

“Estrategia de seguridad informática por Acción Retardante”

Alejandro César Corletti

Universidad Politécnica de Madrid

Departamento de Ingeniería de Sistemas Telemáticos

Madrid, España

acorletti@wanadoo.es, acorletti@hotmail.com

RESUMEN

La actual política de seguridad (RFC – 2196) y también la anterior (RFC-1244, que si bien queda obsoleta por la primera es muy ilustrativa), proponen dos conductas a seguir: - Proteger y proceder.
- Seguir y perseguir.

Luego de leer detenidamente la terminología a la que hacen referencia esos documentos, surge una clara similitud con el empleo de la Fuerza en las Operaciones Militares. Se trata de documentos en los cuales se hace permanente alusión a la figura del “Enemigo o atacante frente a la propia Fuerza”.

El incentivo de este trabajo, nace ante la evidencia que si se debe tratar una confrontación de fuerzas, es estrictamente natural comenzar por organizaciones que llevan miles de años poniendo a prueba estas técnicas. Hoy se trata de otro combate pero al leer la documentación militar, aparece el primer indicio que es el punto de partida de esta investigación: El reglamento de EMPLEO DE LA FUERZA TERRESTRE (DO1 – 001) de OTAN menciona en el punto 14.5.

Proteger y proceder = OPERACIÓN DEFENSIVA = ESTÁTICA.

Seguir y perseguir = OPERACIÓN RETROGRADA = DINÁMICA.

Este trabajo propone la implementación de 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.

Palabras claves: Acción Retardante, Intercambio (tiempo por recursos), Enemigo, Orden de Operaciones militar, Línea a no ceder.

ABSTRACT

The current politics of security (RFC-2196) and also the previous one (RFC-1244 that although it is obsolete for the first one it is very illustrative) they propose two behaviors to continue: - To protect and to proceed.
- To continue and to pursue.

After reading the terminology attentively to which make reference those documents, a clear similarity it arises with the employment of the Force in the Military Operations. It is documents in which it becomes permanent allusion to the "Enemy's figure or attacker in front of the own Force."

The incentive of this work, is born for the evidence that if a confrontation of forces should be treated, it is strictly natural to begin with organizations that take thousands of years approving these techniques. Today it is another combat but when reading the military documentation, the first indication that is the starting point of this investigation appears:

The EMPLOYMENT OF THE TERRESTRIAL FORCE (DO1-001) of NATO it mentions in the point 14.5.

To protect and to proceed = DEFENSIVE OPERATION = STATIC.

To continue and to pursue = OPERATION RETROGRADES = DYNAMICS.

This work propose the implementation of a new planning methodology and execution of the defense of a computer system but under this new strategy, that is to say, to change the current politics at the highest level, leaving aside the medieval defensive concept of " walls ", for the modern focus under which should be been fully conscious which will be given information and land at a vastly superior and unknown enemy, to be able to assure the resources that are truly valuable, in detriment of those that are not it.

Keywords: Delay Action , Exchange (time for resources), Enemy, Military Order of Operations, Line to not giving.

1. PRESENTACION:

El presente trabajo es el resultado de la investigación de una tesis doctoral que nace analizando los conceptos de seguridad en redes, y en virtud de la experiencia militar del autor y de su cargo como Jefe de Redes del Ejército Argentino durante un largo período, se comienzan a entrelazar los conceptos militares con los informáticos, dando como resultado esta nueva estrategia que propone el diseño e implementación de una red basada en la definición de sucesivas líneas de retardo que permitan intercambiar recursos por tiempo generando libertad de acción para seguir y perseguir una intrusión a sistemas informáticos.

En los párrafos siguientes se tratará de resumir los aspectos más importantes del trabajo, en virtud de la magnitud del mismo.

2. INTRODUCCION:

La seguridad de los sistemas informáticos es un problema crítico que sufren hoy todas las Organizaciones. Las estadísticas muestran que aproximadamente entre el 70 y el 80 % de los ataques provienen desde el interior de los mismos, es decir el usuario interno, sin embargo esto se puede acotar e identificar por el conocimiento que se posee de los mismos siempre y cuando se empleen las herramientas adecuadas.

El porcentaje restante es adjudicado a ataques que provienen desde el exterior. En esta clasificación el origen que abarca la masa de los mismos es Internet, realidad que no puede dejar de lado ninguna empresa que quiera competir en el mercado. Lo realmente crítico que posee este hecho es el absoluto desconocimiento del enemigo 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 en esta introducción es nuevamente 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 enemigo 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?

3. BREVES CONCEPTOS DE LA DOCTRINA MILITAR:

La clasificación de las operaciones militares difieren en algunos detalles, acorde al País que se analice, pero en general casi todas consideran tres tipos de operaciones:

- Operaciones Ofensivas.
- Operaciones Defensivas.
- Operaciones Retrógradas.

La primera de ellas, es claro, que lo que refleja es una actitud de avance, ataque o agresiva. En este estudio, 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 una serie de 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 militar al respecto, pero se aprecia necesario incluirla para continuar el estudio.

3.1. Reglamento DO1 – 001 (Segunda Edición) EMPLEO DE LA FUERZA TERRESTRE

“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.

Esta cesión voluntaria de terreno permite a la fuerza de retardo:

- *Ralentizar el impulso del 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 fuerzas propias.*
- *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.

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”.

3. 2. Reglamento DO2 – 002 DOCTRINA OPERACIONES

"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 e sus vanguardias y plazos de intervención de sus gruesos.*
- *Procedimientos ofensivos.*
- *Posibilidades de sus medios ante nuestras acciones de contramovilidad.*

....."

3.3. Secuencia y doble enfoque militar.

Por último un aspecto muy importante a tener en cuenta en la doctrina militar es el análisis de toda operación.

Toda operación que se lleve a cabo responde a una secuencia de pasos establecida para la resolución del Jefe o Comandante. Esta actividad es uno de los pilares fundamentales del funcionamiento de lo que se llama Estados Mayores, que en terminología empresarial es el "Staff de un Director", estos procedimientos son motivo de muchos años de estudio de los oficiales de las distintas Fuerzas Armadas, pues es la experiencia volcada a lo largo de la historia militar.

Los conceptos fundamentales que se pueden resumir y se consideran de especial interés para este trabajo son los siguientes:

- Desdoblamiento del Estado Mayor:

Dentro de la cantidad de miembros que forman parte de un Estado Mayor (Staff), existen dos que desempeñan un rol fundamental. Se trata del Oficial de Operaciones y el de Inteligencia. El primero de ellos es el que realiza el enfoque desde el punto de vista de la propia fuerza y determina los posibles cursos de acción a tomar. El de Inteligencia es el responsable de obtener toda la información del enemigo y a través de un feedback llamado Ciclo de producción de Inteligencia (también estudiado al detalle), el cual mezcla y valoriza la información reunida, se va obteniendo la llamada carta de situación del enemigo.

- Secuencia para la toma de decisiones:

Para la ejecución de toda operación militar se siguen una serie de pasos que están especificados en detalle y de los cuales se puede resumir lo siguiente:

- El Oficial de Operaciones analiza los posibles cursos de acción.
- El Oficial de Inteligencia determina las capacidades del enemigo.
- Se planifican los posibles cursos de acción.
- Se realiza la Confrontación, donde se enfrentan las posturas de Operaciones e Inteligencia y se determina la factibilidad de los distintos cursos de acción, se cuantifican los beneficios de cada uno de ellos y se descartan los que son inviables por el accionar enemigo.
- Sobre esto se elabora la propuesta de los cursos de acción seleccionados, para que el Comandante resuelva y tome la decisión correspondiente a partir de la cual se genera la Orden de Operaciones y ya todo el Staff se pone a trabajar sobre esta elección.

El resultado de este punto de vista comparado con el enfoque civil, es que no suele existir en las empresas este desdoblamiento, es decir dentro del grupo responsable de la seguridad informática no se presenta un responsable de Operaciones y otro de Inteligencia, los cuales dentro del ámbito informático tienen dos roles bien definidos:

- Responsable de Operaciones: Análisis desde el punto de vista interno, es decir debe estar al tanto de:

- Hardware y Sistemas Operativos.
- Actualizaciones de los mismos.
- Herramientas que se disponen.
- Sistemas de detección de intrusiones.
- Auditorías de registros (Logs).
- Monitoreo de tráfico.
- Filtros y listas de acceso.
- Planes y Políticas de seguridad.
- Fuentes de obtención de Información "amigas".

- Responsable de Inteligencia: (Debe ser un verdadero enemigo, pero a favor de la empresa), Debe saber sobre:

- Herramientas de hacking.
- Exploits y vulnerabilidades.
- Penetración de redes.
- Cracking de contraseñas.
- Ingeniería social.

- Hacking blanco.
- Lenguajes de programación de bajo nivel.
- Fuentes de obtención de Información "enemigas".
- Incidentes ocurridos.
- Carta de situación del enemigo.

Si se determinan estos roles, se puede llevar a cabo la secuencia mencionada y la confrontación correspondiente en la cual se presentarán las distintas medidas a adoptar como el producto de dos especialistas que ponen de manifiesto enfoques opuestos. El Jefe de este elemento de seguridad será quien en definitiva decida cuál será el curso de acción a adoptar bajo el asesoramiento recibido.

4. OBJETIVO DEL TRABAJO.

Aunque no sea lo habitual, el objetivo se plantea recién en esta sección para que una vez considerados los puntos de vista militares de la cuestión, se puedan confrontar con el enfoque civil de seguridad en redes. En virtud de este planteo, a lo largo de este trabajo se tratará de hacer reflexionar sobre lo siguiente:

- a. Es posible delimitar exactamente una interfaz entre el usuario interno y el externo. Esta interfaz se llamará Línea a no ceder o Línea de retardo final (LRF).
- b. Determinar sucesivas líneas de retardo que permitan intercambiar recursos por tiempo y alarmas.
- c. Modificar el concepto ESTÁTICO DE DEFENSA actual, por una verdadera dinámica de acción retardante.
- d. Aplicar la Orden de Operaciones como herramienta para la implementación del Plan de seguridad.

5. DEFENSA INFORMATICA POR ACCION RETARDANTE.

La doctrina militar plantea que esta operación se realiza mediante el empleo de "líneas de retardo", es decir interfaces en las cuales se toman un conjunto de medidas para:

- Desgastar al enemigo.
- Obtener información del mismo.
- Ganar tiempo.
- Desviar su atención hacia otras zonas.
- Frenar su avance o inclusive detenerlo.

Este conjunto de medidas en el caso extremo, debería conducir hasta una última línea, la cual ya no se puede dejar sobrepasar por el enemigo, pues superada la misma se estaría ante una derrota en virtud que el enemigo cumplió con su objetivo final. Esta última línea debido a esta importancia es llamada "Línea de retardo final (LRF) o Línea a no ceder".

Al estudiar las distintas políticas y planes de seguridad, esquemas propuestos, implementaciones reales en empresas y planes de contingencias. En su gran mayoría demuestran un enfoque de barreras y alarmas, para negar el acceso o alertar la presencia de intrusiones. Este hecho es lo que se asemeja al concepto militar de defensa, es decir estático, lo que el autor llama "Murallas", hasta el principal actor de estos diseños posee un nombre semejante: "¡Firewall!". Si se comienza un diseño, análisis, plan o política de seguridad bajo esta idea, sólo se podrá:

- Proteger y proceder.

Nunca se logrará:

- Seguir y perseguir.

NOTA: Se hace referencia a estos dos conceptos pues son las dos estrategias que propone la RFC-1244, la cual si bien queda obsoleta por la RFC-2196, posee un gran valor metodológico en la confección de la Política y Plan de seguridad.

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 este trabajo de investigación, 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.

Por lo tanto, lo primero que se propone aquí es el diseño de "Líneas de Fase", desde la periferia hacia el corazón de la red, teniendo en cuenta un cierto intercambio con el enemigo, el cual por ser superior encontrará puntos débiles. Si se desea "Retardar" a este enemigo para ganar el tiempo necesario, se deberá entregar cierta cantidad de recursos, los cuales no deberían causar impacto en la Organización.

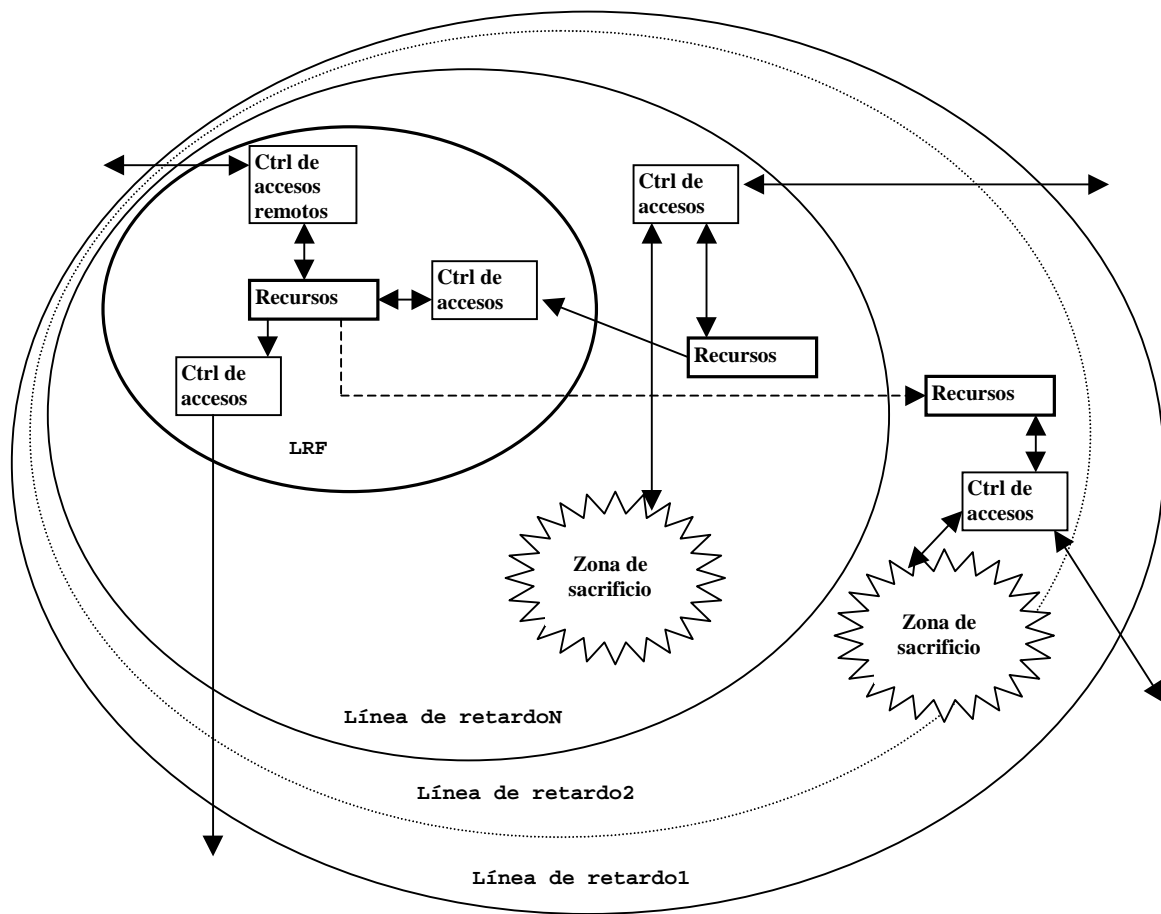
A medida que las líneas de fase se aproximan al corazón de la red, los recursos van cobrando importancia y el avance enemigo, debería ser más difícil.

Al llegar a la Línea de retardo final (LRF), se deberán tomar todas las medidas para que el enemigo no la sobrepase, sino el sistema se encontrará seriamente comprometido, en terminología militar esto sería una derrota.

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 y cuáles definitivamente no.
- Delimitar líneas de retardo 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 y sus probables líneas de aproximación.
- 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, para quebrar el avance de intrusos.

Una primera aproximación puede ser la gráfica que se presenta a continuación:



- > Establecimiento de sesiones en un solo sentido.
 - ←————> Establecimiento de sesiones en dos sentidos.
 - - - - -> Fuera de línea.
- LRF:** Línea de retardo final.

La metodología para plantear esta operación ya que se trata de una confrontación de fuerzas, nuevamente se analiza desde el punto de vista militar y se puede llevar a cabo a través de lo que proponen las operaciones militares y se llama "Orden de Operaciones"

6. ORDEN DE OPERACIONES DE ACCION INFORMATICA RETARDANTE.

Se propone aquí la metodología para implementar en forma real lo propuesto a lo largo de este trabajo. El formato aquí expuesto responde estrictamente a la Orden de Operaciones Militares reglamentada por la OTAN, ajustando los aspectos necesarios para la actividad informática.

Un detalle particular que diferencia la orden de operación de militar de la actividad informática, es que cada orden de operaciones militares, se realiza para una y sólo una misión particular dada. En el caso de la actividad informática, esta actividad es un continuo donde no necesariamente existe una interfaz entre un ataque y otro. Teniendo en cuenta esta idea es que aparece una segunda incorporación a esta orden de operaciones, la cual trata de **“Mantener una base de datos histórica a través de un ciclo continuo”** (característica netamente informática), lo cual no hace más que afirmar la posibilidad de acercar la metodología civil de Internet con la Militar, pues es lo propuesto también por la RFC-2196 en cuanto a analizar cada intrusión, almacenarla y reciclarla en el sistema para posteriores medidas.

Los puntos de implementación de mayor interés son:

- Definición de líneas de retardo.
- Definición de línea a no ceder.
- Operaciones de seguridad.
- Operaciones de Inteligencia.
- Operaciones de decepción (Engaño).
- Medidas de detección y monitoreo.
- Intercambios de información por tiempo.
- Contra medidas.

A continuación se presenta la Orden de Operaciones propuesta:

“Orden de Operaciones de Acción Informática Retardante”

1. SITUACION

a. Enemigo

Este apartado se considera necesario dividirlo en dos (respecto al formato militar) para poder mantener la dinámica de actualización imprescindible en todo sistema de seguridad informático:

- Información General.
- Información particular de esta red.

(1). Información general:

Se desarrollará aquí los aspectos generales conocidos a través de la difusión de diferentes ataques con el mayor grado de detalle posible, pues este apartado servirá de referencia ante la detección de intrusiones, será común desglosar este punto a través de anexos. A medida que se avance con este estudio se detectarán vulnerabilidades del sistema que implicarán modificaciones al cuerpo de la Orden, generando el ciclo dinámico de la misma.

Se plantean aquí las líneas de búsqueda de información, pero se recalca la importancia de llenar estos datos con información real y acotando cada uno de ellos con datos ciertos.

- Composición:

La composición del enemigo si bien no es clara, se puede agrupar a través de los distintos centros de confluencia, de carácter Universitario, Gubernamental, Centros de ocio, centros de formación básico y avanzado, clubes, "sectas", etc.

- Disposición:

Si se logra ir componiendo grupos (apartado anterior), en este punto se tratará de ir creando los organigramas de los mismos, determinando asociaciones entre ellos.

- Localización:

Se trata aquí de su ubicación física real, y de ser posibles, rangos de direcciones, nombres, ISP, empresa, etc.

- Movimiento o no:

Una enorme ventaja que se posee aquí es que la masa de los sitios web que analizan vulnerabilidades, o exploits, suelen hacer alarde y publicar sus “logros”. En este apartado, se analizará justamente estos “movimientos de enemigos informáticos”, es decir como es la secuencia de avance (movimientos) de cada vulnerabilidad.

De lo estudiado en este trabajo, una conclusión que se considera muy importante es que la masa de los ataques serios a redes necesitan bastante tiempo para la obtención de información del “blanco”, durante este lapso se realizan distintos movimientos para obtener información de distintas fuentes, hasta completar un cuadro de situación, sobre el cual recién se comienza a testear las posibles vulnerabilidades sobre las que se irá avanzando. Estos son los verdaderos movimientos enemigos.

- **Potencia conocida:**

La potencia es la capacidad de acción que posee un enemigo, no es lo mismo la potencia que tendrá un grupo de enemigos básico que la que poseerá una Universidad, un grupo Gubernamental, o un grupo experimentado en ataques. Es muy difícil cuantificar estos conceptos, pero sí es posible realizar prioridades de unos con otros para saber con quien se está enfrentando, llegado el momento.

- **Identificación:**

Nuevamente aquí en muchos casos se hace difusión de los distintos grupos, en esos casos, se tendrá bastante allanado el trabajo. La diferencia fundamental aquí radica en los ataques cuyo objetivo no es la satisfacción personal, sino el robo de información que tratarán de mantener el anonimato como medida principal.

(2). Información particular de esta red:

Se detallarán aquí todas las acciones realizadas en el ámbito de interés de la red administrada. El aspecto que mayor interés se tiene en este trabajo es el monitoreo permanente de la actividad de la red, la razón principal del mismo es la obtención de información. Esta información es la que se deberá desmenuzar aquí, desde lo global a lo particular. Es por este motivo que es muy importante el apartado anterior (Información general), pues si se conoce la metodología que se emplea como mecánica global, al detectar alguna actividad suele ser muy fácil relacionarla con esta, y volcarla aquí con los datos que afecten en forma particular a este sistema.

- **Composición:**

¿Cuántos son?, ¿Quiénes son?, ¿Qué grupos?, ¿Qué antecedentes poseen?

- **Disposición:**

¿De quién dependen?, ¿Cómo están organizados?, ¿Qué apoyo tienen?

- **Localización:**

¿Adentro o afuera?, ¿Desde dónde atacan?, ¿Direcciones, nombres, puertos?, ¿ISP?, ¿Se puede seguir el rastro?, ¿Hasta dónde llegó?

- **Movimiento o no:**

Secuencia de actividades detectada, secuencia de avance, ¿Es un ataque conocido?, ¿En qué horarios operan?, ¿Con qué periodicidad?

- **Potencia conocida:**

¿Qué herramientas poseen?, ¿Qué nivel de capacitación?, ¿Qué ancho de banda en total?

¿Qué tiempo disponen?, ¿Borraron registros?, ¿Modificaron Rutas?, ¿Modificaron Información?, ¿Qué privilegios de acceso obtuvieron? ¿Vulneraron nivel físico?

- **Identificación:**

¿Suplantan a alguien?, ¿Contraseñas?, ¿Dejan rastros (Registros)?, ¿Hackers, crackers, investigadores, ególatras, criminales, terroristas, competencia, Gobierno, empleados propios, administradores propios?

(3). Impresión:

Se registrará aquí los supuestos sobre la evolución de la actividad enemiga en particular sobre un hecho, para poder ir analizando los diferentes cursos de acción para cada supuesto. Se tratará de dejar asentado los mismos luego de la evolución de cada detección hayan sido correctos o no, pues los mismos servirán de referencia para posteriores

hechos, los cuales se podrán ir analizando con mayores elementos de juicio, y teniendo en cuenta que no solo se aprende por lo correcto sino también por el error. Los aspectos básicos a tener en cuenta son:

- ¿Es real?
- ¿Qué Quieren? (Ver, robar, destruir, inutilizar, negar acceso, etc).
- ¿Hace cuánto están?
- ¿Qué han logrado?
- ¿Cuáles son los próximos pasos?
- ¿Qué grado de peligrosidad se le asigna?
- ¿Qué impacto pueden causar?
- ¿Qué medidas se deben empezar a analizar?
- ¿Han cometido errores?

b. Fuerzas Propias

(1). Unidad Superior

Este punto se debe tener en cuenta cuando la misma sea parte de una red corporativa y tenga accesos hacia niveles superiores de administración de red.

En estos casos, la seguridad deberá ser estrictamente dependiente de las medidas globales impuestas a toda la red, las cuales se deberán expresar aquí, y recién después de estas se particularizarán las que se tomen dentro del ámbito de esta orden de operaciones, es decir las de responsabilidad de este administrador.

(2). Unidades adyacentes

Este caso es común en empresas que tienen interconectadas distintas sucursales sin ninguna jerarquía administrativa entre ellas.

La seguridad global dependerá de la suma de las seguridades en cada una de ellas. Recordar siempre que “una cadena se corta por el eslabón más fino”.

En estos casos se detallarán aquí:

- Tipos de vínculos de conexión (Protocolos, anchos de banda, empresas prestadoras, etc).
- Administración de los dispositivos de interconexión (Router, Switch, modem, etc.).
- Niveles de acceso.
- Permisos de acceso (Nombres, direcciones, puertos).
- Horarios de acceso.
- Monitoreo de los vínculos.
- Medidas de seguridad combinadas.
- Métodos de autenticación empleados.
- Dispositivos de seguridad entre las redes.
- Vínculos de salida al exterior de las otras redes.
- Relaciones entre los dominios administrados.
- Derechos y obligaciones de los administradores de las otras redes.

(3). Otras Unidades:

Este apartado es la analogía exacta de un socio de negocios o “Partner”. Estas redes no forman parte de la red local, sin embargo en muchos casos se encontrarán conectadas a través de distintos tipos de acceso, los cuales presentarán mayor o menor grado de seguridad. Es por esta razón que se incluyen aquí.

Los detalles a tener en cuenta son los mismos que en el apartado anterior, al cual debería sumarse:

- Descripción de cada empresa.
- Descripción de los administradores de red externos.
- Responsabilidades en cada vínculo.
- Dispositivos propios de seguridad.
- Medidas particulares en estos accesos.
- Transitividad de los accesos (Si se deja acceder a A a esta red y A deja acceder a B a la suya, ¿puede acceder B a esta red?). ¡Especial atención a esto!

c. Agregaciones y Segregaciones

En este punto se deberían incorporar conexiones transitorias o enlaces que por su duración no deban ser contemplados dentro del plan general. Si bien este empleo no es habitual, se presenta en extensiones de redes que se implementan para determinados congresos, presentaciones, stands, puestos móviles, apoyo a comunidades, eventos deportivos, etc. los cuales por su corta duración no merecen ser incorporados en forma permanente.

Estos casos son agregaciones cuando se incorporan a la red para acceder a los recursos de la misma. Contemplados desde el otro extremo, es decir si una determinada subred o parte de los recursos de la misma se desplazan hacia otra zona transitoriamente, como pueden ser también los ejemplos recién citados, para una cierta demostración o aplicación de corta duración (estos casos se han visto por ejemplo al montar sistemas de encuestas o estadísticas en procesos electorales o eventos deportivos como olimpiadas, campeonatos internacionales, etc) que deben mantener ciertos accesos a sus bases de datos pero no a través de los vínculos habituales sino por medio de otras redes o canales de comunicaciones; estos casos pueden ser vistos como segregaciones.

d. Impresión personal del Jefe:

“Resume brevemente la evaluación que el Jefe hace de la situación, asegurándose de que los supuestos son lógicos, reales y establecidos de una forma positiva”.

Si se prestó atención al trabajo realizado hasta aquí, se puede apreciar que se cuentan con los elementos de juicio necesarios para hacer una apreciación inicial de cómo se encuentra la relación costo/beneficio en un caso de presencia concreta de intrusos, basado en la experiencia general recolectada a lo largo de un intenso trabajo de investigación y actualización de hechos producidos y declarados y en particular sobre la información que se haya sabido recolectar de la actividad actual de la operación que se esté planificando. Se pueden realizar algunos de los siguientes planteos que se proponen como ejemplo:

- Se puede continuar o no con la presencia enemiga.
- Dejar superar la línea actual.
- Continuar recolectando información.
- Se encuentra ante un recurso crítico del sistema.
- Es necesario desviar su atención.
- Se aprecia con bajo, medio o alto grado de peligrosidad.
- Se necesitarán determinados recursos.
- Se estima una duración de n días.
- Tomar determinadas medidas o contra medidas.
- Preservar determinados recursos.

- Iniciar algún tipo de operación de engaño o de seguridad.

2. MISIÓN:

La empresa XXX iniciará una acción retardante para desgastar el esfuerzo de una intrusión a partir que la misma es detectada en cualquiera de las interfaces hasta que se logre minimizar el riesgo a valores previamente aceptados, intercambiando permanentemente información que no cause impacto y desviando los ataques hacia zonas previamente establecidas, con la finalidad de ganar el tiempo suficiente que permita llegar al fondo de las causas para erradicar futuras agresiones.

3. EJECUCIÓN:

Aquí se desarrolla el ¿CÓMO? de la operación, todo aquello que por su extensión dificulte la comprensión de este apartado es aconsejable incluirlo como anexo. Esta situación se presentará con la topología (planos de la red), la gráfica de los vínculos, el detalle de los recursos, los planes de contingencia de cada línea, etc.

a. Concepto de la Operación:

El concepto de la operación estará basado en el **diseño de líneas de retardo**, pensadas desde afuera hacia adentro, y en las cuales se tendrá en cuenta fundamentalmente lo siguiente:

- Topología de las mismas (Configuración).
- Accesos y comunicaciones
- Interconexión de zonas.
- Recursos expuestos.
- Acciones a tomar.
- Contra medidas.

Por último se definirá la línea de retardo final (LRF) o línea a no ceder, donde solo se encontrarán los recursos a los cuales no se deberá llegar, sin autorización. Se implementarán medidas para tener absoluta certeza que no podrá permitirse la llegada de un intruso. El principio rector es que todo aquello sobre lo que no se está seguro debe ser excluido de esta zona.

Sobre cada zona se analizarán las operaciones complementarias (Información, Seguridad, Decepción, Contra ataques) particulares a cada una de ellas.

b. Maniobra:

Línea de retardo 1 (Internet):

Esta línea es la frontera con un usuario totalmente desconocido sobre el cual rigen los siguientes principios:

- No se implementarán medidas de validación.
- No se interactúa de ninguna forma.
- La información presente debe ser estática no permitiendo su modificación.
- La sensibilidad de esta información es nula pues es evidentemente PUBLICA.
- Las actualizaciones se realizarán reemplazando la información antigua, por la nueva en su totalidad, un curso de acción muy útil es el de servidores basados en CD en vez de discos rígidos, los cuales no permiten su modificación.

- Los recursos de esta línea tendrán el mayor grado de exposición, por lo tanto no deberán causar ningún impacto a la organización.
- Topología:
 - La conexión a Internet por lo general será permanente, a través de vínculos dedicados.
 - En lo posible se constituirá una red físicamente aislada del resto.
 - Si los parámetros de diseño lo permiten, los servidores de esta zona se encontrarán en la misma sala de servidores de toda la red.
 - Accesos y comunicaciones.
 - El router de acceso (frontera) de ser posible debería ser uno, en particular aislado del resto de la red, de no ser posible debería contar con más de una interfaz para configurar distintas listas de acceso en cada una de ellas.
 - No deberá accederse a un switch o hub que a su vez permita la conexión con otra zona de retardo.
 - Una buena medida es la de cascadas de router antes del acceso a esta zona.
 - El administrador de estos recursos en lo posible lo hará en forma local, negando todo tipo de acceso remoto.
 - Recursos expuestos:
 - Los recursos típicos de esta zona son los servidores web y ftp.
 - Acciones a tomar.
 - La medida básica a tomar es la obtención de información del enemigo, registrando los intentos fallidos de modificación de datos, para ir conociendo los grados de avance potenciales.
 - Se implementarán herramientas para generar alarmas y prevenir ataques de negación de servicio.
 - Ataques conocidos en esta zona:
 - Aquí comienza normalmente la actividad enemiga.
 - El ataque típico es inicialmente la obtención de información por medio de las direcciones IP alcanzadas, luego la determinación de los puertos abiertos, la configuración de la red, y por último la investigación de sistemas operativos y hardware a través de ataques ICMP o TCP/UDP.
 - Negación de Servicio.
 - Modificación, robo, o agregación de información.
 - Contra medidas:
 - La primera contra medida es el resguardo de los archivos de registro de la actividad enemiga (logs).
 - La segunda medida es la determinación del origen de la actividad de rastreo. Sobre esta actividad existen tres posibilidades:
 - Ataque directo desde una dirección IP real (muy poco probable, principiante). Si se puede realizar un monitoreo de puertos sobre esta dirección IP origen y no se encuentra abierto ningún otro puerto sospechoso, es altamente probable que desde aquí provenga el ataque. Puede suceder también que tenga un puerto en escucha, en este caso es muy probable que a través de este se conecte el enemigo, si este fuera el caso, se trataría del párrafo siguiente.
 - Ataque a través de una dirección IP falsa. En este caso el enemigo inserta un gusano en una víctima inocente, deja un puerto en escucha y desde esta lanza el ataque (o a través de esta se pasa a otra y así sucesivamente). La única ventaja que posee esta opción es que así como alguien pudo insertar un gusano en esta IP inocente, se puede hacer lo mismo, y a través de este gusano "amigo", monitorear que puertos tiene abiertos esta primera víctima, luego determinar

con qué dirección IP tiene conectado este puerto y de esta forma se determina el próximo salto a investigar.

- Ataque a través de servidores de Internet, IRC, MP3, etc. Esta es la peor de las alternativas pues es realmente difícil de determinar, pues suele suceder que estos gusanos, habitualmente llamados "bots", se preparan para realizar esta actividad a una hora determinada, y luego de finalizada la tarea, se comunican con su gestor o este lo hace en el momento en que desea y recolecta la información obtenida. Ante este caso lo más eficiente suele ser modificar la información que queda almacenada para que cuando sea consultada, contenga datos falsos. En el mejor de los casos se puede permanecer escuchando ese servidor para determinar la IP enemiga.

En cualquiera de los tres casos, la mejor medida a para comenzar una **acción retardante** es implementar una consola "generadora de datos falsos", es decir el empleo de una consola monitoreo de actividad enemiga de obtención de información, lo cual es muy fácil pues se estarán probando con distintas herramientas las direcciones IP activas y los puertos de cada una de ellas, lo cual es un síntoma claro de actividad anormal. Al detectar esta actividad, se debe tener en cuenta las tablas de determinación de Sistemas Operativos y Hardware del artículo mencionado anteriormente, y generar en la consola patrones falsos, los cuales deberán ser la respuesta ante este ataque, enmascarándolas con las verdaderas.

- En el caso de negación de servicio, uno de estos ataques está tratado en detalle en un artículo de Gibson Research Corporation en la página web www.grd.com con el título "*Denial of Service*", 2001, cuyo autor es Steve Gibson. Y aquí propone una metodología empleada muy útil de seguimiento, pero la realidad es que es muy difícil de contrarrestar. La acción retardante sobre este ataque es la obtención de información sobre el enemigo de todo tipo, y el inmediato contacto con el ISP.
- Si se logra determinar fehacientemente los responsables y obtener pruebas, se pueden implementar acciones legales.
- Se pueden plantear contra medidas de contra saturación, pero no se aconsejan.

Línea de retardo 2 (Customnet):

Se creyó conveniente incluir en este trabajo, por primera vez este concepto, por la característica particular en la que se encuadra un usuario que se hace presente en una red y esta la permite interactuar en base a una cierta información que este proporciona y que una vez identificado tiene ciertos privilegios para personalizar su entorno, por esta razón se creyó oportuna su denominación como **CUSTOMNET**. Debe quedar claro que el grado de veracidad que posee la información del usuario es NULO pues no se toman medidas de detalle en su verificación.

Esta línea es la frontera con un usuario al cual se le puede realizar una validación de acceso, pero la cual no es verificada en forma personal:

- No se implementarán medidas de verificación de información del usuario.
 - A lo sumo se puede plantear un intercambio inicial de contraseñas por correo electrónico para registrar un buzón destino.
 - El usuario tendrá acceso a ciertos recursos de la red, en particular a espacios de discos rígido.
 - La sensibilidad de esta información a la que accede continúa siendo nula pues es evidentemente PUBLICA.
 - Los recursos de esta línea tendrán el alto grado de exposición, por lo tanto no deberán causar ningún impacto a la organización.
 - Los ejemplos típicos son aquellos en los cuales un usuario dispone de espacios de almacenamiento para poder crear sus propias páginas web, cuentas de correo electrónico, almacenamiento de archivos, etc.
- Topología: (Similar a la anterior)
 - Accesos y comunicaciones (Similar a la anterior).

- Recursos expuestos:
- Acciones a tomar.
- Contra medidas:

Línea de retardo 3 (Extranet):

Esta línea es la frontera con un usuario ajeno a la organización pero totalmente conocido e identificado. También formarán parte de esta zona los usuarios de la organización que por sus características o metodología de trabajo no se les pueda incluir en una zona de seguridad extrema. Puede ser subdividida también en dos sub zonas con diferentes niveles de seguridad. En esta zona rigen los siguientes principios:

.....

Línea de retardo 4 (LRF o Intranet):

Esta la línea a no ceder.

- Todo lo que no se conoce está fuera de control. Esta es la regla por excelencia, es decir si dudo sobre una determinada medida, esta se saca de la zona.
- Es una zona muy restrictiva donde el usuario no podrá contar con muchos de los servicios que quisiera tener.
-

NOTA: En este trabajo, no se trata en detalle cada línea por la síntesis realizada del original, en virtud del tiempo disponible.

c. Apoyos:

En este apartado se debe contemplar todo elemento que pueda proporcionar algún tipo de solución o justamente como su título lo identifica "apoyo" a la operación. En el caso de la operación informática, lo que se debe reflejar aquí son:

- CERT(s).
- Fabricantes de Software y Hardware de elementos del sistema.
- Proveedores.
- Listas de discusión y de correo.
- Páginas web de consulta.
- ISP(s).
- Personas de referencia.
- Apoyos legales y medios de difusión.
- Otros administradores vecinos.
- Comunicaciones de interés.

d. Operaciones de Seguridad (OPSEC):

El concepto de OPSEC en la OTAN, es el conjunto de todas las medidas adicionales que se deben tomar para proporcionar un grado adicional de seguridad, a toda operación que se lleve a cabo, mediante el empleo de elementos

pasivos o activos, a fin de asegurar que se impide al enemigo el conocimiento de dispositivos, capacidades, intenciones y vulnerabilidades propias.

Esto en la actualidad se toma como obligatorio, pues hace pensar más allá de toda la operación planificada, ¿Qué más se debe incluir? Para impedir al enemigo el conocimiento de dispositivos, capacidades, intenciones y vulnerabilidades propias.

Se deberá tratar de ocultar en lo posible todo, pero de no poder hacerlo, se deberá identificar aquellos aspectos que se consideran vitales para el sistema. Un enfoque muy práctico es realizar actividades desde el punto de vista del enemigo y realizar estimaciones de lo que se puede descubrir de cualquier indicador del propio sistema.

Aspectos a tener en cuenta:

- Globalidad: La OPSEC debe comprender todas las actividades del sistema, como son: Administración, logística, comunicaciones, movimientos, instalaciones, personal, etc.
- Información crítica: se debe determinar qué información es crítica para el enemigo, pero no la que se encuentra en los servidores, sino qué cuentas de usuario, contraseñas, cuentas de correo, nombres, direcciones, datos de personal, organización de la empresa, el sistema y la red, etc.
- Punto de vista del enemigo: Lo importante aquí es que en Internet, existe más de una clase de enemigos, por lo tanto es útil analizar desde el punto de vista de cada uno de ellos.
- Oportunidad: Horas críticas, fechas clave, al realizar cambios, durante movimientos o resguardo de información.
- Análisis de sistemas: Seguridad de programas, procedimientos, instalaciones fijas o aisladas, puestos de trabajo, documentos, equipos, gabinetes, vínculos, etc.
- Contramedidas: Cuando la protección no es posible o ya está comprometida, pueden iniciarse cambios en el plan o llevar a cabo operaciones de decepción.

El propósito fundamental es impedir que el enemigo obtenga inteligencia, evitar ser sorprendido y preservar la eficacia del sistema. Este plan debe ir más allá de las medidas de seguridad tomadas en cada línea de retardo, es decir comprende el conjunto de medidas globales para ajustar al máximo el conjunto, pero que no están contempladas en el resto de la orden.

Los aspectos clave donde se suele presentar fugas de información y deben ser especialmente tenidos en cuenta en este punto son:

- Capacitación de los usuarios contra Ingeniería social.
- Envíos de información por correo electrónico sin medidas de confidencialidad.
- Listas de correo.
- Clasificación de la difusión de las medidas de seguridad de los sistemas (cada nivel de usuarios debe conocer solamente los derechos y obligaciones que a él le competen).
- Tareas que se transforman en rutinarias.
- Medios de resguardo de la información.
- Elementos de baja o modificados (esta es la principal fuente de obtención de información), documentos, diskette, discos rígidos, PC, robos o pérdidas de notebook.
- Áreas de la empresa.
- Personal que deja la empresa.
- Redundancia en los recursos.
- Proveedores y clientes.

e. Operaciones de Información:

Este tipo de operaciones que también deben ser tenidas en cuenta como complemento de cualquier otra operación, detallan la metodología a seguir para toda información que salga de la empresa. Esta es la que debe analizar y determinar:

- Los distintos niveles de difusión de la Orden de operaciones, pues no deberá ser igual para todos los usuarios.
- La cantidad y veracidad de información que marketing puede difundir en cuanto a la parte Informática de la Empresa.
- El tratamiento a seguir al detectarse un incidente con los medios de difusión.
- El tratamiento a seguir una vez que los medios de difusión tomaron conocimiento del hecho.
- El valor y la cantidad de la información que se entrega al enemigo en las líneas de retardo.
- Un dato real (aunque no debería ser escrito) es a partir de cuándo, cómo y qué información se dará a los niveles superiores de la empresa ante un incidente. Se especifica aquí este punto para tratar de ser lo más sincero posible en este trabajo, pues es un interrogante que se ha visto presente en muchos casos de penetración a redes.

f. Operaciones de engaño (decepción):

Esta operación se considera la principal de las propuestas en este trabajo como complemento a la acción retardante, es apasionante el estudio de medidas de este tipo que se han tomado en algunos sistemas y es un desafío personal para cualquier administrador de sistemas el llevar al éxito estas medidas. La satisfacción que produce el lograr engañar un intruso, no tiene comparación con ninguna otra medida tomada en las tareas de administración de sistemas.

Se define como decepción el conjunto de medidas concebidas para engañar al enemigo mediante la manipulación, distorsión o falsificación de la evidencia con el fin de inducirle a reaccionar en forma perjudicial para sus intereses. Su finalidad es conseguir sorpresa, mantener la seguridad, incrementar la libertad de acción, engañar al enemigo y minimizar el gasto de tiempo y recursos.

Los principales detalles a tener en cuenta son:

- Finalidad: Se debe especificar claramente para qué se toma cada medida y los resultados deseados.
- Preparación: Debe estar dirigida a un objetivo específico, es decir se debe saber con certeza a que nivel de agresión se corresponde.
- Credibilidad: Nunca debe verse como incongruente o ilógica y debe estar de acuerdo con los acontecimientos que el enemigo razonablemente espera.
- Corroboración: Se deben presentar los indicadores falsos o verdaderos por la mayor cantidad de fuentes posibles.
- Tiempo: Al enemigo hay que darle tiempo suficiente para que perciba, interprete y reaccione ante la información falsa, pero no demasiado, ya que esto le permitiría analizarla con más detalle pudiendo descubrir la decepción. Ningún objetivo puede engañar constantemente, toda decepción tiene un tiempo de vida limitado.
- Seguridad: La información debe ser difundida de forma tal que la ausencia de normas usuales de seguridad no levante sospechas, pero respetando seriamente las medidas de seguridad de la información a la cual no se desea dejar acceder.
- La mente humana: Esta cualidad humana tiene varias tendencias que la hacen susceptible para la decepción: ideas preconcebidas, pensamiento anhelante, deseo de aclarar las incertidumbres, tendencia a filtrar la información y el efecto hipnótico de la información regular

Seis etapas se deben relacionar al elaborar un plan de decepción:

- Situación: ¿Qué es verdad?.
- Objetivo: ¿Cuál es el objetivo de la decepción?.

- Percepción: ¿Qué queremos que crea el enemigo?.
- Mensaje: ¿Qué es lo que le decimos?.
- Medios: ¿Cómo se lo decimos?.
- Realimentación: ¿Hay alguien escuchando?

Un detalle más a no olvidar es la contradicción. Pues es necesario también que en estas operaciones exista un responsable que analice todas las fuentes de información proporcionando una base de defensa contra estas acciones que también las va a realizar un intruso. Los aspectos más importantes de este perfil son: Mente abierta, conocimiento del enemigo, discernimiento, escepticismo, evitar sacar conclusiones precipitadamente, búsqueda continua de la confirmación, atención a las anomalías y desconfianza a las interpretaciones automatizadas (Un caso muy preciso de este último son las reglas Smart de los firewalls).

Las implementaciones de este tipo pueden contemplar:

- Zonas de sacrificio.
- Servidores web y ftp de información de muy bajo impacto.
- Falsos servidores.
- Generadores de información falsa ante ataques de descubrimiento IP- ICMP-UDP-TCP.
- Apertura de falsos puertos.
- Redireccionamiento hacia direcciones IP de la organización no utilizadas.
- Mantenimiento del "perfil bajo del sistema".
- Nombres de recursos contradictorios.
- Envíos de falsos correos.
- Generación de tráfico falso.
- Colocación de falsos routers o rutas falsas.
- Falsos segmentos de red.
- Participación con seudónimos en grupos de Hacking.

h. Otros cuando se necesiten.

Se puede agregar aquí cualquier otra operación que deba formar parte del sistema de seguridad.

x. Instrucciones de Coordinación

Contiene las instrucciones globales aplicables a dos o más elementos de la organización.

Contiene cualquier prescripción necesaria sobre:

- Objetivos tanto finales como intermedios.
- Ritmo de la maniobra.
- Líneas de coordinación.

4. LOGÍSTICA

Es la expresión clara y concisa de los recursos materiales necesarios para la maniobra (antes, durante y después de la operación), sin entrar en detalles técnicos que competan a cada uno de los organismos.

Referirse a anexos, si se necesita.

a. **Concepto General del Apoyo Logístico**

Detallando aquí la planificación por etapas o fases para llevar a cabo y mantener vigente por un período de tiempo establecido toda la acción retardante.

b. **Material y Servicios**

- Abastecimiento
- Mantenimiento.
- Desplazamientos.
- Trabajo.
- Obras.
- Servicios.
- Cursos, congresos, seminarios.
- Bibliografía.
- Actualizaciones de software y hardware.

c. **Personal:**

Detalle del personal necesario para toda la operación, teniendo en cuenta también el asesoramiento de especialistas en casos de incidentes, o la asistencia técnica de software o hardware.

d. **Varios:**

Cualquier otro recurso adicional no contemplado anteriormente.

5. MANDO Y TRANSMISIONES

a. **Mando**

Refleja la ubicación, datos, direcciones, mail y TE de toda la cadena de comandos.

b. **Comunicaciones:**

Se refiere aquí a todos los medios de comunicación que posee el sistema para llevar a cabo la misión, no es el detalle de cada uno de los vínculos, los cuales fueron referidos en cada línea de fase, sino el resto de las comunicaciones que se posee.