del tema

A comienzos del Siglo XIX, el Barón Von Reisswtz (*consejero de guerra prusiano*), concibió la idea de un juego en el que todas las actividades de campaña se representaran en un terreno figurado, empleando piezas miniaturizadas para representar las unidades.

El teniente George Heirich Von Reisswitz (*hijo del Barón*), hacia 1825 introdujo nuevas reglas, mapas topográficos y una representación del campo de batalla a escala. La victoria de Prusia sobre Francia en 1871 se atribuye, fundamentalmente, a la organización y educación superior de su Ejército, logrado mediante los juegos de guerra y las excursiones al campo de batalla.

Como éste, otros tantos triunfos obtenidos a lo largo de la historia de la humanidad por los Ejércitos sin experiencia de guerra previa, confirman que el adiestramiento y los ejercicios bien dirigidos durante la paz, preparan el camino de las victorias.

La doctrina militar ha avanzado mucho desde esas épocas en cuanto a la clasificación, la caracterización, la finalidad, lo diferentes tipos, etc. Pero en este texto nos centraremos exclusivamente en el concepto de "Juegos de guerra" por ser, tal vez una de las metodologías que más aplican al tema que en este texto nos reúne.

Como experiencia propia, debo poner de manifiesto, que cuando recién se comenzaba a emplear el correo electrónico a nivel mundial, en el Ejército Argentino Habíamos montado una plataforma importante, sustentada por nuestras propias redes y sistemas de comunicaciones. En el año 1996, realizamos una primera experiencia de "Juego de Guerra basado en herramientas informáticas", lo dirigió el Director del Estado Mayor del Ejército (*yo fui el coordinador del mismo*) y creo que fue una de los

detonantes de los mayores cambios de mentalidad y procedimientos de trabajo en redes que me tocó vivir hasta el año 2000. Luego de este primer ejercicio "Ciber militar" se llevaron a cabo varias más de los cuáles llegué a participar en dos más de ellos.

Tal cual se habló en la reunión de Ciberseguridad del mes de julio de este año en Israel, los juegos de "Ciberguerra" deberían ser una actividad frecuente en las grandes empresas.

11.1. Metodología de evaluación, auditoría y acción de mejora sobre un potencial incidente de Ciberseguridad.

El presente documento es una propuesta de actividad cuyo objetivo es:

1. Estudiar lo sucedido, acciones, respuesta e impacto que pudo haber ocasionado un incidente de seguridad.
2. Evaluar la situación en la que se encuentra la organización luego de ocurrido este incidente.
3. Observar si las diferentes áreas de la empresa, por su propia iniciativa, aplican acciones de mejora sobre experiencias sufridas.
4. Analizar si se ha aprendido algo al respecto o no.
5. Documentar detalladamente la respuesta típica ante este tipo de incidentes.
6. Determinar concretamente: hitos, acciones, medidas, respuestas, tiempos, documentación, responsabilidades, funciones, obligaciones, cadena de escalado y de respuesta, contactos con medios - fuerzas de seguridad y judiciales, capacidad de manejo de medios, eficiencia de las infraestructuras, capacidad de reacción y respuesta, mecanismos de control de incidentes, Resiliencia de la organización, costes e impacto sobre la operación, grado de madurez de los planes de continuidad de negocio y respuesta a incidentes, capacidad de

monitorización y supervisión de la red, seguridad perimetral, soporte técnico, etc.

7. Sobre una adecuada planificación de este desafío, y una vez obtenidos y analizados todos los resultados:
   - Poder preparar una verdadera "**Estrategia de respuesta a Ciberataques**" para toda la organización.

Para que este trabajo pueda ser aprovechado al máximo, se propone la ejecución de uno (o más) "**Juegos de Guerra**" (*componente de los denominados "Ejercicios militares"),* cumpliendo con todos los pasos que la doctrina militar establece para estos ejercicios, reflejando u orientando la misma a un "Ciberataque".

Finalidad de los Juegos de guerra.

a. Capacitar al personal de oficiales para la correcta aplicación de las técnicas de conducción del elemento que, por grado, le corresponda mandar y del inmediato superior, lograr el adiestramiento necesario para apreciar situaciones, adoptar resoluciones, impartir órdenes, y trabajar en equipo, o en el ámbito de la Plana Mayor o Estado Mayor.
b. Comprobar planes.
c. Para los juegos de guerra a un bando. Iniciar al personal de cuadros en las funciones que le corresponden como conductores de una determinada fracción. Es particularmente apto para la capacitación a nivel unidad y superiores.

Para que esto se pueda llevar a cabo de forma eficaz es condición indispensable que esté involucrado (y lo dirija) el más alto nivel de la organización.

11.2. Desarrollo, preparación y realización del Juego de Ciberguerra

Juego de Guerra: Incidente de Seguridad (*proponer un supuesto…).*

Grupo Telefónica: Ejercicio Nº 0xx.

Objeto del Ejercicio:

Situación inicial: Ciberataque sobre la infraestructura **a definir** (…….) de la empresa …….

Arquitectura y unidades involucradas: Elementos / áreas involucradas.

Doctrina: Normativa que regule los temas de seguridad, redes, incidencias, etc. de la organización.

Marco General: Intrusión de origen desconocido ha alcanzado la infraestructura ……. De la empresa …… el día "D" hora "H". (*una buena medida es lanzarlo sin ningún tipo de aviso previo).*

Elemento Inmediato Superior: Dirección de la organización.

Elemento de Trabajo: Nivel máximo de la organización que abarque todas las áreas participantes (*o aclarar si a su vez se involucran más. Áreas de igual o mayor jerarquía*).

Duración: "n" horas o días.

Aspectos fundamentales a considerar:

- La operación no puede sufrir ningún tipo de impacto.
- Las fases del ejercicio deben basarse en situaciones reales.

- Las acciones del juego de guerra serán tratadas por el personal responsable de cada área.
- Deberá realizarse con todo detalle la planificación de la operación para obtener los máximos resultados.
- …….

Factor de éxito: Sorpresa táctica (*total desconocimiento previo por parte de las áreas de la simulación*).

Conducción del Ejercicio:

- Director del Ejercicio: (Nombre)……..
- Subdirector y Conductor del ejercicio: (Nombre)……..

Puntos Principales a Considerar:

- Hitos y situaciones del mismo
- Cronología de situaciones
- Convocatoria, tiempo y capacidad de respuesta del comité de crisis
- Acciones y respuestas a cada situación
- Control de cada situación
- Medidas adoptadas
- Tipo de respuestas
- Tiempos de respuesta
- Documentación previa o generada antes, durante y posterior a cada situación
- Responsabilidades, funciones y obligaciones de las áreas y el personal involucrado
- Cadena de escalado y de respuesta

- Contactos con medios de difusión
- Capacidad de manejo de medios
- Control de la situación (Sobre la difusión de la información en medios)
- Contactos con fuerzas de seguridad y judiciales
- Gestión legal de la situación
- Eficiencia de las infraestructuras
- Capacidad de reacción y respuesta de las áreas técnicas y de gobierno
- Mecanismos de control de incidentes
- Resiliencia de la organización,
- Costes e impacto sobre la operación,
- Grado de madurez de los planes de continuidad de negocio y respuesta a incidentes
- Capacidad de monitorización y supervisión de la red,
- Seguridad perimetral,
- Soporte técnico en las diferentes situaciones
- Capacidad de resguardo y recuperación de infraestructuras
- Conducción del incidente

Metodología del Trabajo:

1. Etapa de preparación del ejercicio (20 a *30 días*).
2. Etapa de revisión y aprobaciones del mismo.
3. Prácticas con el personal participante en la dirección, supervisión, apoyo y árbitros.

4. Llegado el día del ejercicio, se distribuye todo el personal correspondiente en sus puestos de trabajo (*responsables de la ejecución, árbitros y personal de apoyo*).
5. Se plantea el incidente definido (*informando a la dirección que se trata de un ejercicio de simulación* donde se evaluará la respuesta real de sus áreas).
6. Se comienza a realizar y documentar las mediciones y observaciones de actividad.
7. Se van planteando una a una las situaciones planificadas. Cada una de ellas responde a:
    a. Un objetivo concreto.
    b. Una secuencia cronológica preestablecida y planificada.
    c. A sus respectivos parámetros de control y medición por parte de los árbitros.
    d. A los valores a documentar por cada árbitro.
    e. A la evaluación de la respuesta esperada.
    f. A la conducción hacia la siguiente situación.
    g. A un punto o acción de cierre de la misma y paso a la siguiente.
    h. Final y cierre del ejercicio.
8. Recolección y consolidación de resultados.
9. Análisis de los mismos.
10. Determinación de aciertos y errores.
11. Diseño de acciones de mejora.
12. Implantación de acciones de mejora.
13. Seguimiento de acciones de mejora.

Base para la **Estrategia de respuesta a Ciberataques** de la organización

11.3. Resumen de la doctrina militar sobre "Juegos de Guerra"

Concepto de "**Ejercicios militares**"

Los ejercicios constituyen una técnica de enseñanza de la didáctica militar, destinada a capacitar a los cuadros y conjuntos en la totalidad de las operaciones tácticas.

Su finalidad, es capacitar a los cuadros y conjuntos en todas las operaciones tácticas, con el propósito de:

a. Capacitar, ejercitar y comprobar al personal (cuadros y tropa) y organizaciones en el planeamiento, preparación y ejecución de las distintas operaciones militares, para el desempeño eficiente dentro del marco del conjunto.
b. Capacitar y comprobar al personal de cuadros en la conducción del elemento que le corresponde conducir, y del inmediato superior.
c. Obtener, como parte fundamental del Adiestramiento Operacional, eficiencia en la ejecución de las operaciones militares.

Por la clase de ejercicio, se clasifican en:

a. Explicación.
b. Juego de guerra.
c. Ejercicio de planeamiento.
d. Ejercicio de comando.
e. Ejercicio de cuadros.
f. Ejercicio de conjuntos.
g. Excursión.

Finalidad del Juego de guerra.

a. General.

   1) Capacitar al personal de oficiales para la correcta aplicación de las técnicas de conducción del elemento que, por grado, le corresponda mandar y del inmediato superior, y lograr el adiestramiento necesario para apreciar situaciones, adoptar resoluciones, impartir órdenes, y trabajar en equipo, o en el ámbito de la Plana Mayor o Estado Mayor.

   2) Capacitar al personal de suboficiales para la correcta aplicación de las técnicas de conducción del elemento que, por su grado, le corresponde mandar, y lograr el adiestramiento necesario para apreciar situaciones, adoptar resoluciones e impartir órdenes.

   3) Comprobar planes.

b. Para los juegos de guerra a un bando. Iniciar al personal de cuadros en las funciones que le corresponden como conductores de una determinada fracción. Es particularmente apto para la capacitación a nivel unidad y superiores.

c. Para los juegos de guerra a dos bandos. Poner a prueba la capacidad de resolución e independencia de juicio de los participantes.

Para la preparación de un ejercicio, se seguirán los pasos que se enuncian a continuación:

1) Paso previo. Estudio preliminar.

2) Paso I. Concretar la caracterización y el objeto del ejercicio.

3) Paso II. Estudio de la doctrina.

4) Paso III. Interpretación gráfica del objeto del ejercicio.

5) Paso IV. Determinación de los puntos principales a considerar. (PPC).

6) Paso V. Determinación de los motivos particulares de enseñanza. (MPE).

7) Paso VI. Concepción del ejercicio.

8) Paso VII. Selección general del lugar de realización.

9) Paso VIII. Completamiento tentativo de la situación inicial y desarrollo probable.

10) Paso IX. Reconocimiento del terreno o estudio de la carta.

11) Paso X. Conformación definitiva de la situación y desarrollo probable.

12) Paso XI. Elaboración del esquema en que se desarrollará la crítica.

13) Paso XII. Elaboración de las órdenes para el desarrollo.

14) Paso XIII. Revisión del ejercicio.

15) Paso XIV. Compaginación final.

Partes componentes de los Ejercicios.

Todo ejercicio está constituido por un número determinado de partes, cada una de las cuales satisface una finalidad parcial. El conjunto de las finalidades parciales conforma la finalidad didáctica del ejercicio. Por lo tanto, no podrá faltar ninguna de ellas (*Ver figura número 1*).

a. Los ejercicios contendrán las siguientes partes:

1) Bases.

2) Situación inicial.

3) Desarrollo probable.

4) Crítica o conclusión.

5) Órdenes para el desarrollo.

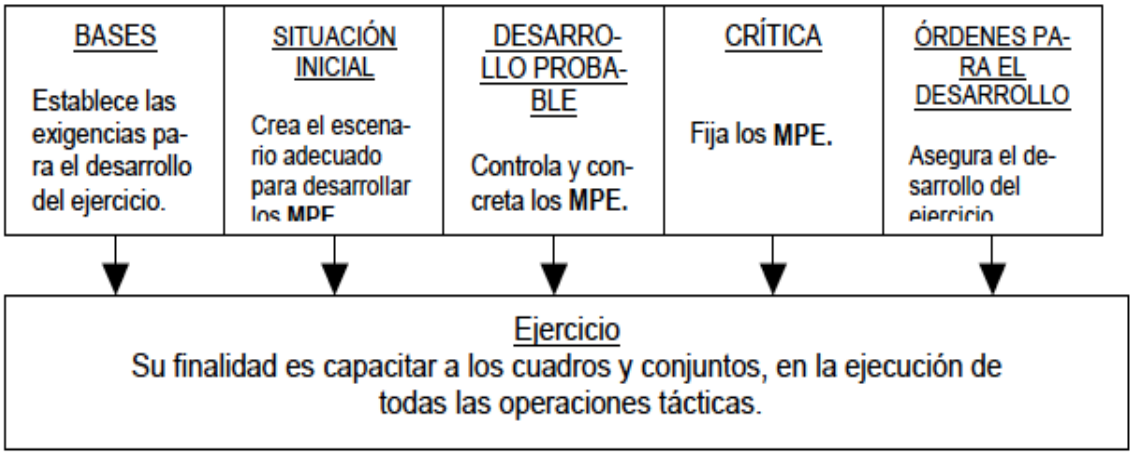


Figura número 1

b. Cada parte deberá estar perfectamente relacionada y coordinada con las demás, como lo representa la figura número 2. La inobservancia de lo mencionado producirá inconvenientes serios en el desarrollo del ejercicio, llegando a impedir la concreción de los motivos particulares de enseñanza.

c. Los ejercicios contendrán, únicamente, los documentos enunciados en el punto a. descartándose, en los de menor nivel, todo otro documento o aspecto que no haga a la presentación del mismo (antecedentes doctrinarios, bibliografía, etc.)

En el caso de los ejercicios desarrollados en el ámbito académico, las clases que contribuyan al desarrollo de los mismos, se realizarán previamente y con las formalidades de estas.

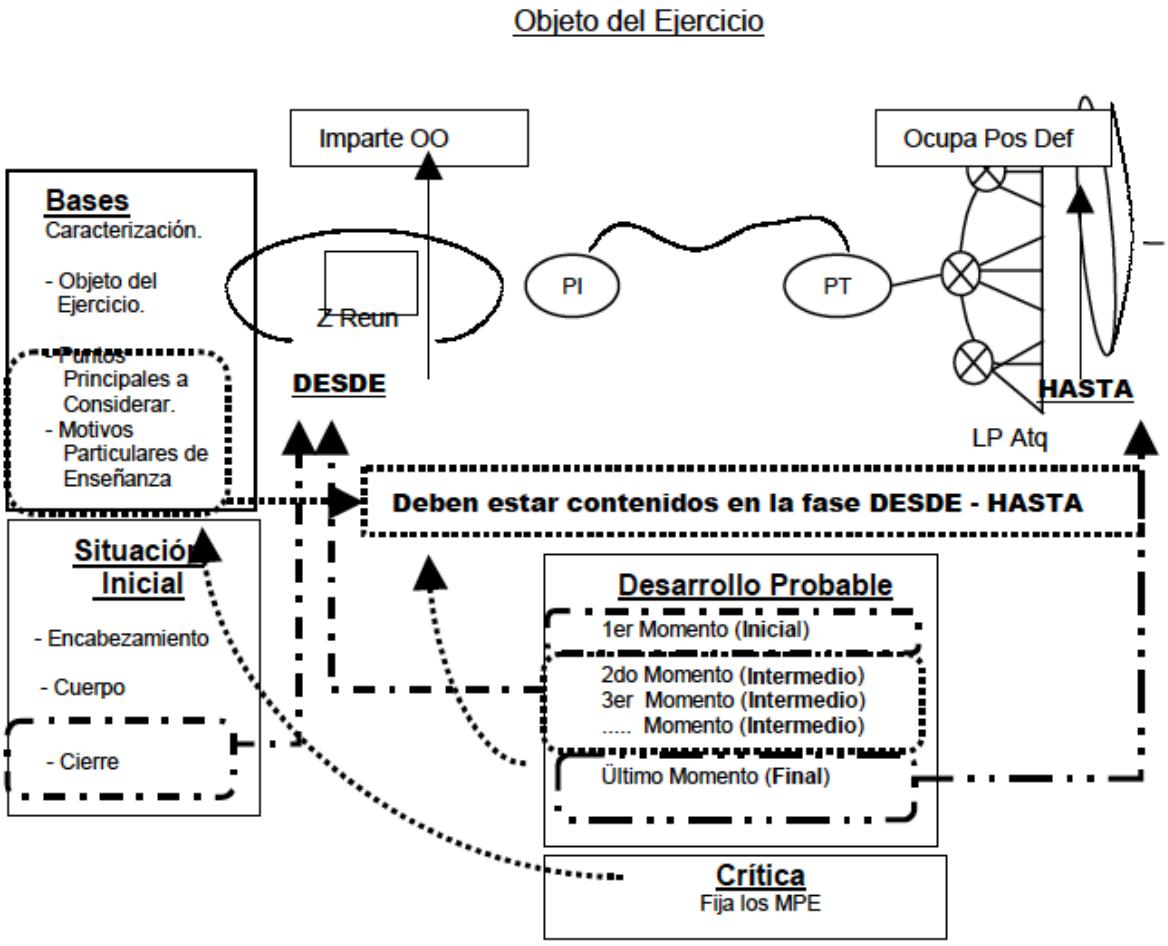


Fig Nro 2 - Relación entre las partes del ejercicio.

Bases del Ejercicio

a. Conceptos básicos (tipo de ejercicio, participantes, tiempos, lugar de desarrollo, operación táctica, actividades de cada fase (desde-hasta):PPC, motivos que dan origen al ejercicio.
b. Caracterización.
c. Objeto del ejercicio (OE)
d. Puntos principales a considerar (PPC)
e. Motivos particulares de enseñanza (MPE)

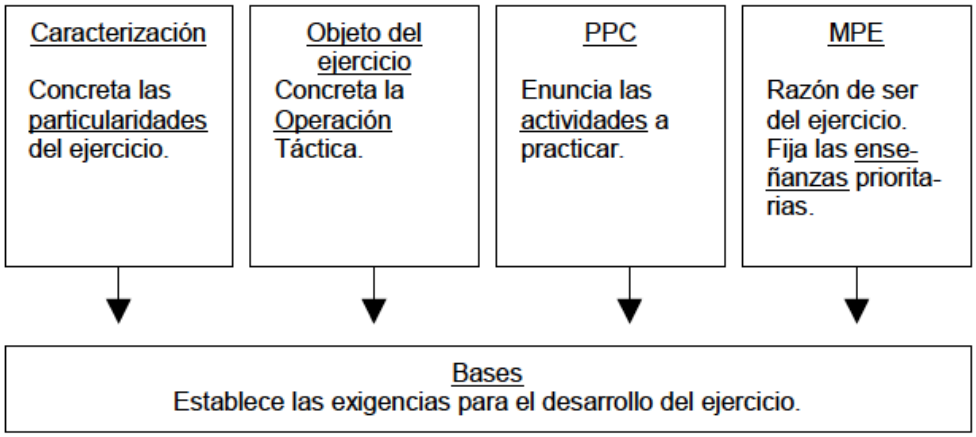


Fig Nro 3 - Finalidad de las Bases.

Situación inicial.

El esquema de la situación inicial comprenderá:

1) Encabezamiento.
2) Cuerpo (texto y notas).
3) Final.

Desarrollo probable.

a. Es la sucesión de situaciones coordinadas y relacionadas entre sí, con soluciones posibles, que tienen, por finalidad posibilitar la ejecución del ejercicio, su control y concreción de los motivos particulares de enseñanza.
b. Estas situaciones se presentan enmarcadas en "momentos del ejercicio". El momento comprende una visión integral de la presentación de un problema (situación a plantear) y de las acciones que se esperan por parte de los participantes para darle solución al mismo (finalidad o solución probable), ubicadas en un tiempo determinado (fecha y hora) y en un contexto preparado

para que se ejecute correctamente (árbitros, otros aspectos, etc.).

El primer momento siempre deberá coincidir con el desde y el último con el hasta, de la fase a desarrollar en el OE: Al último momento se lo denominará "de cierre".

c. Será en la concepción y desarrollo de los momentos donde se verá la creatividad y eficiencia del Director del Ejercicio para hacer "vivir la situación"

Órdenes para el desarrollo.

Deberá contener todas aquellas órdenes que el director de ejercicio considere necesarias impartir para asegurarse que el ejercicio se lleve a cabo sin inconvenientes. Deberán abarcar el antes, durante y después del ejercicio.

a. Fecha y hora de presentación.

b. Distribución de puestos.

c. Orientación topográfica.

d. Orientación táctica-topográfica.

e. Tareas previas.

f. Vestuario y equipo.

g. Medios auxiliares.

h. Previsiones de transporte.

i. Racionamiento.

j. Oportunidad y lugar de la crítica.

k. Etc.

Crítica.

a. Permitirá, mediante un análisis serio y detallado, la explotación del desarrollo apuntando los errores cometidos, afianzando las enseñanzas obtenidas y fijando los conocimientos, criterios y conceptos que asegurarán la eficiencia en combate. Se resaltará lo que hubiere sido bien ejecutado para estímulo y perfeccionamiento, y los errores para evitar su repetición.
b. Aun cuando la crítica deba hacerse apenas terminado el ejercicio, no significará que, necesariamente, se realice en forma inmediata y en condiciones que no favorezcan la finalidad didáctica y educativa.
c. Como lo expresa el Art 1.023; en este capítulo, se explicará las características particulares de la crítica, con la intervención directa de la totalidad del personal que participó del ejercicio.
    1) Se señalará, de acuerdo recibidas, lo que debía ejecutarse.
        a) Los Jefes de fracción expondrán las órdenes que recibieron y las que impartieron.
        b) Algunos soldados expondrán las órdenes recibidas.
        c) El director del ejercicio: evalúa y, de ser necesario, complementa o corrige algún aspecto. De ser necesario, señala alguno de los aspectos contenidos en la caracterización del ejercicio.
    2) Se establecerá qué sucedió:
        a) Los participantes señalarán qué sucedió durante el cumplimiento de las órdenes impartidas y recibidas (flujo de eventos), discutiendo los eventos y los resultados.
        b) El enemigo señalará los aspectos que, desde las posiciones ocupadas, pudieron observarse con relación a la fracción de trabajo, en forma simultánea al punto anterior.

c) El Director del Ejercicio aclarará, de ser necesario, la situación inicial ("lo que se quería hacer y de donde se partió"), participará del "análisis de lo realizado" y, en su carácter de experto, "fijará los motivos particulares de enseñanza", evaluando y relacionando lo realizado con los MPE.

3) Determinará que estuvo correcto e incorrecto:

a) Los participantes establecerán los puntos fuertes y débiles de sus desempeños.

b) El Director del Ejercicio guiará las discusiones, de tal forma que las conclusiones de los participantes sean doctrinariamente correctas, y que guarden relación con el Objeto del Ejercicio.

4) Determinará en qué forma deberá llevarse a cabo la tarea o actividad en el futuro:

a) Los participantes expondrán sus conclusiones sobre la forma en que deberán llevar a cabo las misiones / tareas que ejecutaron.

b) El Director del Ejercicio:

(1) Dirigirá al elemento de trabajo en la determinación de la forma en que deben llevarse a cabo las misiones / tareas que se ejecutaron.

(2) Destacará lo fundamental del ejercicio.

(3) Evaluará la actuación de los participantes.

(4) Motivará al personal en forma individual y orgánica.

12. Ciberdefensa: nuevos conceptos, nuevas metodologías, nuevos desafíos.

Resumen del tema

El objetivo de este último tema es consolidar la mayoría de los conceptos ya tratados anteriormente y reforzarlos con nuevas ideas.

Como se verá, en esta parte el desarrollo será eminentemente gráfico, para reforzar y cerrar conceptos de la forma más clara posible.

Por esta razón, la estructura de este final, es diferente al resto del libro, presentándolo de la siguiente forma.

- Conceptos ya difundidos:
  - Defensa en profundidad y en altura.
  - Dinámica de la defensa.
  - De "Proteger y proceder" a "Seguir y Perseguir" (**RFC-1244**).
  - Ciber operación de Acción retardante.

- Nuevos conceptos y desafíos:
  - Compartimentación de redes (la familia IEEE-802.x).
    - *Reducir superficie de ataque.*
    - *Arquitectura de red de confianza cero.*
    - *Organización por tecnologías.*
    - *Granularidad.*

- *Exfiltración de datos.*
- *Gestión de actualizaciones.*
- *Capacidad de reacción.*

- Ruido en la red.
- Resiliencia.
- Virtualización (de host y de redes).
- Delegación y segregación de responsabilidades y funciones.
- Contra inteligencia.
- Juegos de ciberguerra.

12.1. Presentación.

Nuestras infraestructuras de red y TI se nos están haciendo cada vez más "pesadas".

En los últimos años, día a día se van incrementando el nivel de actualizaciones, parches, dispositivos de seguridad, de detección, de monitorización, de prevención y detección de ataques, de antivirus, antiDDoS, antispam, antiphishing, anti…..

Llevando una vez más la seguridad informática al terreno militar, esto me hace acordar a las campañas de los grandes ejércitos de la historia, donde en virtud de los miles de combatientes, necesitaban una cantidad generalmente superior de infraestructura logística, de apoyo, de seguridad en sus puntos de conquista, de salvaguarda de sus fronteras y flancos, de fábricas y almacenes de material, de medios de transporte, etc. Me atrevería a afirmar que la totalidad de estos casos sucumbieron pues no podían soportar esta carga colateral a la acción de guerra en sí. Si se analiza la historia militar, detrás de todos ellos hubo verdaderos estrategas militares pero su ambición los llevó a los límites del concepto de "seguridad" y fueron siendo

derrotados por no ser capaces de mantener estas enormes infraestructuras de guerra.

Hoy nuestras infraestructuras de red y TI se nos presentan como algo similar. Nos encontramos batallando en esta Ciberguerra sobre un escenario sin fronteras, obligados a exponer cada vez más nuestros recursos, incorporando nuevos elementos, aplicaciones, protocolos de comunicaciones, información que en muchos casos no llegamos a conocer a fondo pues no damos abasto, dejando con ello cada vez más potenciales amenazas.

El Ciber enemigo opera como si fuera "guerrilla". No es un enemigo convencional, no le aplica ninguna de las leyes de esta guerra (leyes y regulaciones nacionales y/o internacionales). Nos ataca con "golpes de mano" precisos, no da la cara, tiene organización celular, está al margen de la ley, tiene muy fácil las medidas de velo y engaño, de enmascaramiento, de evasión y escape.

Nuestra estrategia de "Ciberdefensa" no puede seguir siendo la convencional o clásica, debemos operar dentro de la ley con: nuevos conceptos, nuevas metodologías, nuevos desafíos.

No profundizaremos más sobre conceptos que ya han sido presentados desde hace años, sólo los mencionaremos brevemente.

12.2. Nuestra visión del problema.

Vamos a comenzar el tema, definiendo la idea de "Redes, Nodos y Zonas".

- **Red**: medio físico que una 2 o más nodos (*cero saltos IP*).
- **Nodo**: Elemento direccionable por direccionamiento IP (*Posee 1 o más direcciones de igual o diferente tipo*).

Zona: Área que mantiene el mismo nivel de seguridad.

Sería positivo emplear rangos diferentes de IPs privadas:

10.x.x.x	= 2^{24} direcciones =	16.000.000 nodos
172.16/31.x.x	= 2^{20} direcciones =	1.000.000 nodos
192.168.x.x	= 2^{14}direcciones =	65.000 nodos

Redes

- Gestión
- Corporativa
- Servicios

Nodos

- Seguridad
- Servicio
- Pasarelas *(Unen zonas diferentes)*

Zonas

- Pública (DMZ)
- Militarizada (MZ)
- Interna (Core)
- Administración (Restringida)
- Intercambio de nivel de seguridad

Como detalle de la experiencia, es una muy buena práctica a la hora de diseñar redes, hacer uso de lo que nos establece la **RFC 1918** en cuanto a las direcciones IP privadas.

Si es posible, se pueden asignar diferentes rangos basados en alguna cierta lógica como puede ser a título de ejemplo:

10.0-7.x.x/11 zona central,

10.8-15.x.x/11 zona A,

10.16-23.x.x/11 zona B,

10.24-31.x.x/11 zona C

……..

10.128-135.x.x/11 zona N,

etc…

Para los enlaces punto a punto, o punto multipunto, entre estas zonas hacer uso de otro rango, por ejemplo:

192.168.0-7.x/19 para enlaces de la zona central,

192.168.8-15.x/19 para enlaces de la zona A,

192.168.16-23.x/19 para enlaces de la zona B,

192.168.24-31.x/19 para enlaces de la zona C,

……

192.168.128-135.x/19 para enlaces de la zona N,

etc…

Se puede dejar el rango 172.16-31.x.x para cualquier otra red "especial" que deseemos.

Esta asignación de direccionamiento IP, desde el punto de vista de seguridad es muy importante, pues a medida que el trabajo en la red se va haciendo cotidiano, es muy fácil identificar cualquier dirección IP, con una región geográfica, un edificio, una planta del mismo, un área de trabajo, etc. Si consideramos este detalle, cuando se deba analizar tráfico, reglas de un FW, configuración de rutas, listas de control de acceso, etc. Cualquier decisión que se tome al respecto será mucho más sencilla, clara y finalmente segura.

Volviendo a nuestros conceptos de "defensa en profundidad" presentados en el capítulo 4, retomamos a continuación la imagen de zonas de red, en la cual representamos, las diferentes "líneas defensivas" y genéricamente los dispositivos que nos proporcionan la información y las comunicaciones necesarias para el funcionamiento de las infraestructuras.

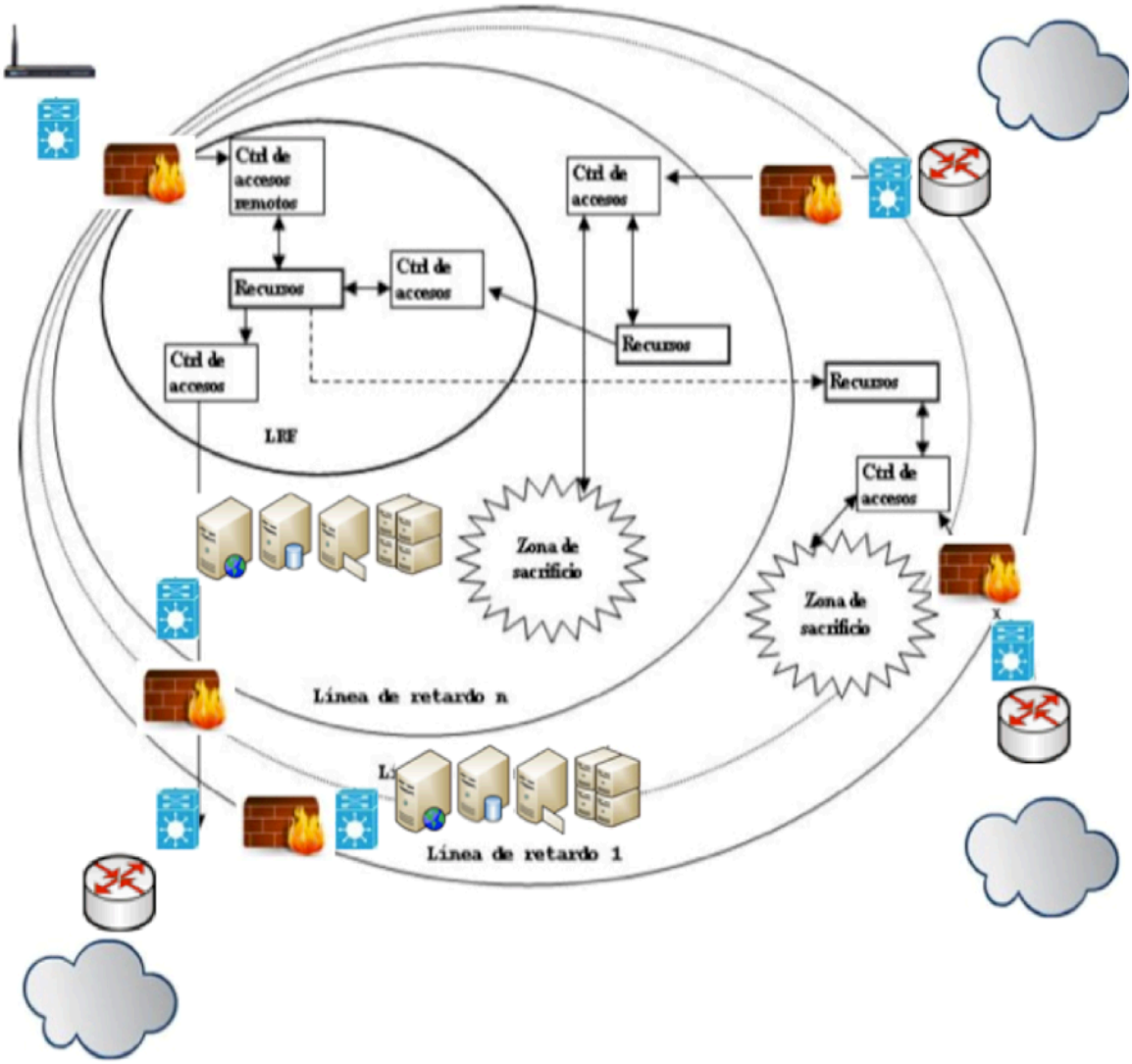


Imagen de zonas de red

Si sobre la imagen anterior, deseamos continuar el nivel de detalle, la realidad es que cada uno de estos dispositivos y/o zonas de red, se comunican a través de "**medios físicos**". Un medio físico, como su palabra lo indica es algo "tangible" que permite el tránsito de la información, dependiendo de las características físicas de este medio, la información viajará por medio de una señal óptica o electromagnética. En la actualidad sólo existen los siguientes medios físicos:

- Cable (*UTP, STP, Coaxial, etc.).*

- Fibra óptica (*monomodo y multimodo*).
- Radio (Microondas, satélite, radioenlaces, LF, HF, VHF, etc.)
- Guías de onda (*en general sólo empleadas en laboratorio o dentro de los sistemas de antena*).

Para profundizar sobre cualquiera de ellas, aconsejamos la lectura del capítulo 3 del libro "**Seguridad por Niveles**".

En definitiva, estos medios físicos, interconectarán los dispositivos, bajo tres tipos posibles:

- Punto a punto.
- Punto a multipunto.
- Multipunto a multipunto.

Estas conexiones llevadas al plano real, las veríamos tal cual se presentan en la imagen siguiente.

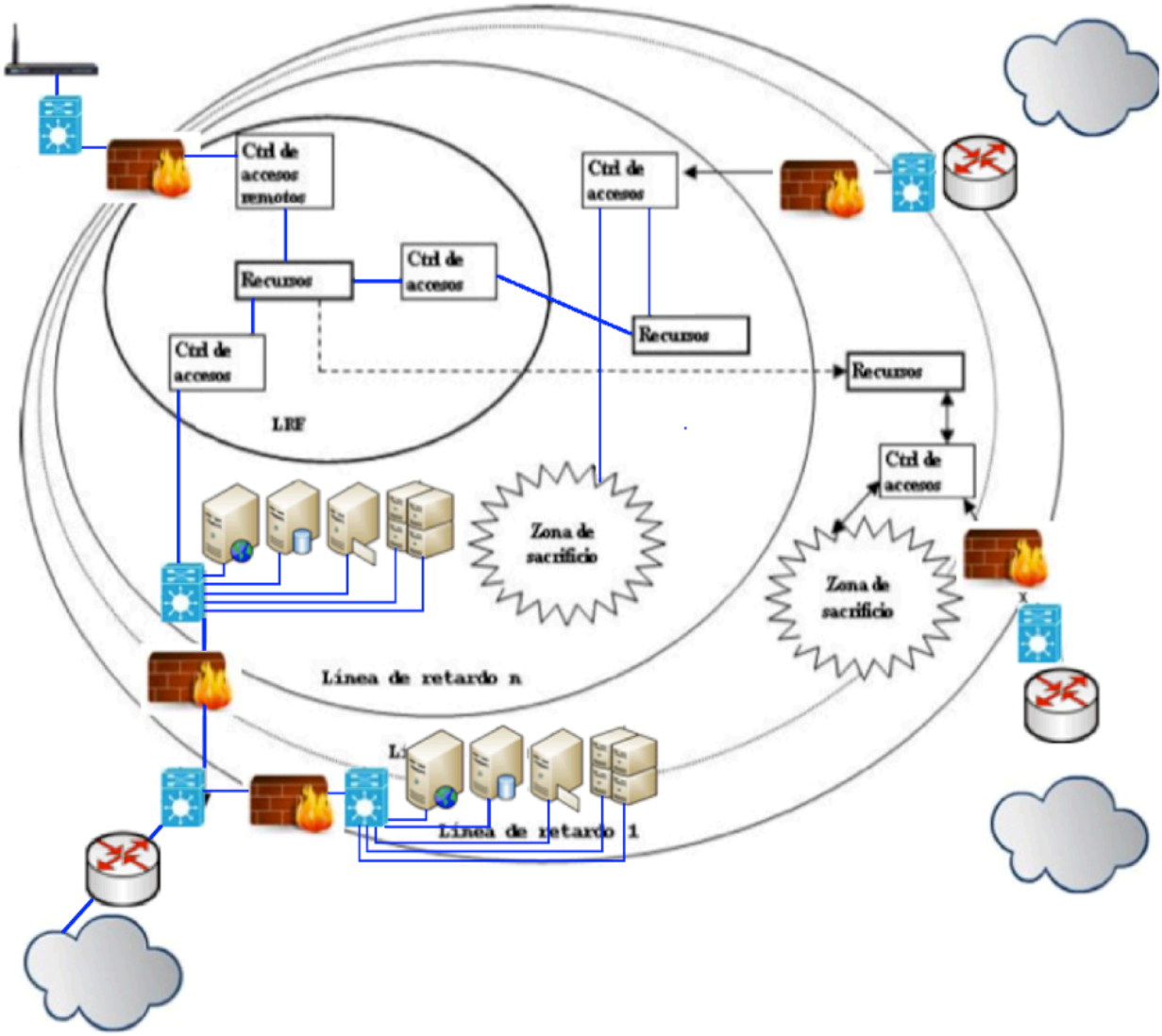


Imagen de conectividad a nivel físico

Siguiendo con nuestra "consolidación" de conceptos, si recordamos lo tratado en el capítulo **5. Ciberdefensa en profundidad y en altura** (la conquista de las cumbres) de este libro, el tema se encontraba dividido en dos líneas de avance:

1) Planos de altura (niveles TCP/IP)

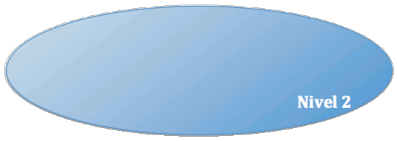
2) Planos de Segmentación en redes de: Gestión y Servicio.

Los niveles del modelo TCP/IP, una vez más, si los graficamos desde la realidad de nuestras redes, en definitiva, van asociados directamente con los dispositivos que empleamos en ellas. Como siempre hacemos

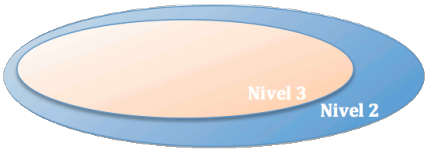
mención, en virtud de la potencia de la electrónica actual los diferentes dispositivos, van asumiendo cada vez más funcionalidades, ocupando "capas" que no fueron su función original, por lo tano podemos discutir si hoy en día es taxativamente así, pero si somos rigurosos conceptualmente, en concreto la relación nivel/dispositivo es:

- **Nivel 2**: Switchs. 

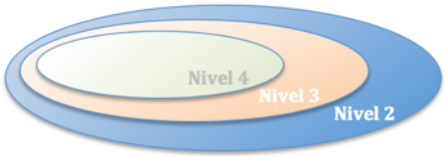
  Podemos representarlos también como si fuera una "carta topográfica", en la cual por medio de "curvas de nivel, se representan las diferentes cotas de altura, por ejemplo, de la siguiente forma:

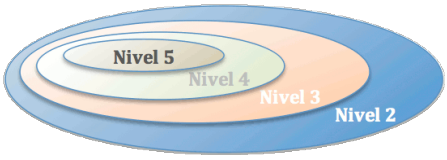
- **Nivel 3**: Routers. 

  Idem anterior: 

- **Nivel 4**: Firewalls. 

  Idem anterior: 

- **Nivel 5**: Servidores. 

  Idem anterior: 

Ahora, si queremos reflejar este tipo de representación, podemos hacerlo de acuerdo a la imagen que sigue.

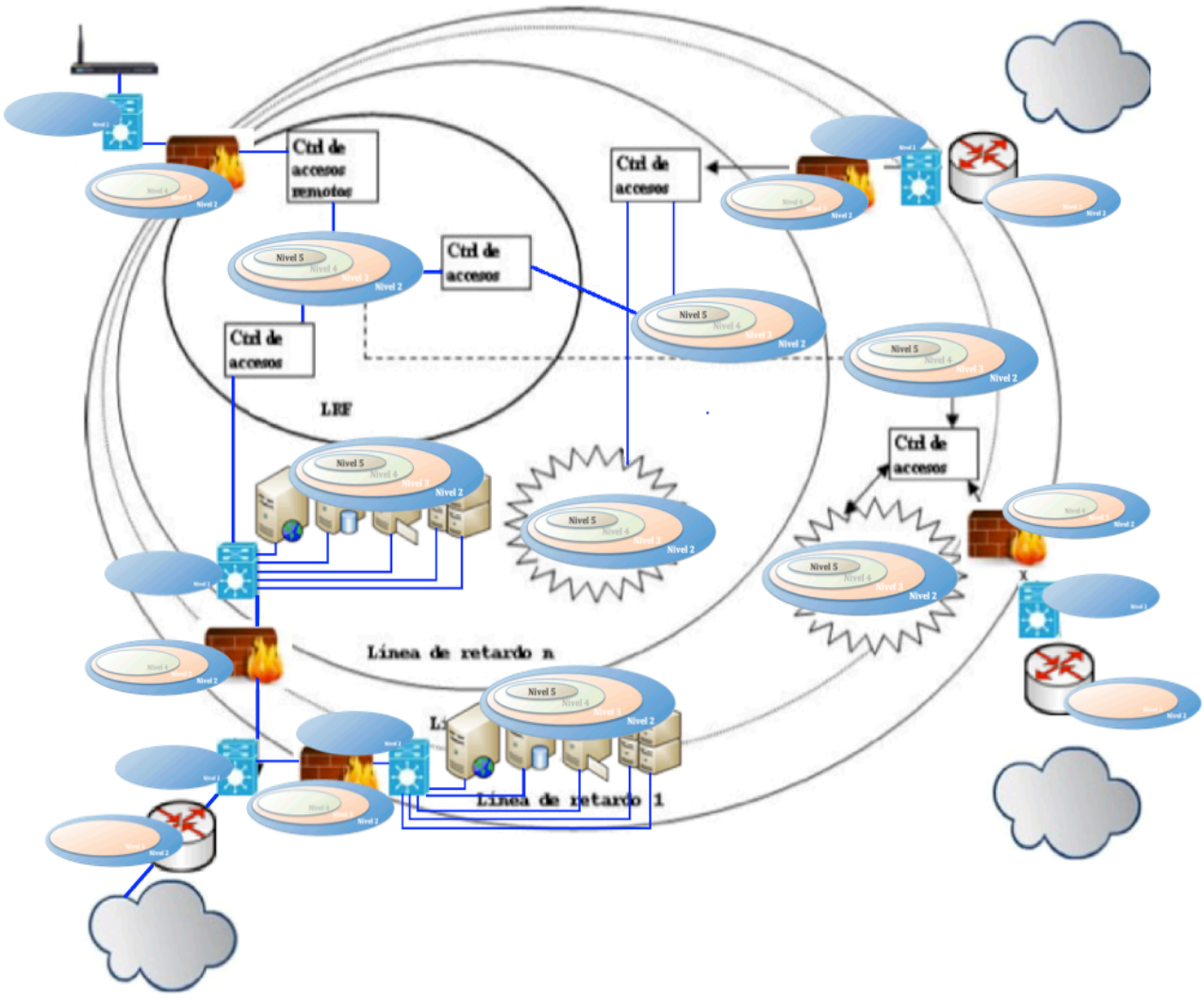


Imagen de planos de altura según niveles TCP/IP

Si avanzamos sobre esta misma imagen, pero sumándole ahora los "Planos de Segmentación en redes de Gestión y Servicio", tal cual acabamos de recordar de este capítulo 5, podríamos presentarlo de acuerdo a la imagen que se ve a continuación.

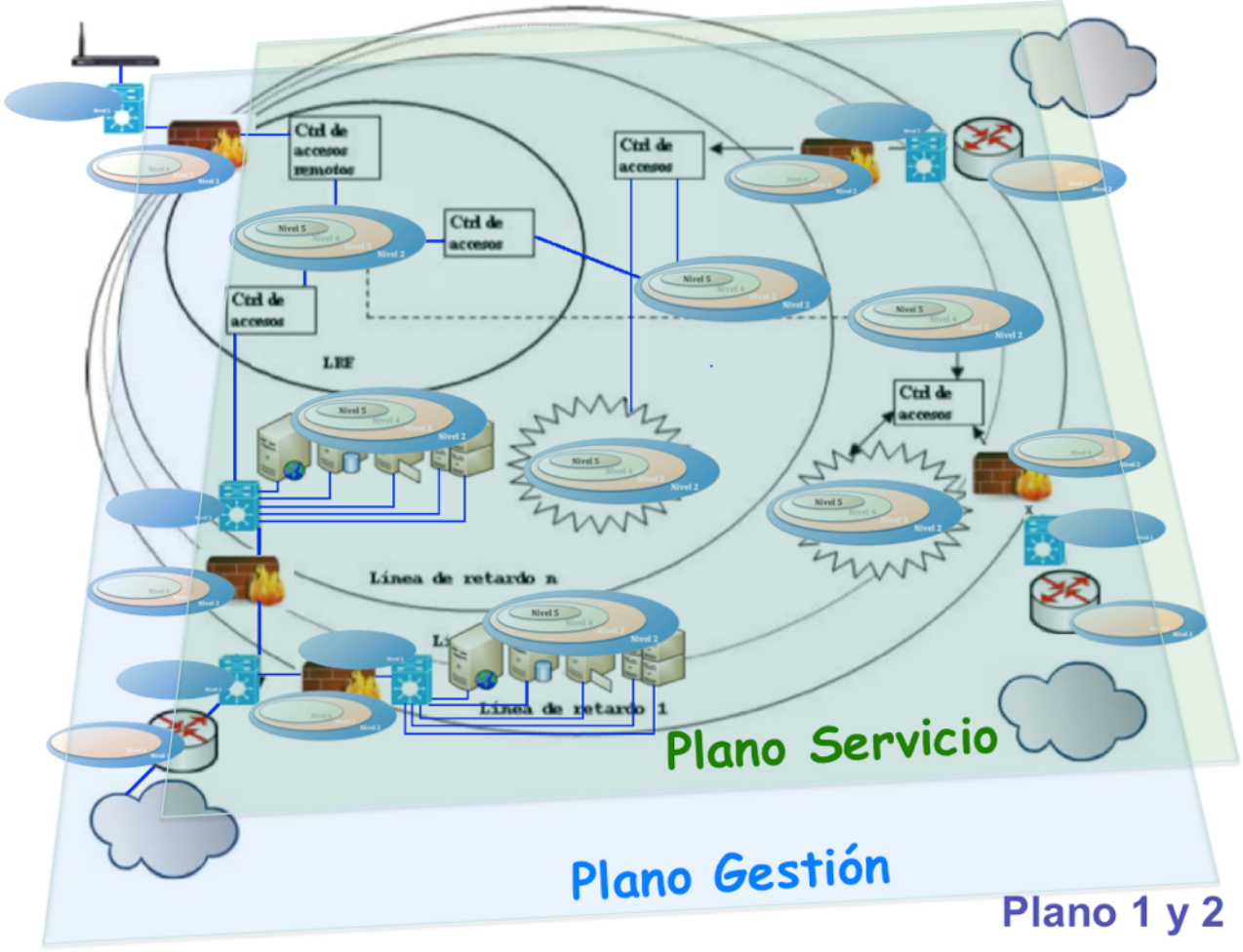


Imagen de planos de altura según redes de "Gestión" y "Servicio"

Con las dos imágenes anteriores tenemos una visión clara y representativa de cómo podemos tratar y definir las diferentes "alturas" desde el punto de vista de la seguridad de nuestras infraestructuras.

Si seguimos desarrollando gráficamente los conceptos de los capítulos anteriores, podemos presentar lo tratado en el capítulo **4. Estrategias de Ciberseguridad en grandes redes** (Seguir y perseguir - proteger y proceder).

Supongamos inicialmente un "vector de ataque" (*que en la gráfica que sigue, lo podemos ver en el extremo inferior izquierdo*). Cuando nuestra infraestructura y recursos humanos no están lo suficientemente preparados, debemos plantearnos la estrategia de "Proteger y proceder", tal cual se representa en la imagen, lo único que podríamos hacer es ir desconectando enlaces (en color rojo) y apagando dispositivos (también en rojo). Recordemos (o repasemos) lo presentado en el punto **4.1. Planteo inicial** de este libro.

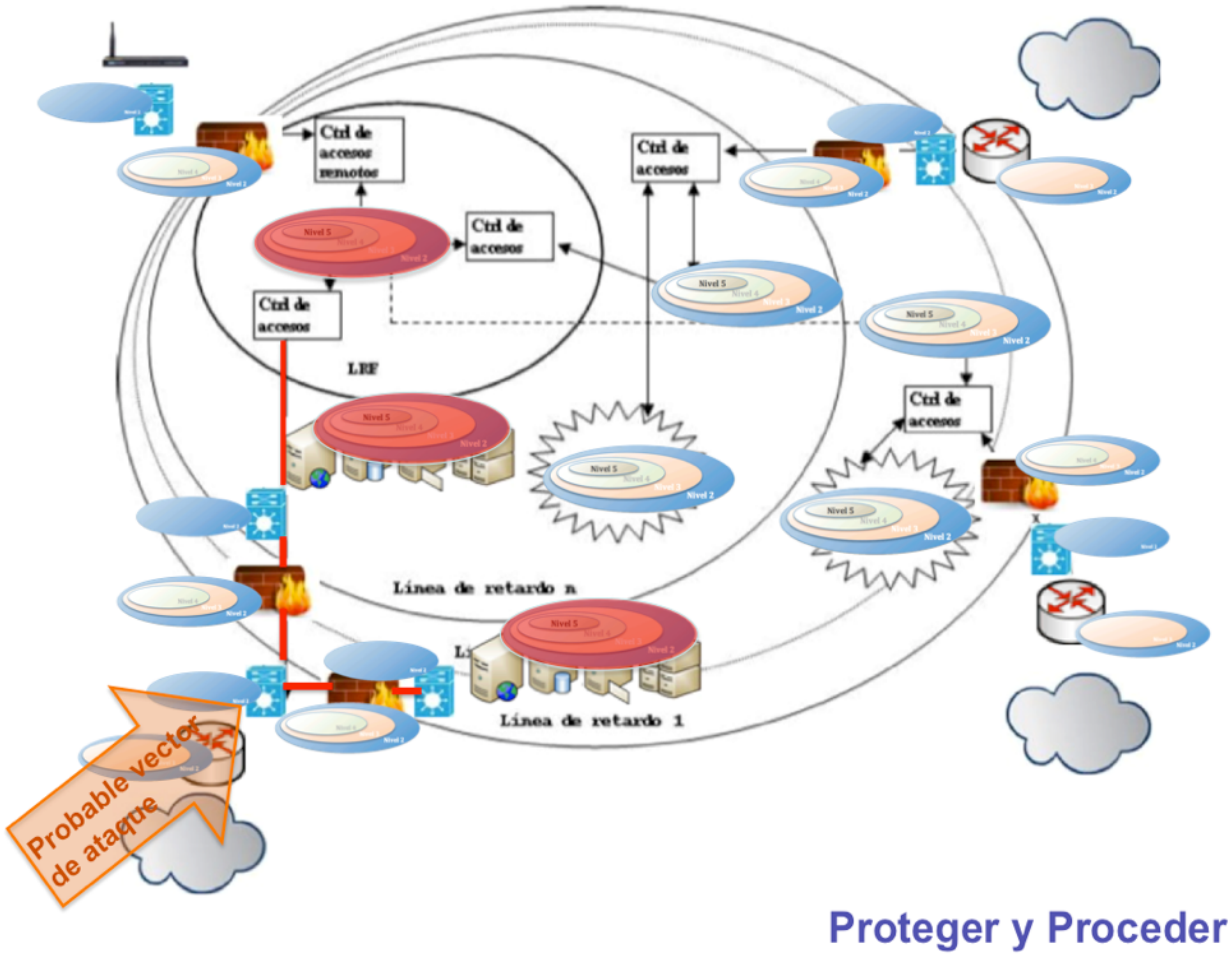


Imagen vector de ataque 1, Proteger y Proceder

Manteniendo los conceptos del capítulo 4, supongamos ahora otro vector de ataque (*que en la gráfica que sigue, lo podemos ver en el extremo inferior derecho*). Cuando nuestra infraestructura y recursos

humanos ***sí*** están lo suficientemente preparados, podemos entonces plantearnos la estrategia de "Seguir y perseguir". A través de esta postura, como ya mencionamos, podremos **llegar a la raíz del problema** y operando adecuadamente erradicarlo definitivamente.

Si hemos trabajado en cada uno de los niveles, nuestra respuesta podrá ser también en cada uno de ellos y estaremos en capacidad de "Monitorizar", "Mantener", "Almacenar datos", "Prevenir", "Evaluar", "Decidir" y hasta adoptar "Contramedidas" generando nuevas reglas en los FWs, Routers, y sistemas AntiDDoS, instalando nuevos parches y actualizaciones de seguridad, y finamente adoptando todo el conjunto de medidas que haga falta.

Esta metodología de gestión de incidentes es la que se representa en la imagen que sigue.

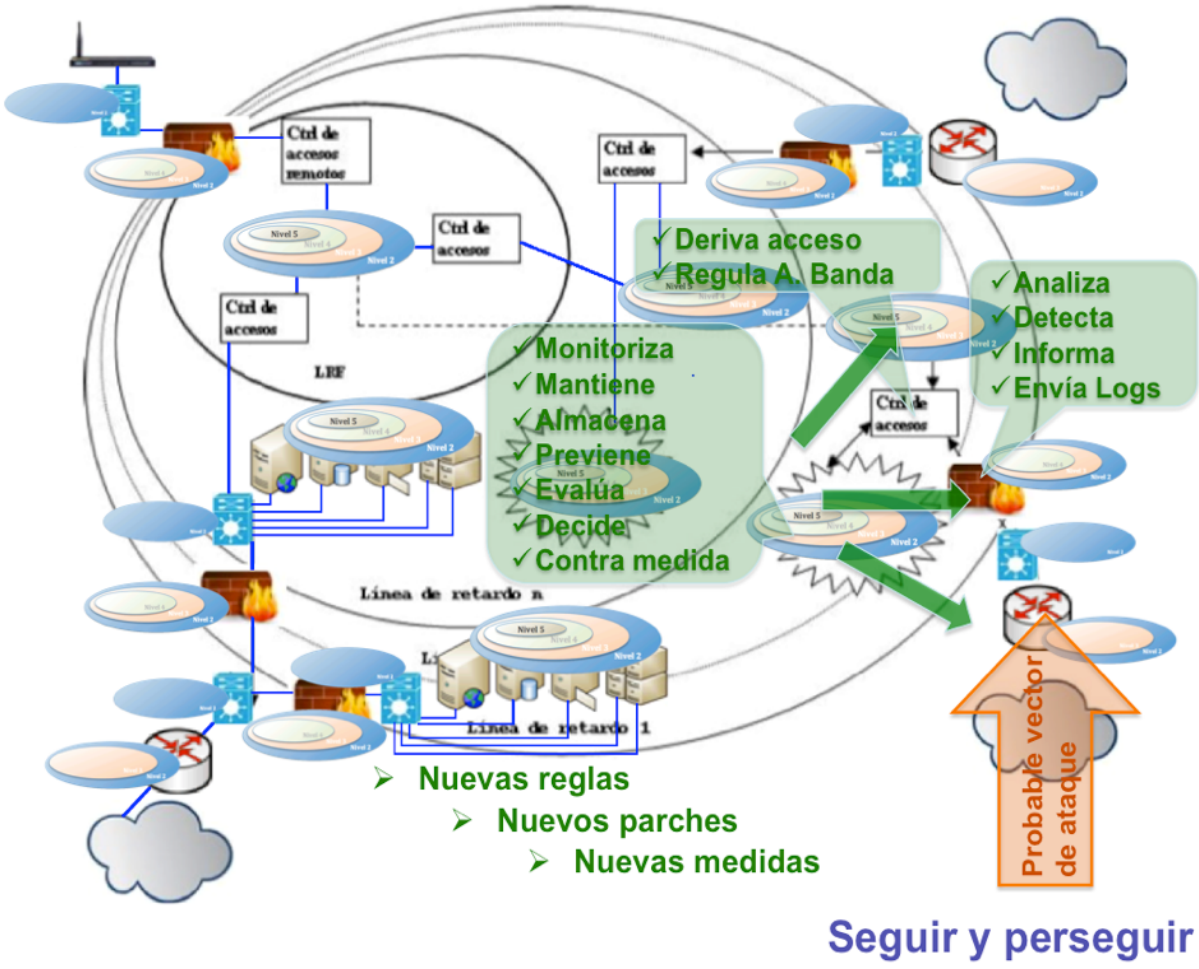


Imagen vector de ataque 2, Seguir y perseguir

En las dos imágenes que siguen, solamente se representan ambos escenarios y, con la intención de hacer repaso de conceptos, se hace hincapié en los conceptos fundamentales que nos pueden llevar a adoptar una u otra estrategia.

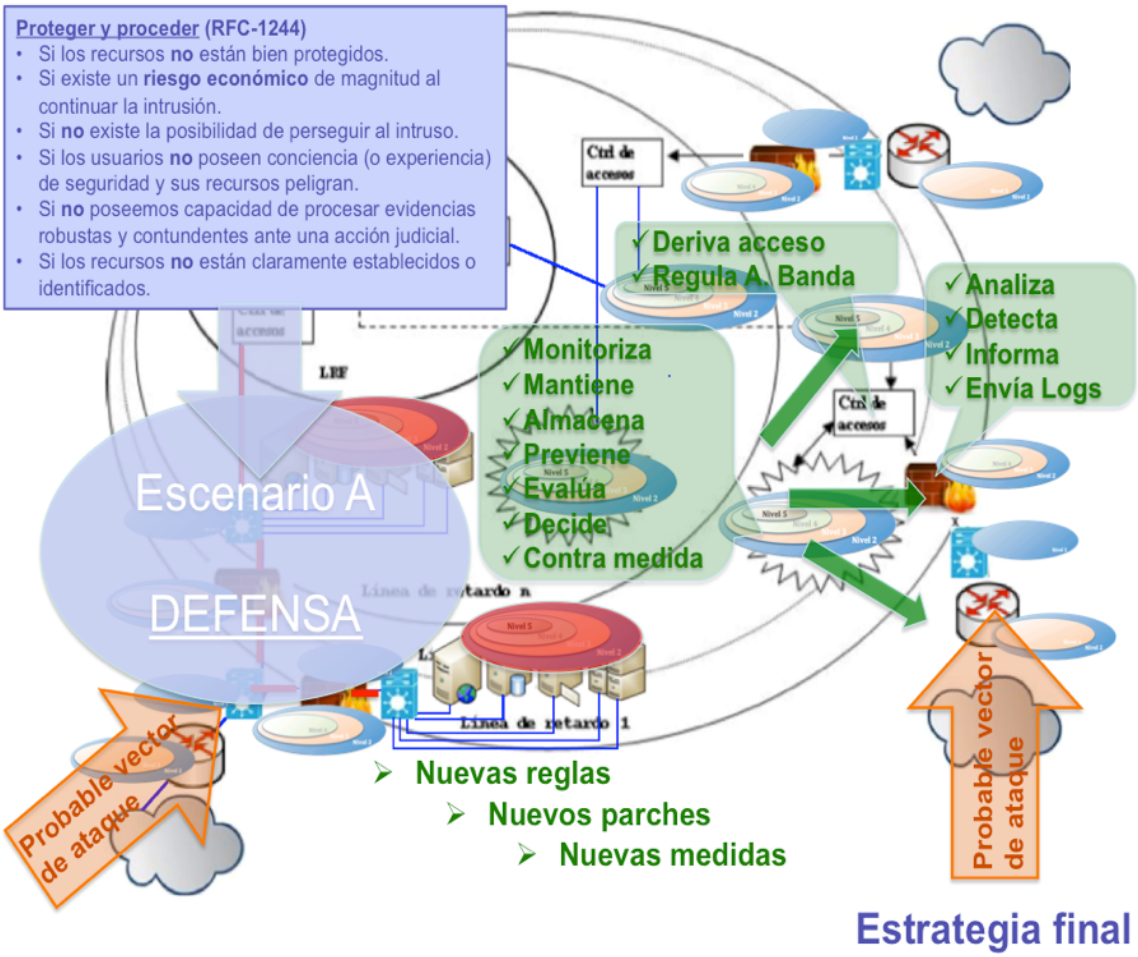


Imagen vector de ataque 1, conceptos de Proteger y Proceder

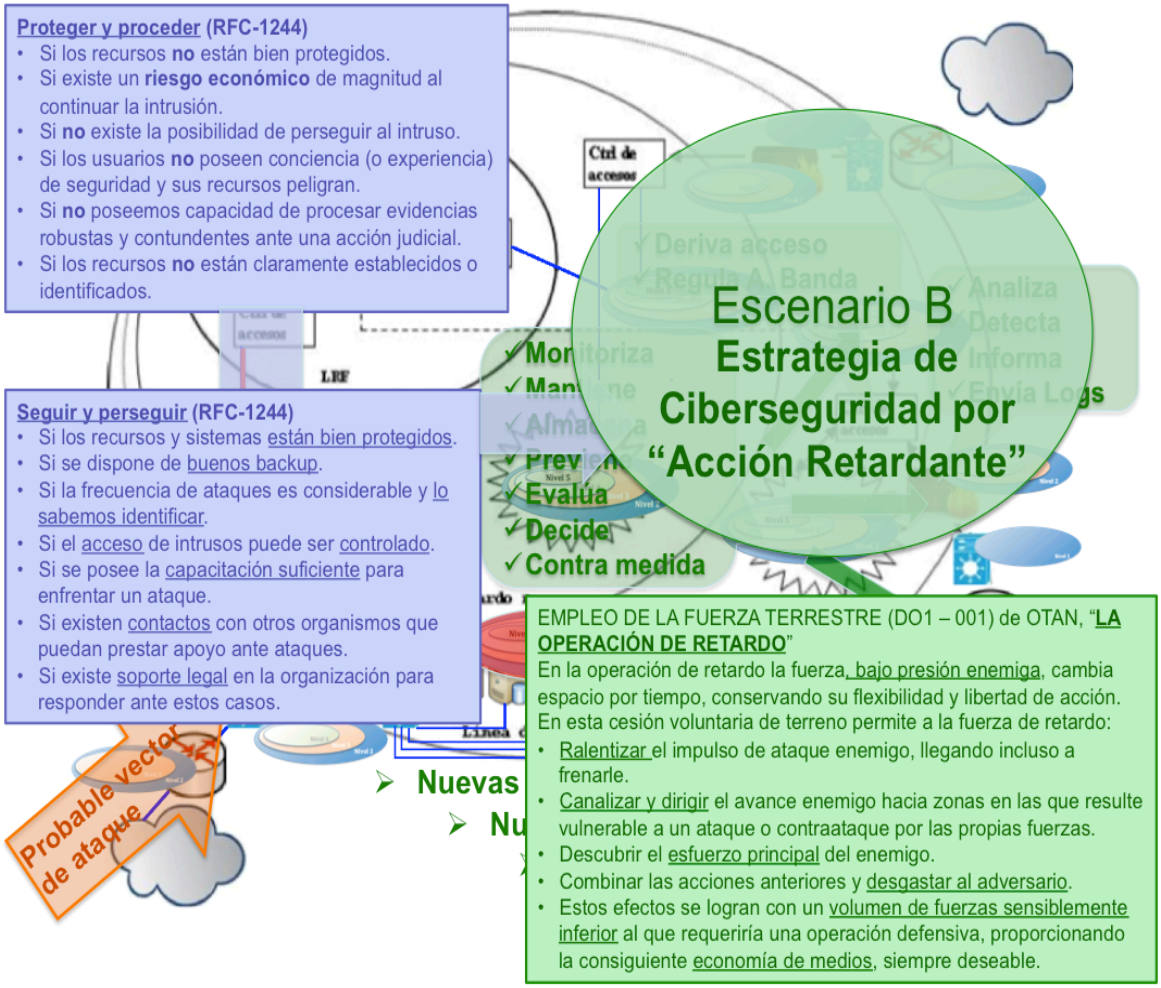


Imagen vector de ataque 2, conceptos de Seguir y perseguir

12.3. Análisis por zonas.

Considerando los conceptos del inicio de este capítulo "Redes, Nodos y Zonas", vamos a avanzar con más detalle sobre las diferentes "Zonas" que podemos considerar en nuestras redes.

Hasta ahora siempre nos hemos basado en nuestro modelo de "defensa en profundidad" sobre una arquitectura de rede tipo "capas de cebolla", en la cual a medida que profundizamos hacia el corazón de nuestra arquitectura vamos incorporando mayores exigencias de seguridad. Esta postura implica que SIEMPRE que deba decidir sobre la ubicación de cualquier tipo de dispositivos, deba evaluar su función y

los servicios que vaya a prestar, sobre esta base, definir las exigencias a las que se le someterá desde el punto de vista de la seguridad, y finalmente, en la medida que cumpla o no cada una de ellas, se le deberá asignar un "rating" o un valor que le permitirá o no estar conectado (o ser visible o alcanzable) desde una zona un otra.

Este conjunto de medidas y acciones es lo que dará origen a un verdadero plan de "Segmentación de redes". Si se desea profundizar en este tema, aconsejamos deis una mirada a un artículo que está publicado en Internet desde hace varios años "**Matriz de Estado de Seguridad**" (http://darfe.es/joomla/index.php/descargas/summary/5-seguridad/43-matriz-de-estado-de-seguridad).

Si hemos logrado valorar el nivel de seguridad de nuestros dispositivos y podemos identificar claramente en cuál de las zonas de nuestra red puede o no puede ser conectado, evidentemente nos surgirá necesidad de implementar medidas, interfaces o dispositivos que "permitan" o "nieguen" la visibilidad para cada IP/puerto de cada uno de los elementos de todas las zonas.

Estas interfaces o puntos de comunicación entre zonas de diferentes niveles de seguridad, en definitiva, terminarán siendo "interfaces" que se encuentran física o virtualmente uniendo zonas. Esto es lo que denominaremos "**Zonas de intercambio de Niveles de Seguridad**", y es importante que las visualicemos como "Zonas". En la realidad serán routers, firewalls, VPNs, host con más de una interfaz de red, conexiones dentro de un VMCenter, etc. Pero insistimos, veámosla SIEMPRE como "**Zonas**" para que quede claro que, en ese tramo de cable, en las bocas de ese switch, entre las interfaces de ese router, o dentro de ese "rack" de comunicaciones existe una "Zona" en la cual podemos "regular" el paso entre dos niveles de seguridad diferentes.

De forma gráfica, podemos representarla, por ejemplo, como la imagen que sigue.

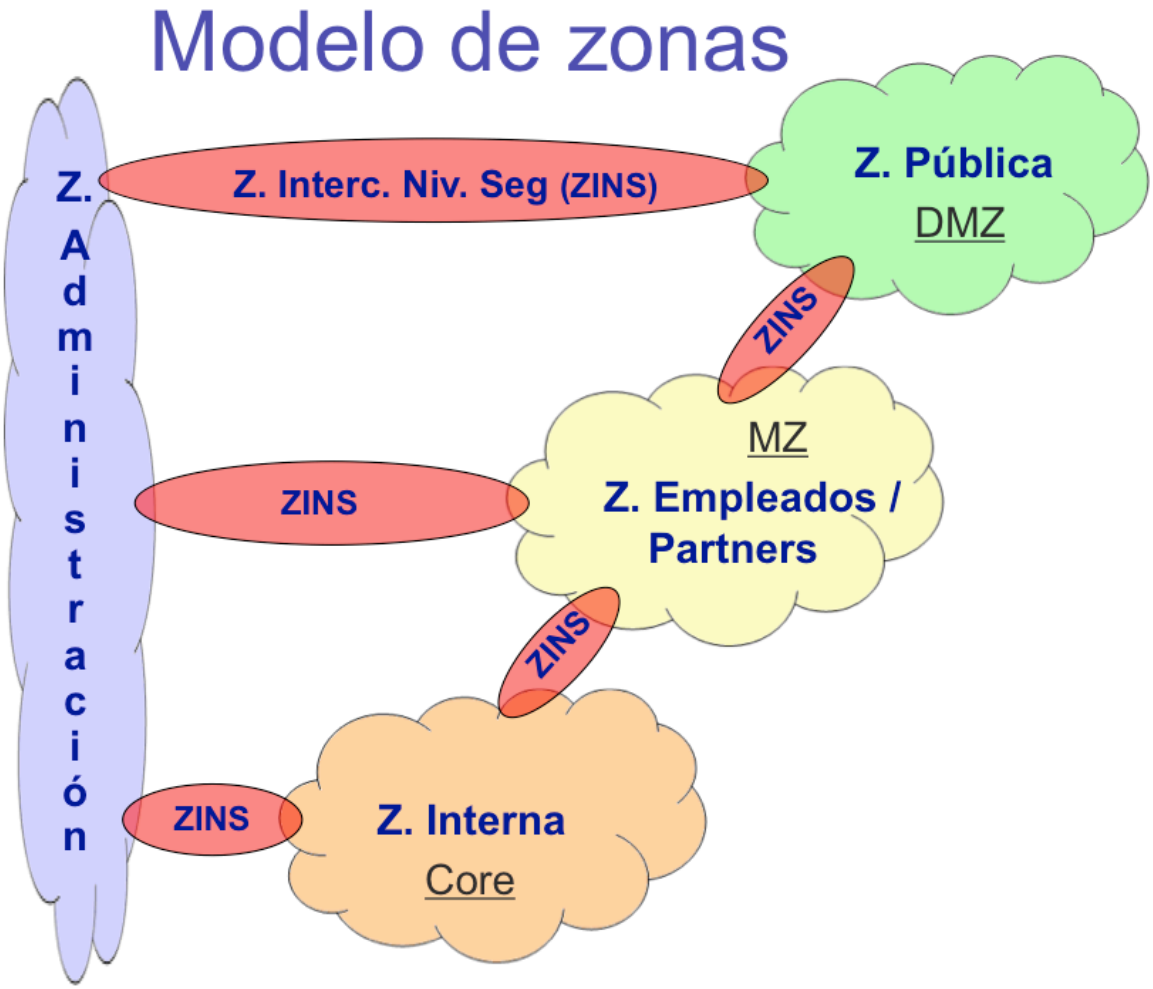


Imagen modelo de zonas

Si tenemos claro la función y los servicios que ofrecen los dispositivos y plataformas de cada una de esas zonas, entonces podemos aplicar una buena política de "Autenticación" y "Gestión de Accesos", para definir con total claridad los usuarios, roles y grupos que podrán o no acceder a cada una de ellas.

La imagen que sigue, es un ejemplo de cómo podríamos representar este control de accesos.

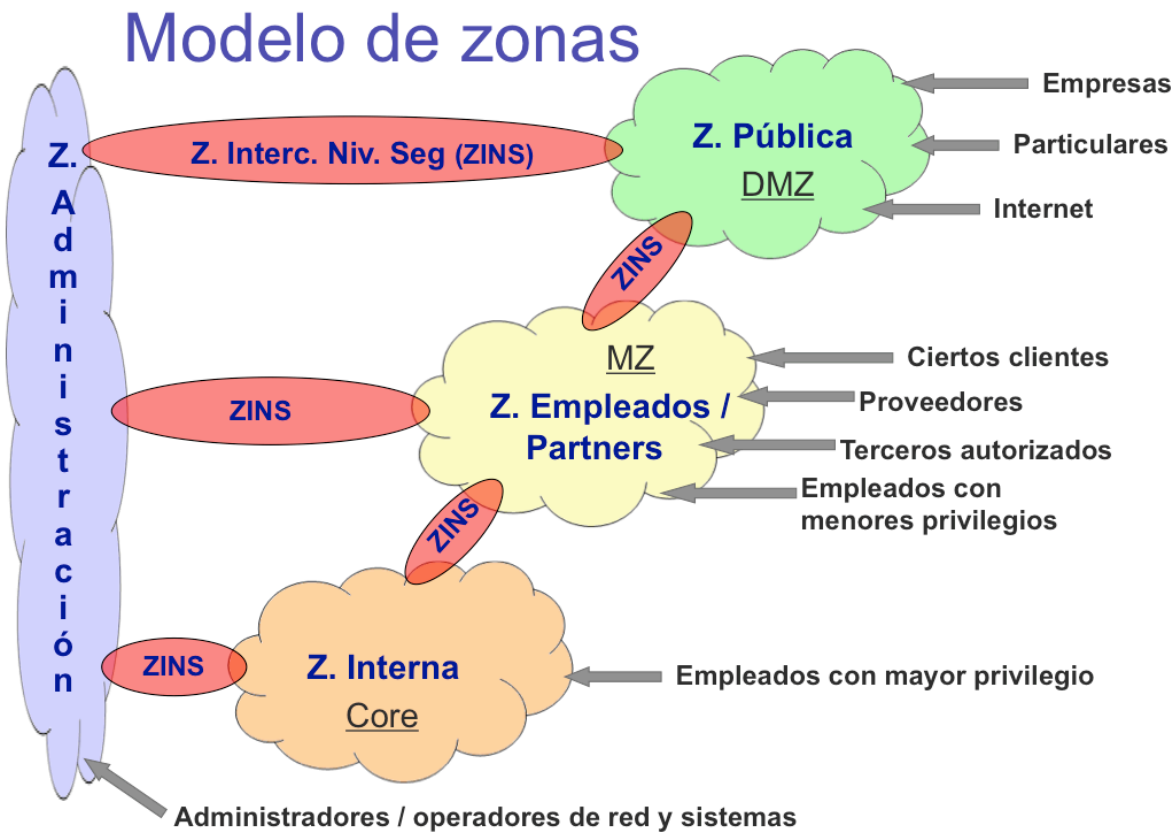


Imagen modelo de zonas y gestión de accesos

A medida que nuestra infraestructura va creciendo y avanzando en su ciclo de vida, como es normal en todo sistema, comienza a degradarse, desde el punto de vista de seguridad esto es sumamente peligros pues estaremos ofreciendo cada vez más "flancos" o puntos débiles.

Un concepto interesante a tener en cuenta es el de "**Reducir la superficie de ataque**".

Este concepto que nos parece natural, es antiquísimo, es lo que hacían las legiones romanas con su formación en "tortuga", compactando la formación y protegiendo con sus escudos cuadrados el frente, flancos, retaguardia y altura como si fuera una caja rectangular que avanzaba inmune a lanzas y flechas. Es lo que se hacía en los castillos medievales, cerrando su perímetro, sin dejar aberturas innecesarias. Es lo que haríamos en cualquier casa cuando salimos de vacaciones.

Para nuestras infraestructuras, implica no ofrecer servicios innecesarios, cerrar o deshabilitar puertos y protocolos que no se usan, "homogeneizar" plataformas, SSOO, servicios y aplicaciones. No dejar configuraciones por defecto o temporales, limitar accesos a que los necesite, mantener una buena política de borrado y modificación de usuarios y privilegios, Evitar obsolescencia de hardware y/o software. No emplear protocolos inseguros, mantener una seria política de parcheado y actualizaciones, concienciar al personal, etc.

Podemos representar estos conceptos como se puede ver a continuación.

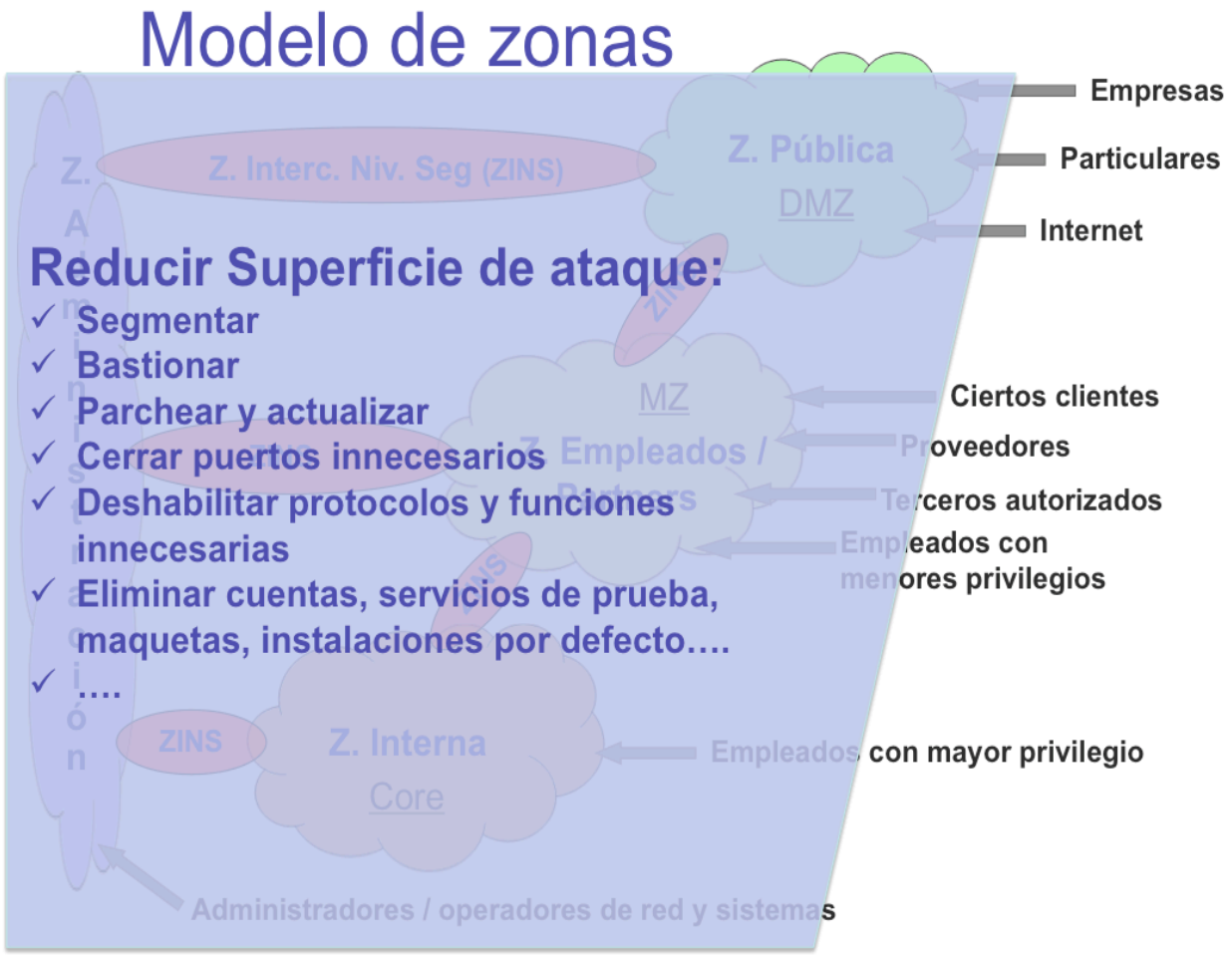


Imagen reducción superficie de ataque

12.4. Nuevos desafíos.

Todo este conjunto de medidas que venimos describiendo, nos obligan a ser "proactivos", a innovar día a día en nuestro trabajo, a investigar novedades que aparecen en la red.

En esta sección vamos a presentar algunas medidas técnicas que nos ofrece la tecnología actual, las cuáles pueden mejorar substancialmente nuestra arquitectura de ciberseguridad.

12.4.1. Protocolo 802.1x

El resumen de este protocolo, podríamos definirlo como: Autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP) que regula la **RFC 3748**.

802.1x es una norma para incrementar el control de accesos. Básicamente propone un dispositivo que hace las veces de "puerta de acceso" que por defecto está siempre cerrada, al hacerse presente un elemento que desea acceder (*suplicante*), el dispositivo que recibe esta petición (y que reiteramos, tiene su puerta cerrada), realiza las veces de "pasarela" enrutando esta petición hacia el dispositivo responsable de la "Autenticación" (LDAP, RADIUS; Kerberos, etc.), el mecanismo o algoritmo de autenticación puede operar de diferentes formas, pero en definitiva, luego del diálogo de autenticación, si la misma es válida, entonces recién allí "abre su puerta" de acceso. Este

protocolo puede ser empleado tanto en redes cableadas, como en redes inalámbricas y opera en el nivel 2.

Desde el punto de vista de seguridad de una red LAN, no puede ser dejado de lado, al menos en su análisis y mínima configuración, y es altamente recomendable su implementación pues hoy en día cualquier switch o punto de acceso programable de gama media ya incorpora este protocolo.

El detalle de este protocolo puede analizarse en el punto 4.2.5. 802.1x Autenticación de dispositivos conectados a un puerto LAN, del libro "**Seguridad en Redes**".

En esta sección, sólo deseamos hacer una representación gráfica del funcionamiento del mismo, y cómo este protocolo puede ser implementado en las diferentes zonas que venimos desarrollando en este libro.

La representación de su funcionamiento queda bastante clara, haciéndolo según la simbología de los circuitos electrónicos, en los cuáles, un "conmutador" (*es decir la tecla que presionamos en casa para encender una luz*) es una llave de paso "Normal Abierta" que al ser presionada cierra ese circuito permitiendo el paso de la corriente eléctrica. En nuestro caso, tal cual lo venimos describiendo el protocolo 802.1x funciona de forma similar en su lógica.

La imagen que sigue podemos ver representado este modelo de circuitos sobre las diferentes zonas de nuestra arquitectura propuesta.

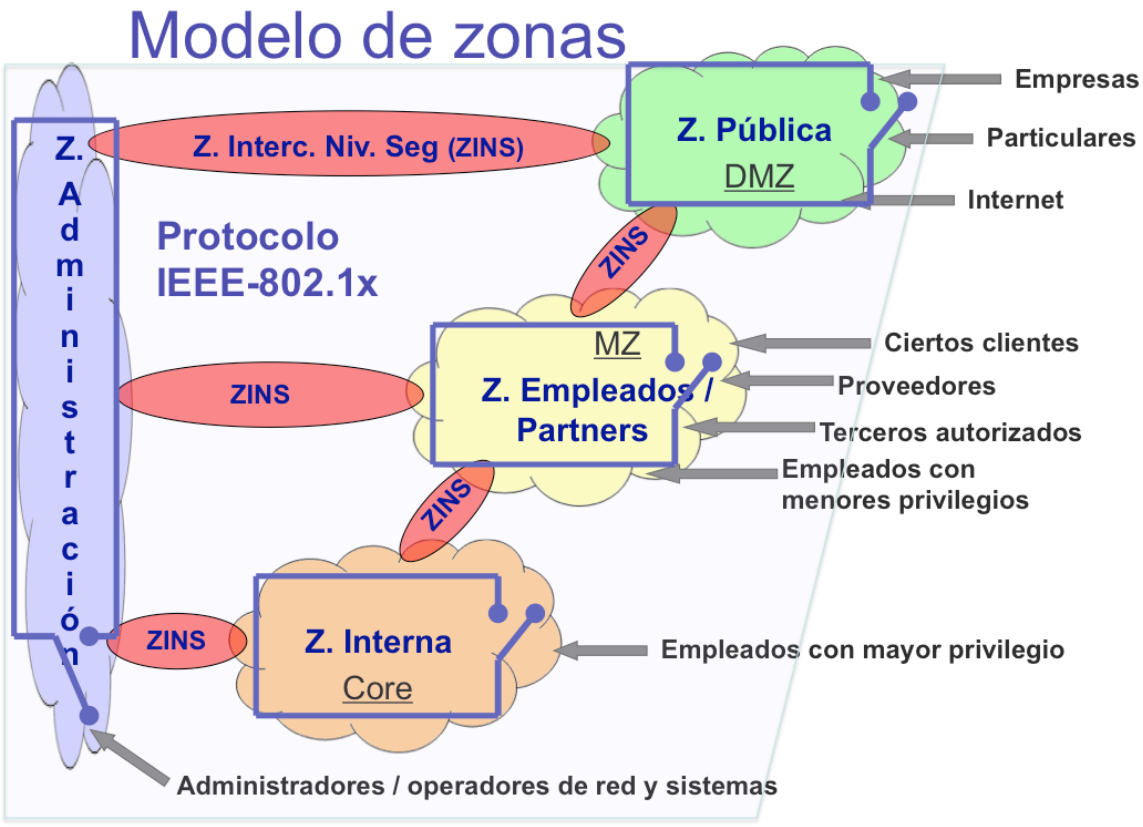


Imagen representación del protocolo 802.1x

*12.4.2. **Protocolo 802.1Q** (Virtual LAN).*

Este protocolo es el empleado justamente para la creación de **VLANs** dentro de un mismo switch y poder separar diferentes "dominios de colisión" bajo el concepto de "Trunking", lo veremos con mucha frecuencia y desde el punto de vista de la seguridad merece la pena prestarle atención pues un uso inadecuado, es foco importante de problemas.

802.1Q permite la creación de VLANs, agregando un encabezado de 4 bytes dentro de la misma trama Ethernet. Para que un Switch "encapsule 802.1q" debe tener configurada sus interfaces y sus VLAN para ello. Las buenas prácticas, nos indican que si tenemos más de un switch, es mejor hacerlo bajo la idea de

Interfaces "Trunk" (o troncal), que no son otra cosa que enlaces físicos entre los dispositivos (*generalmente Switchs, aunque no exclusivo de estos*) por los cuales "entroncaremos" (*aunque suene feo…)* varias VLAN, transportando el tráfico de varias de estas a la vez creando una especie de jerarquía entre ellos. Existe una VLAN por defecto que es la VLAN 1 (*o VLAN nativa*), la cual, ante cualquier error, omisión o ausencia de configuración, será por la que el switch envía toda trama y sin agregar ningún encabezado 802.1Q, por esta razón es que esta VLAN 1 SIEMRE debe estar deshabilitada como medida de seguridad, debiendo tener precaución (*en cuanto a switching*) de cómo opero o creo esta ruta por defecto o nativa en mi switch. Por supuesto que cada VLAN que es configurada en un extremo de cada Trunk debe ser idéntica en el otro pues en definitiva se trata de una conexión punto a punto.

¿Por qué es importante considerar la aplicación de 802.1Q?

Como veremos en la imagen siguiente, la primera ventaja es poder identificar: áreas, zonas geográficas, grupos de trabajo, tecnologías diferentes, etc.

En segundo lugar, a medida que vayamos avanzando en este capítulo, podremos comprobar que todo este conjunto de medidas, aplicadas de forma "Organizada y Coherente" conllevan a concatenar barreras de seguridad que en su conjunto nos ofrecerán un valor agregado substancial y muy diferenciativo a que si cada una de las mismas se adoptaran o analizaran individualmente.

Para ampliar más aún sobre este protocolo, os recomendamos la lectura del punto 4.2.3. 802.1Q (Virtual LAN) del libro "**Seguridad en Redes**".

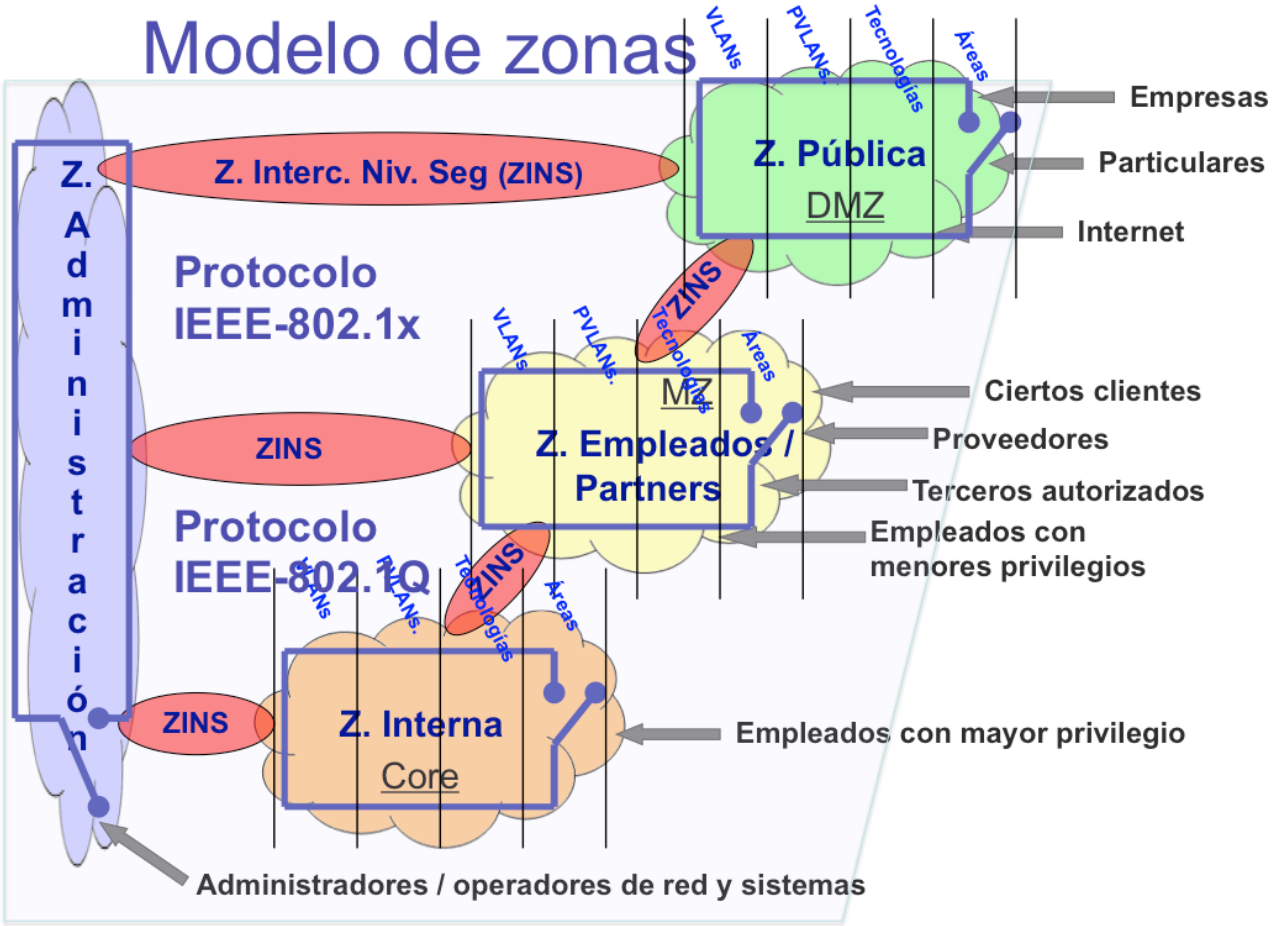


Imagen representación del protocolo 802.1Q

Para comenzar a "Concatenar" medidas de seguridad, presentamos a continuación una imagen, en la cual solamente ampliamos una de estas zonas. En este ejemplo la presentamos como la Red de Gestión de esa zona y hemos elegido el rango privado 10.x.x.x.

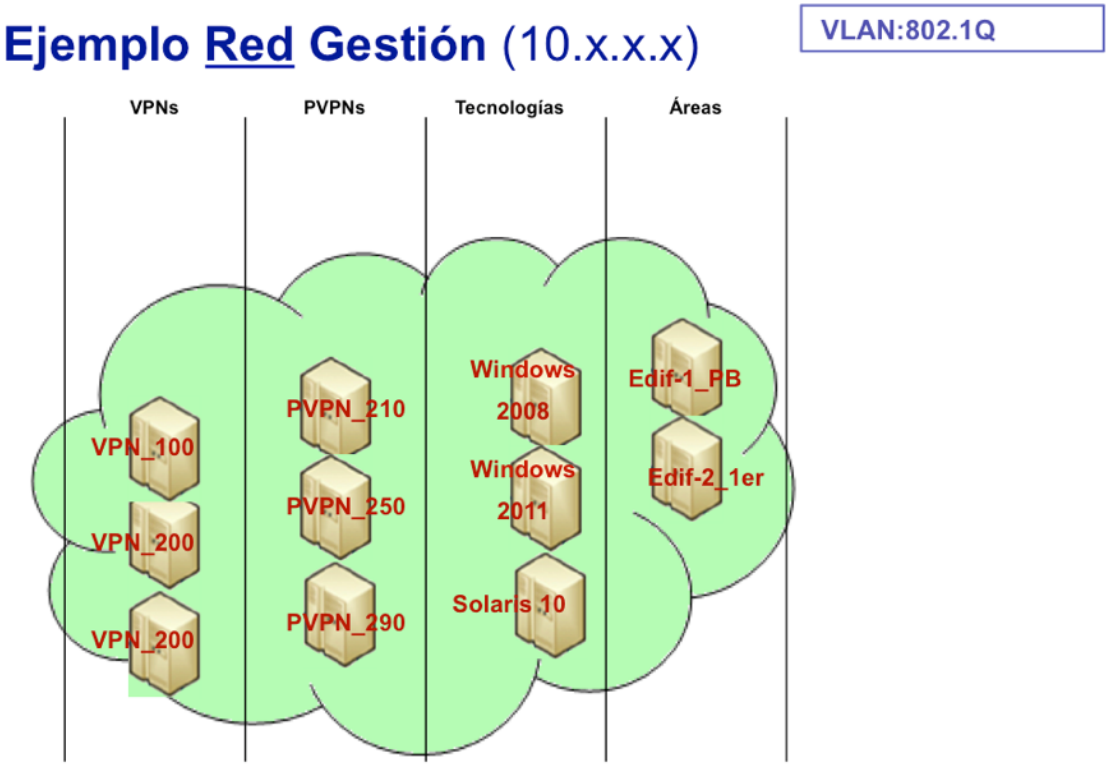


Imagen ejemplo de una red de gestión 10.x.x.x

12.4.3. Segmentación a nivel 3

Una de las principales medidas que podemos emplear a nivel de red, es la "Segmentación" de redes, empleando justamente el concepto de máscara de red y/o máscara de subred. Para ampliar sobre estos conceptos, recomendamos la lectura del capítulo 5. El nivel de Red, el libro "**Seguridad por Niveles**".

Una vez que hemos implementado una buena (*y lógica*) política de segmentación a nivel direccionamiento IP, podemos avanzar tranquilamente al control de rutas y de reglas de control de acceso. Todo aquello que no "enrutemos" concretamente entre esos segmentos de red, no será alcanzable a través de los diferentes segmentos de nivel 3, por lo tanto, si alguien logra comprometer un dispositivo en uno de estos segmentos, y las

reglas que hemos puesto en nuestras "Zonas de Intercambio de Niveles de Seguridad" son adecuadas, este intruso solamente podrá navegar en ese segmento, pues no tendrá acceso, ni siquiera enrutamiento a ninguna otra. En la siguiente imagen, podemos ver un ejemplo sencillo de cómo hemos segmentado esa zona en cuatro rangos diferentes de subredes, y concretamente, si no se establecen rutas o permisos en el Firewall que vemos en la parte superior (*y regula nuestra ZINS*), ningún dispositivo podría llegar a otro segmento.

Como detalle adicional, en esta gráfica vemos también como a su vez estamos empleando 802.1Q para crear VLANs dentro de estos segmentos de red y también para seguir avanzando en el tema, hemos definido algunas tecnologías y áreas diferentes (*Windows, Solaris, Edificio-1 PB, Edificio2 primer piso).*

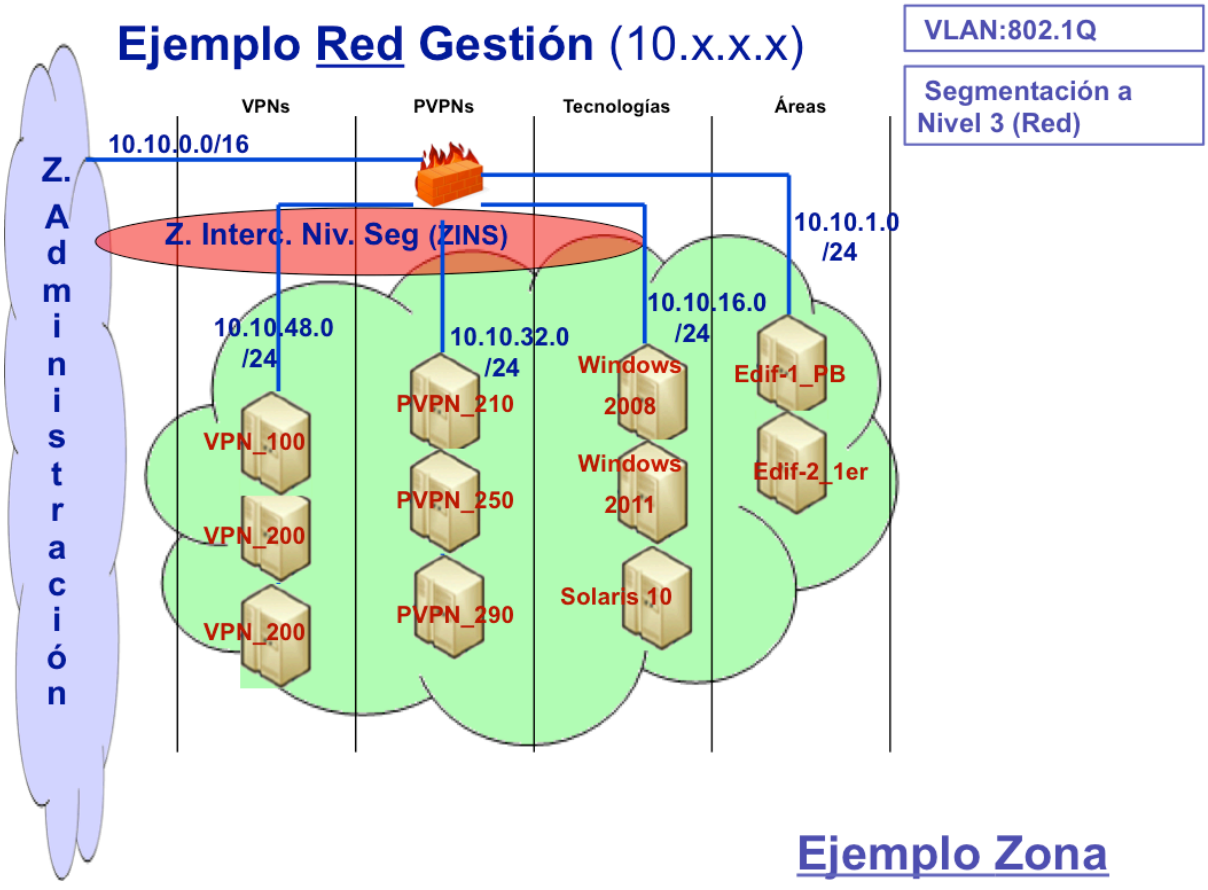


Imagen ejemplo de una red segmentada y de VLANs

Sobre esta misma imagen, superpongamos ahora el empleo de 802.1x. Podríamos representarlo de acuerdo a la siguiente imagen.

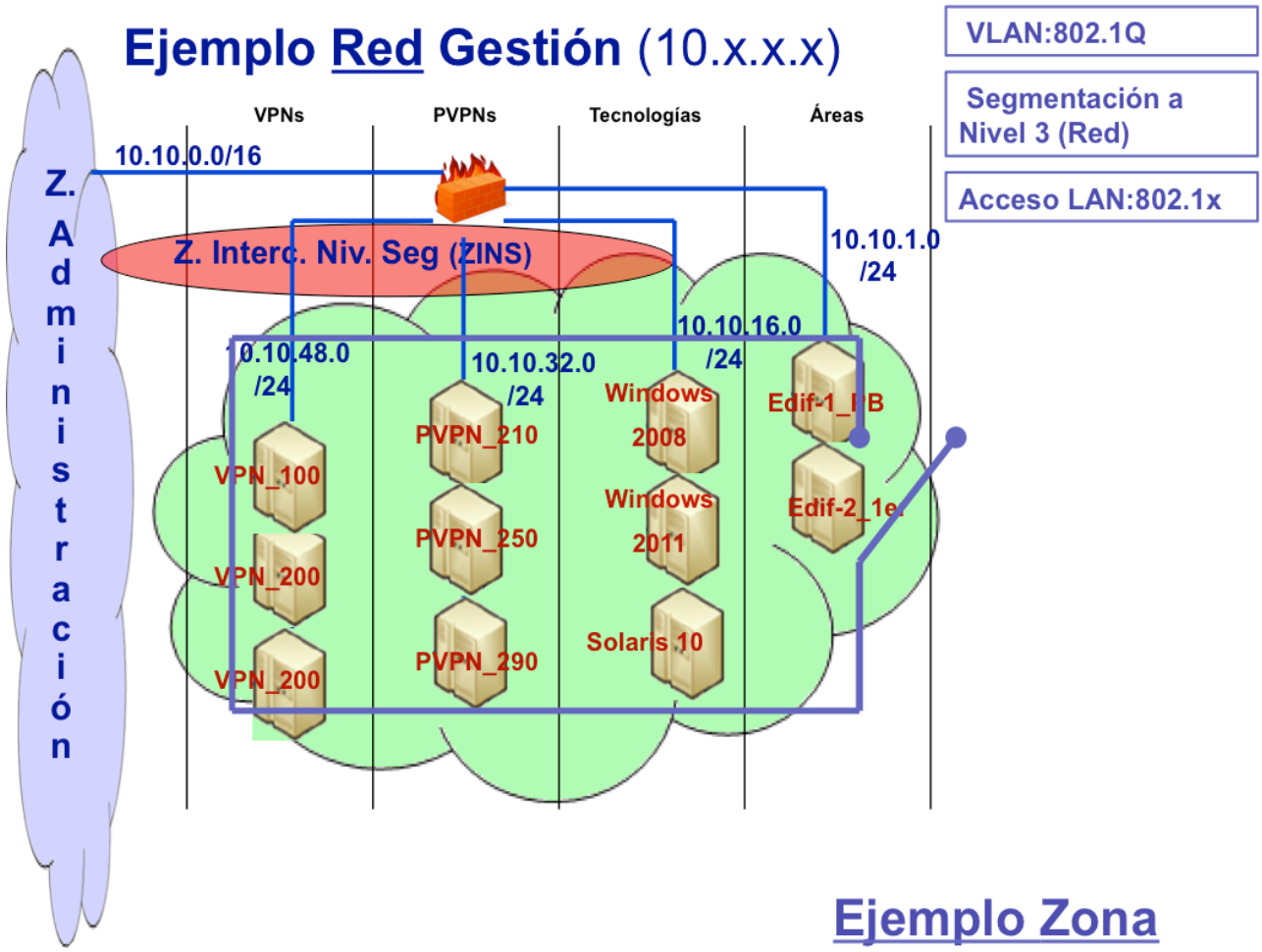


Imagen ejemplo de una red segmentada, 802.1Q y 802.1x

12.4.4. Seguridad en WiFi

Hoy en día, podríamos afirmar que toda infraestructura de red tiene habilitado algún tipo de acceso WiFi, es prácticamente una necesidad más del mercado.

Siguiendo con esta secuencia gráfica de medidas de seguridad que podemos adoptar, en redes Wifi, lo primero a considerar es la "**Segmentación**". JAMÁS permitamos que una red de invitados (*o guest),* pueda tener algún tipo de visibilidad con nuestra red corporativa (ni de servicios, ni mucho menos de gestión). El resto de las medidas de seguridad, siguen en la línea que estamos presentando, pues todo punto de acceso wifi de empleo profesional (no así los domiciliarios), permiten incorporar 802.1x y 802.1Q.

¿Qué me aporta esto último?

Justamente, concatenando estas medidas de seguridad podemos lograr que cuando alguien, se hace presente en el punto de acceso WiFi, el protocolo **802.1x** lo mantenga fuera de la red hasta tanto valide contra nuestra plataforma de Autenticación y control de accesos (*TACACS, Kerberos, LDAP, etc.)* si este usuario está dado de alta o no. En caso de estarlo, si continuamos concatenando medidas de seguridad, puede también verificar su rol, perfil o grupo y a través de **802.1Q** asignarle una VLAN determinada para ese perfil en concreto, por lo tanto, dependiendo del usuario que se haga presente, logrará un determinado tipo de accesos en base a los permisos que tenga configurado.

Todos los conceptos de seguridad en WiFi están desarrollados en el estándar **802.11i**, cuyo objetivo es la seguridad WiFi.

Tal cual venimos describiendo, este estándar abarca los protocolos **802.1x**, **TKIP** (Temporal Key Integrity Protocol), y

AES (Advanced Encryption Standard). Cada uno de ellos nos propone poder ofrecer un nivel de seguridad igual a una red cableada, en la actualidad sólo si se implementa a través del algoritmo **WPA2** (*Wifi Protected Access versión 2*).

Para ampliar más sobre el tema podemos consultar en el punto 2.4. Operación de la Seguridad del libro "**Seguridad en Redes**" o en el punto 4.2.1. WiFi (Wireless Fidelity) del libro "**Seguridad por Niveles**".

A continuación, presentamos una imagen donde se aprecia un punto de acceso WiFi y un recuadro poniendo de manifiesto esta necesidad (*hasta podríamos decir "obligación"*) de emplear **802.11i**.

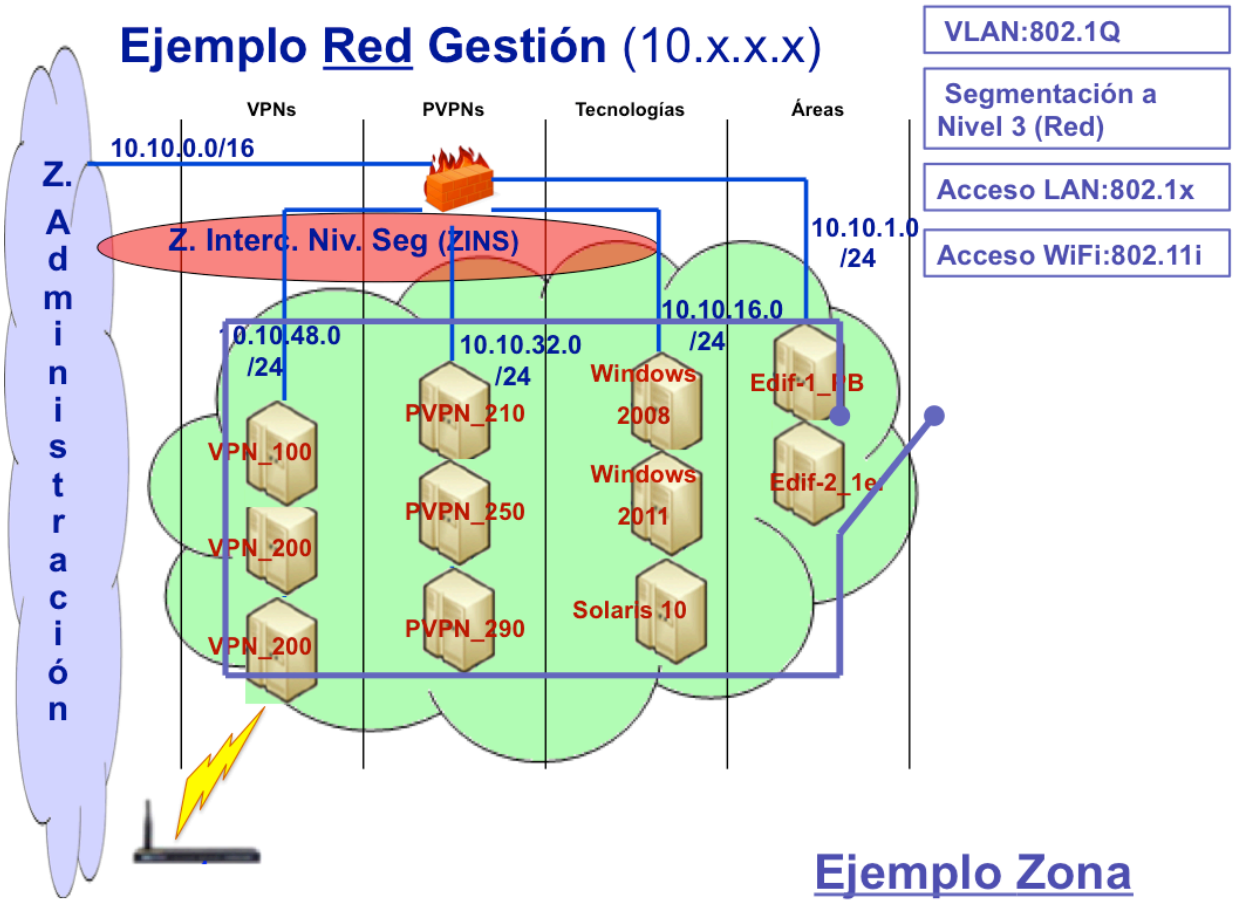


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x y 802.11i

12.4.5. Protocolos 802.1ae y 802.1.af

Estos protocolos ya fueron tratados brevemente en el punto 7.3. Tema base de hoy de **este libro**. Volvamos a la imagen que presentamos allí.

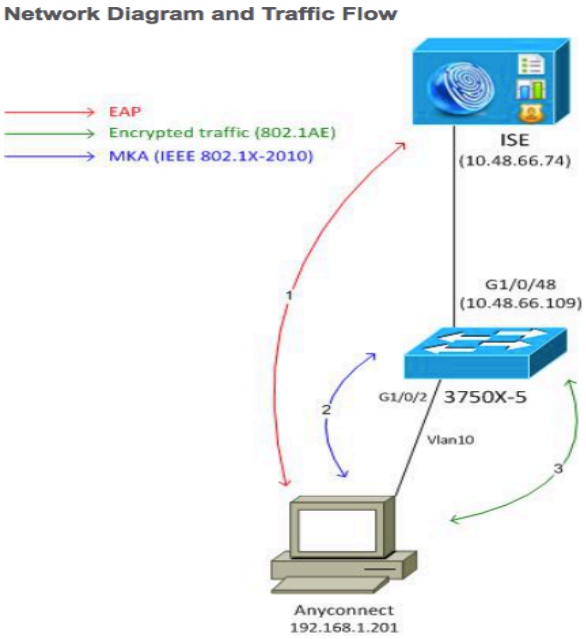


Imagen (Combinación de 802.1x con 802.1ae)

Tal cual desarrollamos en el punto mencionado (**7.3.**), el protocolo **802.1ae** "Media Access Control (MAC) Security", publicado en 2006 y cuya última enmienda es del 2013: 802.1AEbw) es conocido como **MACSec** ofrece confidencialidad, integridad y autenticación de origen, introduciendo nuevos campos a la trama Ethernet.

MACsec crea una "asociación de Seguridad" entre los extremos de ese nivel de enlace, criptografiando todas las tramas en un esquema "Point to Point Encryption".

Las tramas a nivel enlace, se cifran entre el switch y el ordenador que configuren este protocolo. Si se desea que las

tramas también se transmitan cifradas entre switchs, puede hacerse configurando también 802.1ae entre ambos switchs.

No es motivo de este punto reiterar conceptos, solamente deseamos seguir "sumando" medidas de seguridad en esta secuencia que venimos presentando gráficamente, así que a continuación presentamos una nueva imagen donde se puede apreciar un ejemplo de un área que se ha designado como de "máxima seguridad" y sobre la cuál específicamente se aplican estos protocolos.

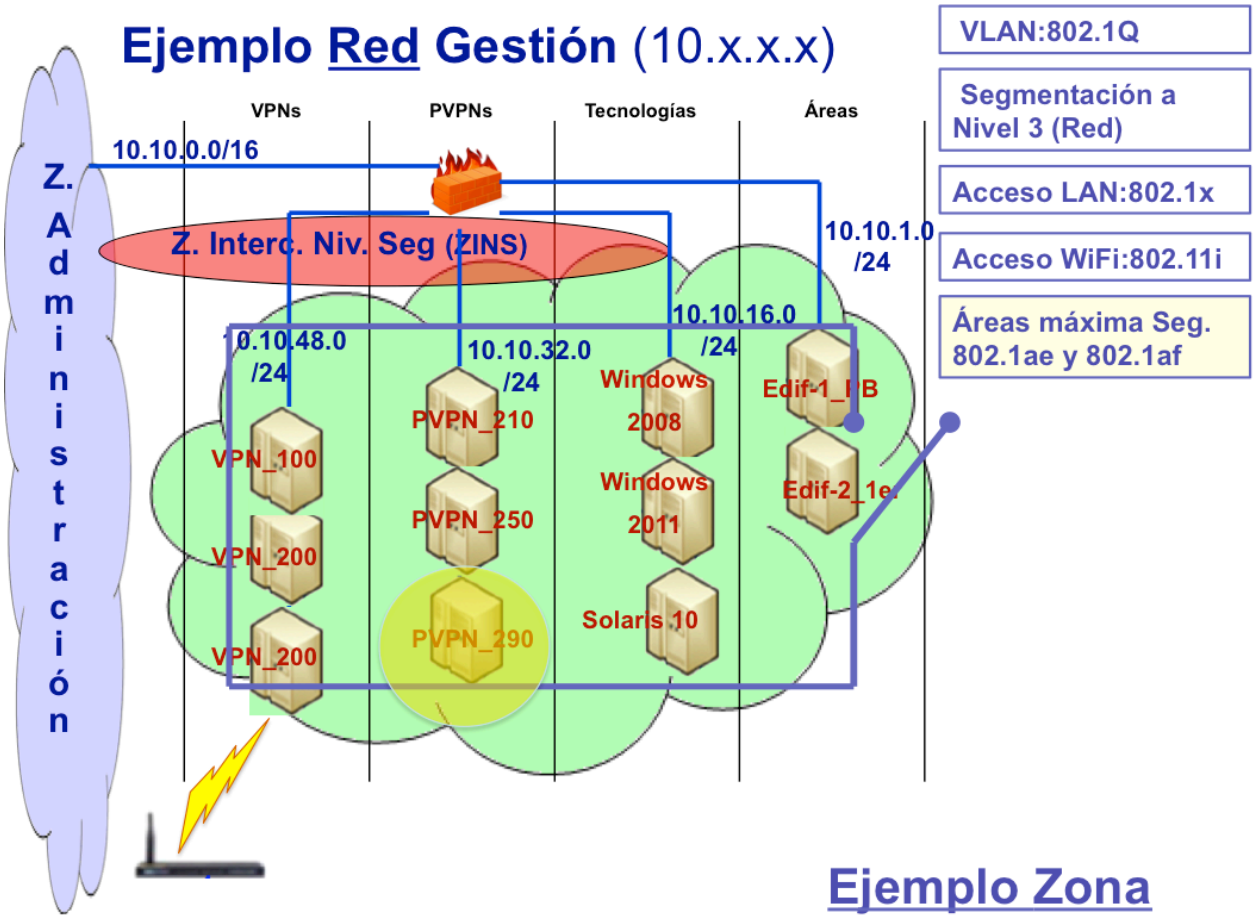


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae y 802.1af

12.4.6. Protocolo 802.1D (STP) y 802.1aq (SPB)

Uno de los peores problemas que puede presentarse para un Switch es cuando escucha la misma dirección **MAC** (*Medium Access Control*) por dos interfaces físicas diferentes, este es un bucle que, en principio, no sabría cómo resolver. Este problema si bien parece poco probable que pueda ocurrir, en realidad en redes grandes al tener cientos o miles de cables (*muchos de ellos para redundancia*), este hecho es tan sencillo como conectar el mismo cable en diferentes patch pannels que cierran un lazo sobre el mismo dispositivo, y en la realidad ocurre con cierta frecuencia, mayor, en la medida que más grande sea la red LAN. También es un hecho concreto cuando el cableado se diseña para poseer caminos redundantes, justamente para incrementar la disponibilidad de la red.

Cuando físicamente se cierra un bucle, la topología pura de red "Jerárquica" deja de serlo y se convierte en una red "Malla". Para tratar este problema el protocolo Spanning Tree (**802.1D**) crea una red "Jerárquica lógica (*árbol Lógico*)" sobre esta red "Malla Física". Este protocolo crea "Puentes" (bridges) de unión sobre estos enlaces y define a través de diferentes algoritmos que se pueden configurar.

Para ampliar más este tema, aconsejamos ver el punto 4.2.1. 802.1D (Spanning Tree Protocol: STP) del libro "**Seguridad en Redes**".

El protocolo **802.1aq** (***SPB**: Shortest Path Bridging*) aparece en al año 2006, si bien es alrededor del año 2012 cuando se difunde todo su desarrollo completo. La principal característica que ofrece SPB es que permite mantener "activos" todos los enlaces redundantes, sin necesidad de deshabilitar los bucles físicos (*como hace STP*), manteniendo una real topología de "Malla", con ello mejora la eficiencia y los tiempos de convergencia de la red.

Para ampliar más este tema, aconsejamos ver el punto 4.2.2 802.aq Shortest Path Bridging (SPB) de libro "**Seguridad en Redes**".

Uno de los ataques más sencillos de realizar sobre redes LAN es la falsificación de direcciones MAC. A través de este ataque, se pueden obtener diferentes tipos de objetivos (*a cuál más peligroso*), desde sencillamente realizar "MAC spoof", hasta aprovechas la misma para realizar "ataques del hombre del medio", realizar escuchas e inyección de tráfico sobre otros dominios de colisión (*es decir otros segmentos del Switch*), escuchar, interceptar y generar tráfico de **VOiP** (*Voz sobre IP*), hasta varios métodos de negación de Servicio.

También existen anomalías de red muy habituales a nivel enlace, que no son provocadas intencionalmente, sino que son fallos de hardware, software o humanos.

Para evitar (*o al menos minimizar el impacto*) todo este tipo de inconvenientes, es que se han diseñado estos protocolos. En la imagen que sigue, presentamos también a estos como otra medida para seguir "concatenando" acciones desde el punto de vista de la seguridad.

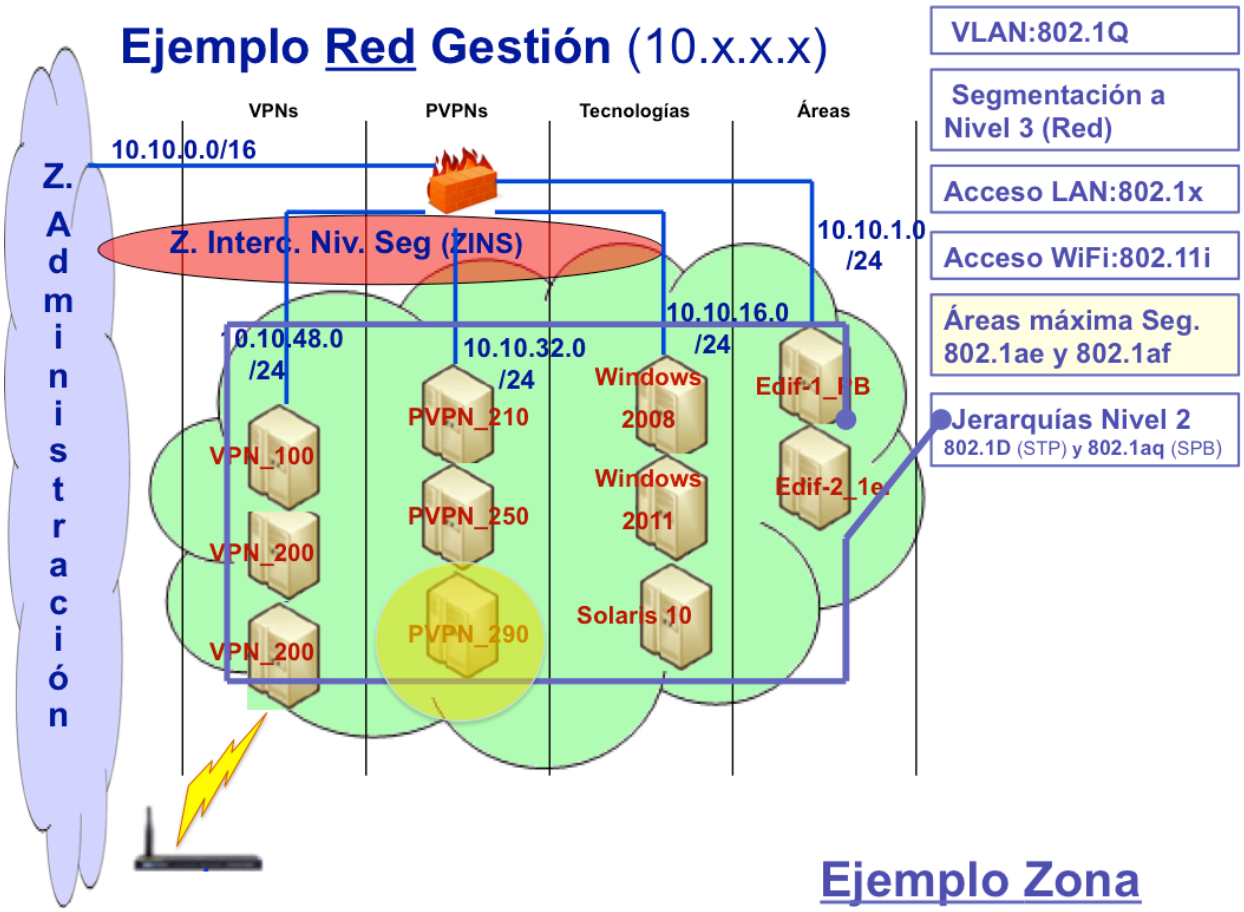


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae, 802.1af, 802.1D y 802.1aq

12.4.7. Virtualización de host

La tecnología de virtualización ha avanzado de forma exponencial en los últimos años. Hemos visto aumentar su capacidad de forma inimaginable. Hace unos meses, en la visita a un gran CPD (Centro de Procesamiento de Datos) vimos trabajar en sólo tres racks de comunicaciones, más dos únicamente para almacenamiento, un VMCenter que alojaba cuatro mil servidores virtuales, por supuesto que cualquiera de ellos tenía al menos las mismas prestaciones que si fuera un servidor real (*me atrevería a afirmar que bastante más aún*).

Se trata de estas paradojas de la vida, pues si lo analizamos fríamente, estamos retrocediendo a 40 años atrás como si fueran los viejos "main frames" de arquitectura "maestro – esclavo" pues también los hosts a nivel cliente y sus aplicaciones, hoy en día se están ejecutando de forma virtual en grandes plataformas virtuales….

La virtualización es probable que sea el camino de los próximos años.

Desde el punto de vista de ciberseguridad, es también un aspecto clave, si bien debemos prestar mucha atención a su adecuada configuración y bastionado, también nos ofrece un camino nuevo que como iremos viendo en las próximas líneas puede ser muy ventajoso.

Este concepto es la configuración y el control de "**GRANJAS**".

Lo que proponemos aquí es que desde el o los servidores de virtualización, diseñemos (desde el principio) una filosofía de administración del mismo a través de **GRANJAS de servidores**. Cada granja puede contener una misma tecnología, diferentes versiones de esta tecnología, mismas aplicaciones, funcionalidades, servicios, etc.

Si somos capaces de avanzar en esta línea, iremos centralizando sistemas operativos, versiones, administradores de plataformas, inventariado, obsolescencia, etc. De forma coherente.

Esta medida, en cuanto a ciberseguridad tiene muchas ventajas:

- Control por tecnología, prestación, servicio, modelo.
- Sencillez de procesos de entrada en producción y control de cambios.
- Plantillas de bastionado por granja.
- Centralización de actualizaciones y parcheado.
- Segregación de debilidades.
- Facilidad en los controles de flujo, routing y filtrado.
- Facilidad de Supervisión y monitorización.

- Gran capacidad de resguardo y recuperación.
- Facilidad en redundancia, clusters y disponibilidad del servicio.
- Alta disponibilidad de hardware y software.
- Velocidad en ABM de servicios.
- Ahorro de tiempo y velocidad en tiempos de respuesta.
- Puntos comunes de control (servidores de actualización, parcheado, antivirus, killswitch, etc.)
- "Compartimentación" (*a desarrollar más adelante*).
- Etc.

En la figura que sigue, representamos la capacidad que nos ofrecería la implementación de diferentes tipos de "granjas" a nivel host en nuestro segmento de red.

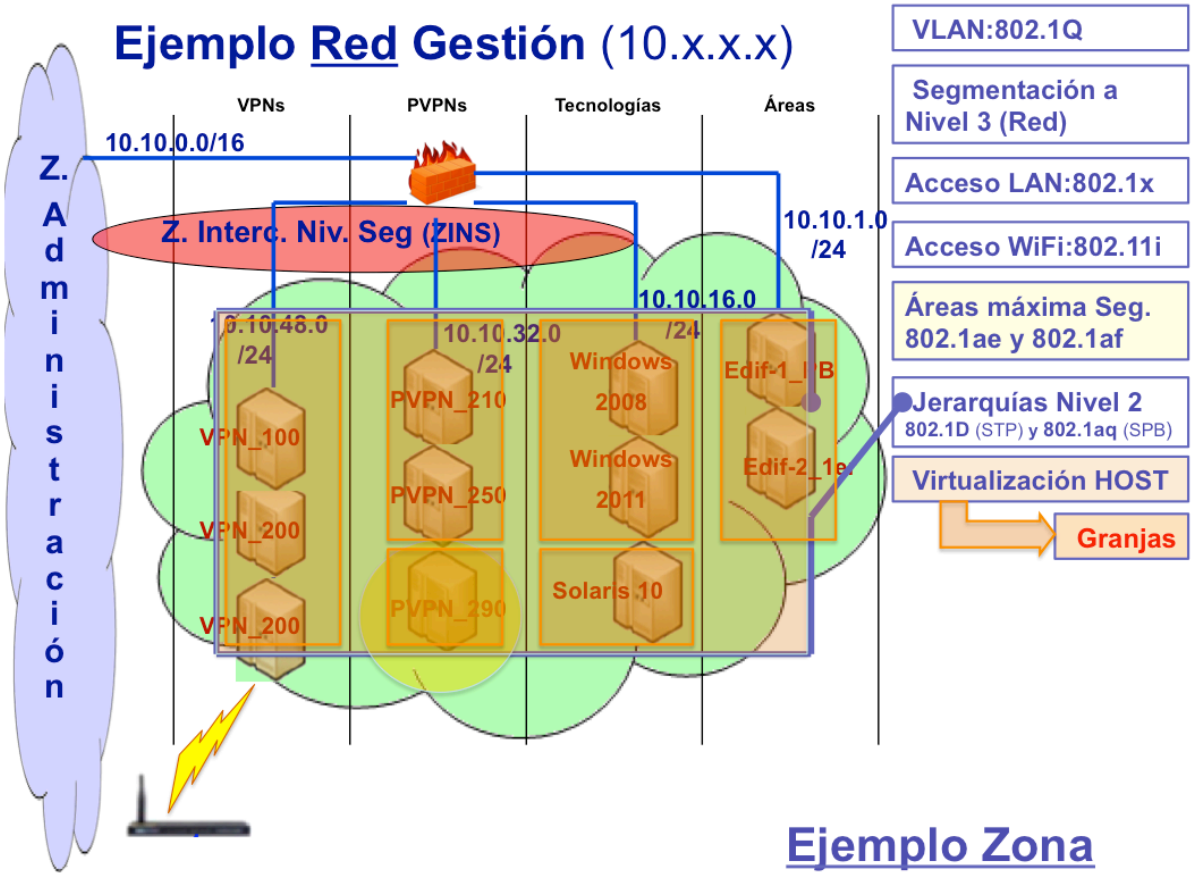


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae, 802.1af, 802.1D, 802.1aq y virtualización de hosts

12.4.8. "Compartimentación" de red.

Tal vez la ventaja más importante que nos puede ofrecer este último concepto, concatenado con los anteriores, es esta nueva idea que vengo impulsando desde hace meses que la denominé "**Compartimentación de red**".

Este concepto, es fundamental en los tiempos que vivimos.

La idea es que, si hemos llegado hasta este punto, siguiendo el conjunto de medidas de seguridad propuestas, tendríamos una capacidad de gestión de la seguridad con un altísimo nivel de granularidad.

Supongamos (*como viene sucediendo cada vez más a menudo*) que surge un nuevo tipo de malware que ataca a cualquier tipo de tecnología, sistema operativo, versión, etc. (*Recordemos WannaCry o Petya*). Si hemos cumplido con los pasos propuestos, tenemos a nuestra disposición varios cursos de acción, para que solo haciendo un "**click**" podamos **aislar completamente** en target de este ataque, y acotarlo exclusivamente a la zona, área, granja o VPN que queramos.

La idea es diseñar e implantar todo este conjunto de medidas, de la mejor forma que se ajuste a nuestra arquitectura de redes y sistemas. Una vez que tengamos bien encaminada esta fase, dediquemos todo el tiempo que esté a nuestro alcance para:

1) Realizar breves análisis de riesgo de estas zonas.
2) Identificar hipótesis de ataques.
3) Planificar y realizar "juegos de ciberguerra" (sobre estas hipótesis).

4) Reciclar las experiencias de estos ejercicios, mejorando la capacidad de reacción o "resisliencia" de nuestras infraestructuras.

En la imagen que sigue, presentamos gráficamente los conceptos de este punto.

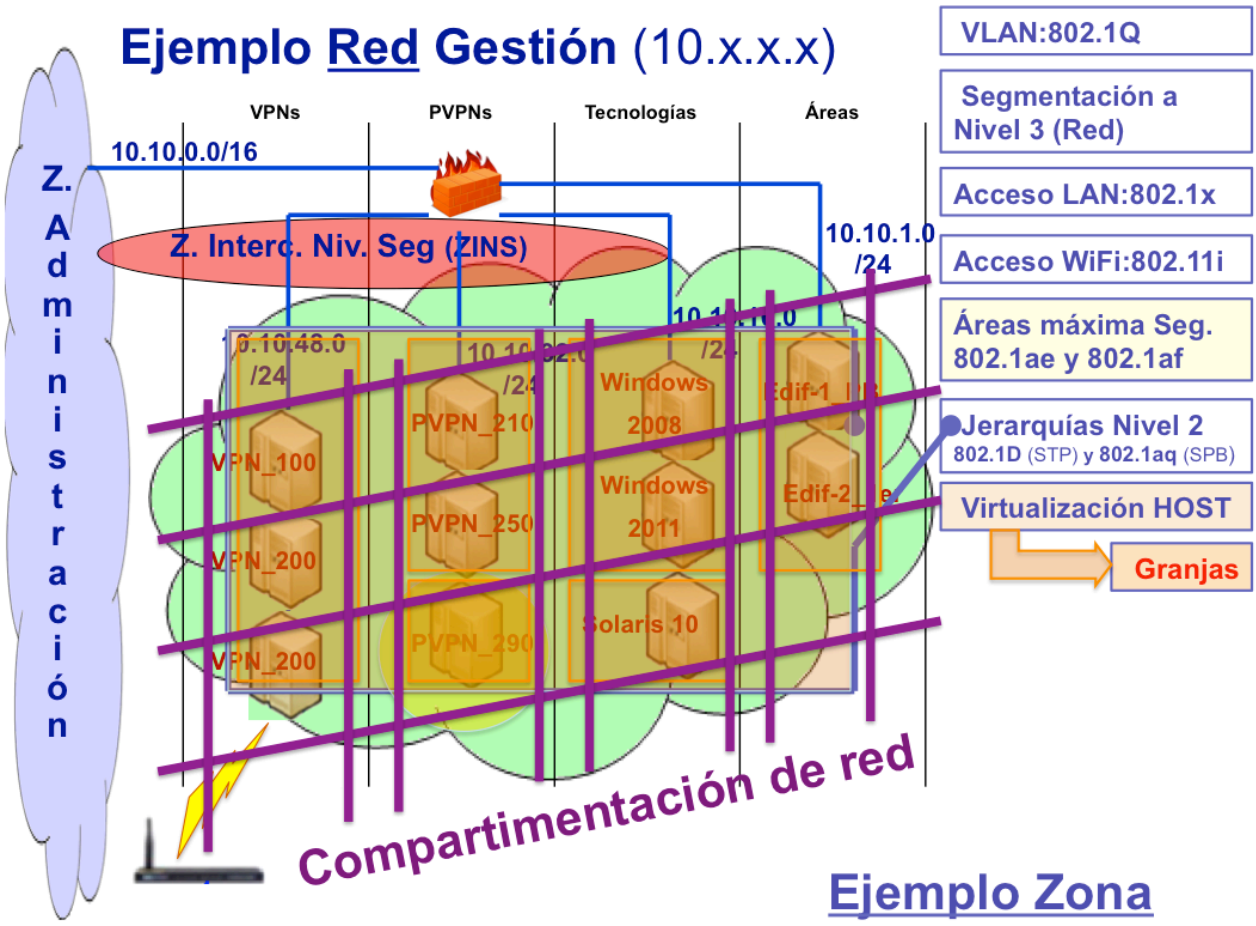


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae, 802.1af, 802.1D, 802.1aq, virtualización de hosts y "Compartimentación"

12.4.9. Virtualización de red

El último aspecto técnico que desarrollaremos, son las diferentes metodologías que podemos emplear para conectarnos remotamente a nuestras infraestructuras, de forma tal que la conexión sea exactamente igual a la que realizaríamos si estuviéramos sentados frente al dispositivo o en su propia red LAN.

Tal vez esta no sea la definición más escolástica de las redes virtuales, pero es probable que sea la más clara, pues lo que intentaremos detallar a continuación, es precisamente esto, las técnicas concretas que podemos emplear estando en casa, o en cualquier sitio del mundo para poder trabajar con las mismas funcionalidades y servicios que desde la misma oficina.

Existen varias herramientas comerciales y de open source que ofrecen más o menos amigabilidad o potencia a la hora de cumplir este cometido, pero básicamente todas ellas se basarán en las siguientes técnicas:

- VPN empleando SSL (*Secure Socket Layer*)
- VPN utilizando IPSec
- VPN a través de SSH (*Secure SHell*)

Este tema ya fue desarrollado con suficiente detalle en el punto 7.3. Tema base de hoy del **presente libro**, por lo tanto no profundizaremos más, sencillamente presentamos la imagen siguiente para cerrar todos estos conceptos.

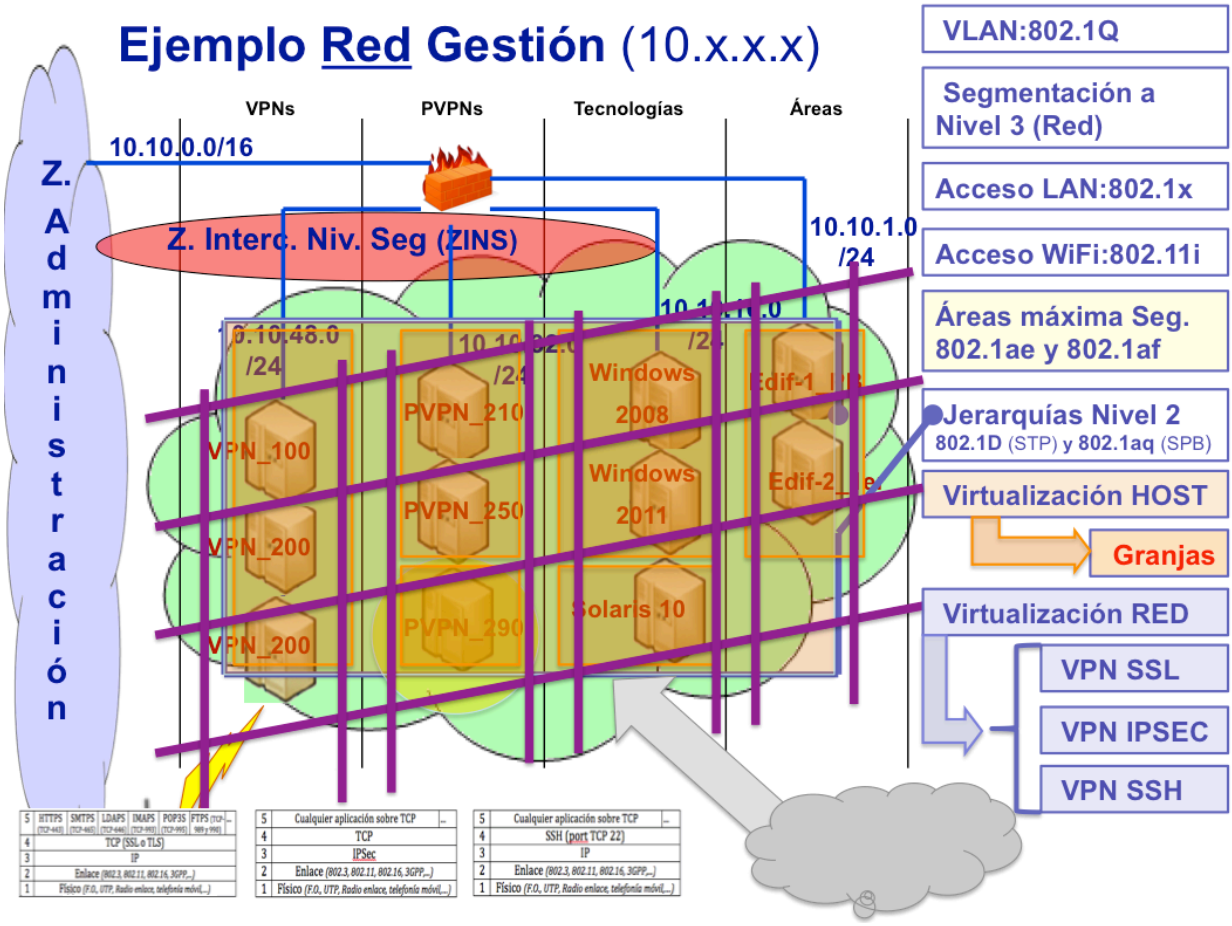
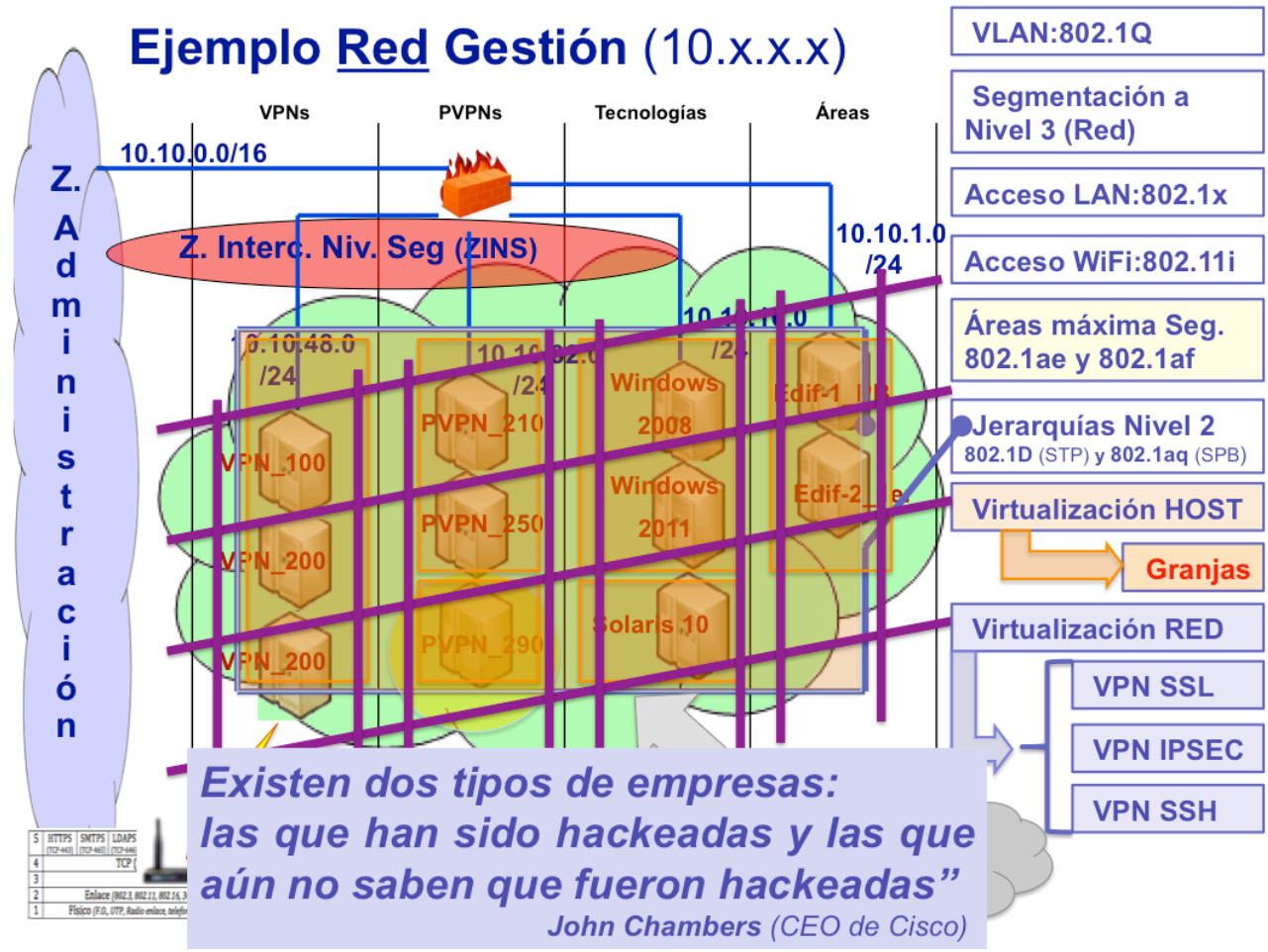


Imagen ejemplo de una red segmentada, 802.1Q, 802.1x, 802.11i, 802.1ae, 802.1af, 802.1D, 802.1aq, virtualización de hosts, "Compartimentación" y virtualización de RED

12.4.10. Resiliencia

Analicemos la siguiente frase.

-



¿La compartes, o aún te queda alguna duda al respecto)?

Seamos conscientes que nuestras infraestructuras, tarde o temprano sufrirán algún tipo de incidente de seguridad. Dejemos de pensar que somos invencibles pues ese fue el gran error de los grandes imperios o dictadores, tarde o temprano cayeron.

Si somos capaces de enfrentar esta realidad, entonces sigamos adelante mejorando todo este conjunto de medidas que hemos ido presentando y, como último aspecto, reiteremos una vez más lo siguiente:

El conjunto de procedimientos y las adecuadas acciones para su implementación, lo que conlleva todo su "**ciclo de vida**", serán la salvaguarda final que nos permitirá retornar nuestra organización a un estado operativo en el menor tiempo posible.

12.4.11. Ruido de red

El tema final de cierre de este libro, lo desarrollaremos nuevamente con un concepto que propone "Cisco" en su análisis del 2017. Este concepto lo ha titulado "Ruido de Red.

Veamos primero la imagen que presentamos a continuación para poder seguir adelante con este concepto.

Ruido de red:

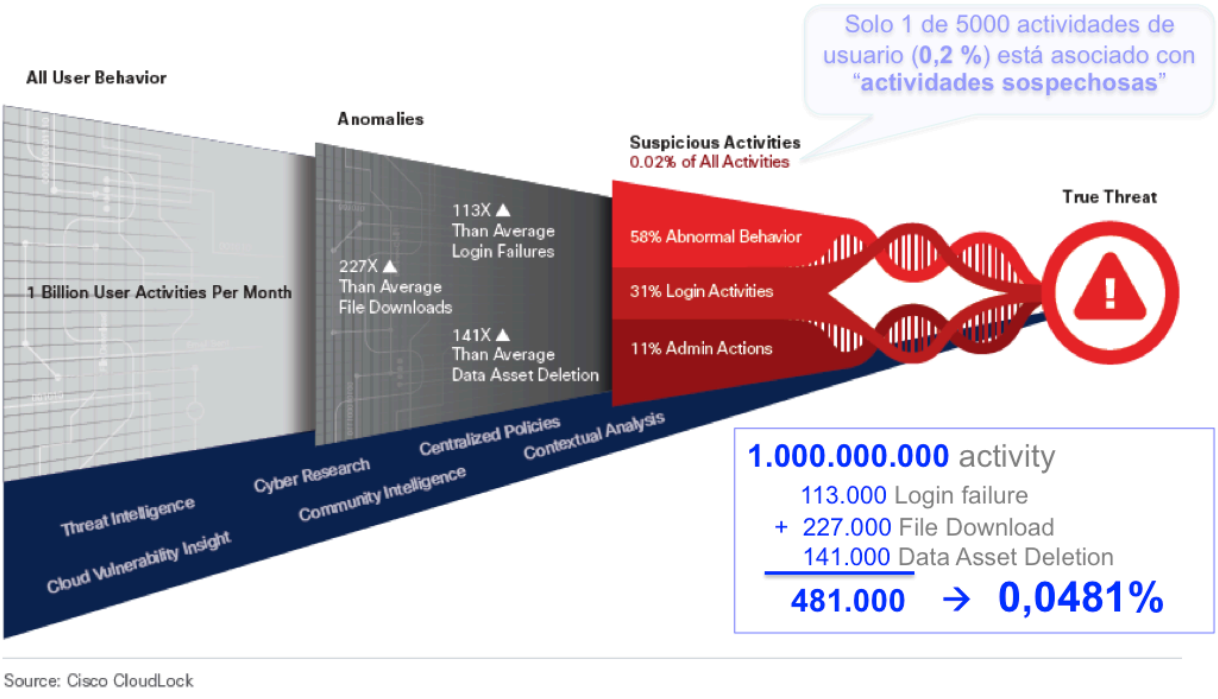


Imagen tomada del "2017 Annual Cibersecurity report" de Cisco

Esta imagen se genera, como se puede apreciar (*en la parte gris clara de la izquierda*), sobre la base de 1.000.0000.000 de actividades de usuarios por mes, es decir podemos considerarlo como una muestra suficientemente significativa en relación a cualquiera de nuestras organizaciones.

En el centro de la imagen (*parte gris oscuro del centro*) se pone de manifiesto que sólo el 0,0481 % de esta actividad pueden ser consideradas "Anomalías" de la red, estas peculiaridades las asocia a Fallos de login, descargas de ficheros y borrado de datos.

Por último, la parte **roja** de la derecha, nos muestra que únicamente 1 de 5000 paquetes se consideran como "**Actividad sospechosa**".

La propuesta de esta imagen es totalmente clara y al igual que cualquier otra señal electromagnética, para su análisis, debemos obtener una señal de "**calidad**", debemos ser capaces de limpiar este tráfico, eliminando todo el ruido posible. El trabajo de análisis de seguridad se potenciará en gran medida, si somos capaces de "separar la paja del trigo" y quedarnos con los eventos que realmente merecen nuestra atención.

Esta es la idea que Cisco propone como "**Ruido de Red**" y lo hace (*como siempre suele hacerlo*) sustentado en datos reales y con una muestra inmensa que no puede ser refutada.

Este tema lo venimos desarrollando a lo largo de muchos de nuestros textos, pues debemos ajustar reglas, políticas, eliminar falsos positivos, seleccionar los Logs a enviar, generar local rules, que miren específicamente los aspectos que particularizan nuestra infraestructura, esas debilidades que no podemos parchear o actualizar, o restringir. Nuestras infraestructuras son diferentes entre sí y cada una de ellas tiene sus defectos y virtudes, por lo tanto, si somos capaces de ir "eliminando el ruido" de las mismas, podremos realizar un trabajo de seguridad mucho más transparente y eficiente.

Este es el mensaje final de nuestro libro, apliquemos todo el conjunto de medidas que esté a nuestro alcance para que cada mes, año sea un nuevo escalón de ciberseguridad, un verdadero "Ciclo de Vida" o "Sistema de Gestión de la Seguridad de la Información" (***SGSI**, tal cual propone la familia ISO 27000),* seamos capaces de tener una red de "Calidad" pues hemos eliminado en gran parte todo ese ruido innecesario y estamos en capacidad de "escuchar y evaluar" lo importante, para poder obrar en consecuencia.

Ciberseguridad (Una Estrategia Informático Militar): Se trata de la tercera obra de **Alejandro Corletti Estrada** que desarrolla temas de Redes y Seguridad.

Ha tenido la amabilidad de escribir su prólogo **Julio Ardita**, un famoso "hacker" que a principios de los años 90' preocupó seriamente a EEUU de Norteamérica y hoy en día sigue siendo un importantísimo referente en temas de seguridad.

Esta nueva obra, es un poco la continuación de las anteriores: "**Seguridad por Niveles**" (*2011*) y "**Seguridad en Redes**" (*2016*), pero tratando más específicamente el problema de Ciberseguridad. Se encuentra basada en una serie de Webinars que impartió su autor a lo largo de ocho charlas durante este año, sumándole a estos contenidos bastante más detalles, tanto técnicos como de experiencias personales y ejemplos reales.

El libro comienza con una presentación, basada en que "***La unión hace la fuerza***" hoy más que nunca, en particular pensando en Sud y Centro América. Como se irá viendo a lo largo de sus capítulos, el tema de la Ciberseguridad solo puede ser llevado al éxito, a través de grandes y serias alianzas entre países y con las empresas privadas. Luego va desarrollando una serie de conceptos y analogías entre estrategias militares y su aplicación a las nuevas tecnologías, mezclando estos conceptos con protocolos, procedimientos y metodologías de ciberseguridad.

El libro, una vez más, como los anteriores, está disponible en su versión digital bajo licencia **"Copyleft"** para su libre descarga y difusión sin fines de lucro en la página Web: **www.darFe.es**. Se recomienda especialmente para su uso en todo tipo de ámbito de docencia por su marcado enfoque metodológico.

Alejandro Corletti Estrada:

Es Doctor en Ingeniería Informática, MBA. Fue militar, Jefe de Redes del Ejército Argentino, profesor universitario de las materias Redes y Comunicaciones y Director del Centro de Investigación en Seguridad Informática de Argentina (CISI.ar), y actualmente docente del master en Ciberseguridad de la Universidad Alfonso X y Director de la empresa "DarFe Learning & Consulting S.L.". Vino a Madrid en el año 2000, lugar donde actualmente vive. Se ha desempeñado como consultor experto y asesor en temas de seguridad informática y Redes en muchas empresas. Ha disertado en varios congresos internacionales y publicado artículos siempre relacionados a seguridad y redes de ordenadores.

"**Ciberseguridad (Una Estrategia Informático / Militar)**" es la continuación de "**Seguridad en Redes**" (*2016*) y "**Seguridad por Niveles**" (*2011*). Todos ellos son el resultado de muchos años de apuntes, clases, cursos, artículos, conferencias y auditorías de seguridad que han sido recopilados y presentados de forma técnica, con muchos ejemplos, capturas de tráfico y ejercicios.

Según **John McAffe** "La tercera Guerra Mundial será una Ciber guerra"…

¿Será Cierto?