CIBERDEFENSA, DE LOS MONJES SHAOLIN A LA CIBERINTELIGENCIA

RODRIGO CÁRDENAS HOLIK*

Ingresando al templo

Como todo entrenamiento marcial, se comienza desde pequeño, para preparar la mente, el espíritu y el cuerpo para el futuro. El camino es arduo, el aire falta, la altitud es mayor a cada paso, tenemos miedo, pero tenemos que recorrerlo para saber defendernos, para que si nos atacan, sepamos responder. Tomará tiempo y deseo, pero es nuestra energía la que nos llevará a encararlo con entereza. Nos recibe el maestro, nos muestra el entorno, vemos a nuestros hermanos –algunos muy avanzados– y tememos hasta mirarlos, y sabemos que es en serio, que no hay retorno.

La decisión de establecer un esquema de ciberdefensa como parte de la Defensa Nacional comienza por el hecho de reconocer que existen amenazas y que es necesario aprender de ellas, de cómo atacan, qué atacan, sus fortalezas, nuestras debilidades. El entorno

*Licenciado en Sistemas de la Información (Universidad del Salvador) y magister en Seguridad Informática (Universidad Internacional de La Rioja). Analista del Ministerio de Seguridad y docente de Ciberseguridad en la Facultad de la Defensa Nacional (UNDEF).

de las tecnologías de la información y las comunicaciones poseen un factor de valor para las diferentes organizaciones que coexisten en un ecosistema real, pero así como pueden ser utilizadas con fines benéficos, también pueden serlo con el fin opuesto.

Y así como la doctrina lo especifica, nosotros debemos defendernos de los ataques de otros. Es por ello que es posible que hayamos sido víctimas y hayamos sabido responder, o al menos percibimos que en algún momento podemos ser víctimas.

En primer lugar, es crítico que hagamos una evaluación sobre el estado en el que nos encontramos. ¿Entendemos que antes de la ciberdefensa debemos tener una adecuada ciberseguridad? ¿Las autoridades entienden la criticidad de la información y del valor que posee como activo? ¿Se conoce la normativa vigente local? ¿Existen buenas prácticas internacionales que podamos importar y adaptar a nuestro escenario?

Estos interrogantes, entre otros, deben ser respondidos en forma honesta, para así saber cuál es el punto de partida para poder crecer y tener una madurez donde todos los actores que participan del esfuerzo de obtener, procesar, almacenar, eliminar y transmitir información cumplan con su papel dentro y fuera de la organización.

Si bien no nos hemos elevado al nirvana, sí hemos experimentado algún grado de iluminación, en el sentido en que somos conscientes de nuestras limitaciones.

Nuestro primer contacto con la ciberdefensa personal es el hecho que hay una política de seguridad de la información, que debe estar escrita, actualizada, comunicada, aprobada y apoyada por los más altos rangos de una organización.

En este documento, vivo y por ende no estático, se establecen las reglas sobre qué debe protegerse y la respuesta ante esa necesidad. Pero como en cualquier disciplina marcial, existe detrás una serie de conceptos, ideas y principios que deben ser expuestos y entendidos por todos, y del devenir de la práctica más visible, se verá la necesidad de un basamento metodológico consensuado y que la teoría le dará un recinto de descanso a la práctica.

Deberemos meditar en el Wuguan si existe una diferencia entre seguridad de la información y la seguridad informática. Sin duda, hay grandes discusiones al respecto, y distintos profesionales y expertos esgrimen conceptos válidos y diametralmente opuestos. No estamos ajenos a tal conflicto, no porque sea negativo, sino porque no establece una definición clara. El punto de partida ya es difuso y el camino adelante se abre en demasiados brazos.

Uno de los puntos de vista es la protección de los activos de información para que mantengan la confidencialidad, integridad y disponibilidad, lo que permite que la organización arribe a sus objetivos mitigando en forma efectiva los riesgos. Otra es que se deben proteger los contenedores de información, el acceso de los usuarios a éstos, cuando ellos lo necesiten. Ahora piensen cuál corresponde a la seguridad informática y a cuál a seguridad de la información. Hasta que no hagamos clara la imagen en nuestra mente, no podremos ver el horizonte, ya que la niebla se interpondrá ante nuestros ojos y nos cegará.

Luego de una meditación y desbloqueando los chakras, sentimos el chi fluir y entramos en un estado de conciencia pleno para distinguir las diferencias. Comprendemos ahora que la seguridad de la información va más allá de lo que conocemos como seguridad lógica y la administración de usuarios y sus perfiles, que se aplica a la organización, a su personal, a sus objetivos, a sus procesos, a sus funciones, a lo lógico y lo físico. Es decir, que la información, en el estado en que se encuentre, debe estar protegida desde su ingreso hasta su eventual eliminación.

Mi primera clase

Estoy en este templo para aprender a defenderme y, por lo tanto, lo primero que me muestra el maestro es una pelea entre los alumnos más avanzados, para ver lo que me falta y a lo que tengo que prestarle atención, ya que puedo ser yo el que reciba algunos de

los ataques y debo saber cómo neutralizarlos, evitarlos, e incluso responder; y de cualquier manera, que el resultado final sea poder seguir con vida.

Eso significa que tengo que saber que hay riesgos y que debo ver cómo debo responder a ellos. Eso lo entiendo, pero, ¿qué es un riesgo y qué respuesta útil hay?

Primero, entonces, debemos definirlo, y una posible concepción es que el riesgo es un evento que, de materializarse, es decir, si se hace realidad, puede afectarme y evitar que cumpla con mis deseos. Pasado a un entorno organizacional, puede causar daño y evitar que se cumplan los objetivos.

Acto seguido, tomo en consideración que el riesgo tiene una probabilidad de ocurrencia, por ende no es 100% seguro, pero tampoco puedo decir que nunca me va a pasar nada. Como dice el viejo adagio, una grulla no anida en la madriguera de los leones.

¿Hay una graduación del riesgo? ¿Puede crecer el riesgo? ¿Puede disminuir? ¿Hay resto? Vamos por partes. Primero podemos clasificar el riesgo según el ámbito en el cual se aplica el concepto, y eso atañe a toda organización: riesgo inherente, riesgo de control, riesgo de detección, riesgo de auditoría, riesgo residual, riesgo legal, riesgo contable, riesgo procesal, riesgo de Tecnología de la Información (TI), etc. Como se puede apreciar, el riesgo tiene un amplio campo de acción y afectación, lo que permite inferir que no importa de qué organización o individuo hablemos, el riesgo está a la vuelta de la esquina, latente, expectante, listo para entrar en ebullición, si se dan las condiciones.

Existe una gran cantidad de metodologías de análisis de riesgo, y de la misma manera que en las artes marciales hay distintas escuelas, linajes y maestros, también hay distintas técnicas para distintas realidades y condiciones.

Una opción elegida fue Octave Allegro, con una leve adaptación en cuanto a la clasificación de los riesgos de acuerdo a su probabilidad de ocurrencia y el método algebraico detrás de ese resultado numérico que determinará su nivel y, por consiguiente, su prioridad

en la segmentación y aplicación de respuestas, es decir, la estrategia más apropiada de acuerdo a los objetivos organizacionales.

En este sentido, y debido a la complejidad de los procesos internos, los actores involucrados, los consumidores del producto final, la dependencia estructural y el entorno de TI complejo, que se aplicará el modelo de Mosler para arribar a la ponderación del riesgo.

Otro matiz de importancia de esta metodología, en particular aquellas que deben dar un producto claro en materia comunicacional, en particular para aquellas personas ajenas a los riesgos, y en particular lo de TI, es la entrega de una serie de fichas que surgen del cumplimiento de cada una de las etapas, que se detallarán a continuación, y una planilla final con los hallazgos y medidas a tomarse.

Aplicando esta metodología, primero se deben establecer las directrices de la organización que serán utilizados para evaluar los efectos del riesgo en la misión y objetivos de la organización. La materialización del riesgo se puede evaluar en forma cualitativa y convertirse en la base de su evaluación. Por ello, un criterio de medición del riesgo es importante para asegurar que la visión organizacional sobre cómo mitigar los riesgos es consistente teniendo en cuenta todos los activos de información, sus contenedores y las unidades operacionales que los utilizan.

Además, la gerencia deberá determinar cuáles son las áreas más significativas, ya que el impacto será mayor aún en cada una de ellas, lo que permitirá evaluar la extensión del impacto.

El segundo paso es identificar los activos de información de la organización y crear un perfil de ellos, una representación de aquellos elementos únicos, como funcionalidades, particularidades, características, valor y dependencia. Así, el activo se encontrará descripto en forma apropiada, no habrá ambigüedades, se entenderán los límites de este bien y sus requerimientos de seguridad.

Por supuesto, estos activos de información se encuentran en contenedores donde son procesados, almacenados o transmitidos. Además, la organización deberá tener en cuenta cuáles son

los contenedores que se encuentran dentro de las fronteras institucionales y cuáles fuera, sabiendo que cualquier riesgo donde hay ausencia de control, se hereda en el activo de información. Como resultado, se obtendrá un inventario de estos bienes luego de ser identificados. Se habrán mapeado y, por ende, definido los límites y sus circunstancias singulares que deben ser examinadas por el riesgo.

Esta metodología tiene como valor agregado la percepción de una explotación de una vulnerabilidad. Es decir, que el riesgo se materializa y se percibe su impacto. Para ello, se identifican las áreas de preocupación, que son aquellos escenarios reales que pueden representar amenazas y su correlativo efecto nocivo, mediante la discusión que condiciones o situaciones posibles que pueden afectar los activos de información de la organización. No será necesario listar todos los escenarios, sino aquellos que surjan primero en la mente de los integrantes del grupo de análisis.

Tras identificar estos escenarios de amenazas, se detallarán las propiedades de la amenaza. Pero como este esfuerzo no acompasa todas las variedades, un rango de amenazas adicionales se incorpora en forma de árbol para examinar estar otras alternativas. Cada uno de los escenarios puede afectar a uno o más activos de información, y cada uno de ellos puede estar involucrado en uno o más escenarios, por ello es importante trasladar estas combinaciones a cada rama del árbol. Además, se podrá determinar la probabilidad de ocurrencia, lo que servirá a posteriori para priorizar las actividades de mitigación. Pero como es difícil calcular realmente y cuantificar la probabilidad de ocurrencia, esta metodología traduce el resultado en tres rangos: alto, medio y bajo.

Llegando al corazón de este método, identificamos los riesgos y sus posibles impactos multisectoriales en la organización. Las actividades involucradas en este paso aseguran que las variadas consecuencias del riesgo hayan sido recolectadas.

Después de identificarlos, es necesario analizar los riesgos, de los cuales se deberán tener en cuenta las variadas consecuencias que

conllevan, donde un cálculo cuantitativo mide la extensión en que la organización es impactada por la amenaza. Al priorizar estos criterios de impacto, la organización se asegura que los riesgos están ordenados en el contexto de sus directrices.

El último paso de este proceso es donde las organizaciones deciden qué riesgos de los que han identificado requieren mitigación y desarrollan una estrategia de mitigación para dichos riesgos. En primer lugar, se deben priorizar los riesgos de acuerdo a su valor relativo, obtenido en el paso previo, para luego desarrollar las estrategias que consideran el valor del activo y sus requerimientos de seguridad, los contenedores en los que se hallan, y el particular entorno operacional de la organización.

Mi cuerpo es un arma y cada parte cuenta

Cada disciplina marcial posee un arsenal de técnicas, tanto de defensa como de ataque. Cuando hablamos de la primera, puede ser el canto de la mano, el antebrazo, el codo, la rodilla, el peroné, etc. Para la segunda, tenemos el canto de la mano, la palma, el dorso, los dedos en forma de lanza, los nudillos, el codo, la rodilla, el talón, el empeine, el metatarso, etc.

Para aprender a defenderme tengo que tratar y practicar con cada una de estas secciones del cuerpo y, a mayor complejidad, se requiere un mayor nivel de madurez y responsabilidad, ya que una técnica mal utilizada puede darnos resultados negativos. El desconocimiento o la negligencia son factores que debo desterrar por medio de la práctica constante.

En un mundo cada día más dependiente de las TICs, donde las vulnerabilidades son explotadas por diversos actores, tanto externos como internos de una organización, la mayoría de ellas se visualizan como en su estado operativo, aunque en realidad se debe a un débil esquema o proceso en la etapa preliminar, donde se realiza el relevamiento, el diseño, la programación, la implementación y luego el monitoreo y

soporte post puesta en funcionamiento.

De la misma manera que existen metodologías para el análisis y diseño de software, como lo propusiera Edward Yourdon en su libro Análisis Estructurado Moderno, existen otras que buscan reforzar los conceptos de software seguro como son la confidencialidad, integridad y disponibilidad (la denominada "Santísima Trinidad" de la seguridad de la información), la resiliencia, fiabilidad, robustez, autenticación y la trazabilidad, estas últimas como actividades complementarias.

Existen 12 prácticas y principios de diseño, donde el personal de desarrollo y diseño deben trabajar bajo 2 perspectivas de modelado: defensor, para fortalecer la aplicación y minimizar las oportunidades del adversario, y atacante, para intentar conocer el trasfondo de la amenaza y contrarrestar el ataque aumentando el uso de contramedidas.

Ambos esquemas se basan en una visión interna del software. También existe una taxonomía basada en procesos y orientación del evento, para poder determinar, con un fin prospectivo, los tipos de ciberatacantes que pueden ofuscar las capacidades y limitaciones del desarrollo, y luego priorizar los tipos de ataques para enfocar el esfuerzo de la mejor manera posible.

Los S-SDLC, como evolución de los SDLC, que entran en juego como forma de mitigar, antes de la puesta en operación, los riesgos en cada una de las etapas internas en el diseño y el desarrollo.

Como parte del proceso de diseño y desarrollo seguro de un sistema informático tendiente a obtener un sistema informático seguro, es necesario tener un enfoque adecuado en cuanto las técnicas de control a utilizar para validar el cumplimiento de cada etapa de este proceso, en particular el denominado modelado de amenazas. Para ello, existe una gran variedad de metodologías.

En primer lugar, debemos exponer que los enfoques de estas metodologías determinan lo que van a visualizar, ponderar y concluir. En ese sentido, debemos presentar las 3 perspectivas:

• Centrada en el software: este enfoque involucra el diseño del sistema y puede ser ilustrado utilizando diagramas de arquitectura del software como diagramas de flujo de datos (DFD), diagramas de casos de uso o diagramas de componentes. Este método es normalmente utilizado como modelo de amenazas de redes y sistemas y ha sido adoptado como el estándar de-facto para el modelado de amenazas.

• Centrada en el activo: refiere a identificar los activos de una organización confiada a un sistema o software. Los activos son clasificados de acuerdo a la sensibilidad de los datos y su valor intrínseco a un atacante potencial, para priorizar así los niveles de riesgo. Se utiliza este enfoque para el modelado de amenazas. Pueden ser generados árboles de ataque, grafo de ataque o mostrar patrones para los cuales un activo puede ser atacado.

• Centrada en el atacante: requiere de perfilar las características de atacante, su conjunto de habilidades y motivación para explotar vulnerabilidades, y luego utilizar esos perfiles para comprender el tipo de atacante que podría ejecutar más posiblemente tipos específicos de explotaciones e implementar una estrategia de mitigación adecuada. También se utilizan diagramas de árbol, ya que al focalizarse en los objetivos del atacante prevemos las diferentes consideraciones relacionadas al sistema donde el ataque puede ser perpetrado, junto a su software y activos, cómo el ataque se despliega, y finalmente, la manera de detectar o mitigar dicho ataque.

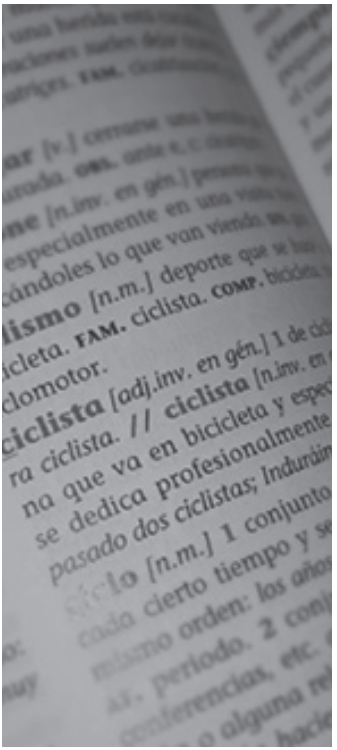
Con el fin de comprender mejor el escenario, las metodologías de modelado de amenazas utilizan una representación visual para cumplir tal objetivo, como se expresa en los párrafos previos. La aplicación o la infraestructura son descompuestas en varios elementos para asistir al análisis, por lo que se pueden identificar y enumerar potenciales amenazas en distintos lugares o etapas del procesamiento de información. A continuación, se mencionan las más utilizadas:

• Árboles de ataque
• Redes de Petri

- Diagramas de flujo de datos
- Diagramas de actividades o flujo de procesos

Es importante mencionar que, además de los aditamentos mencionados arriba, algunas organizaciones han desarrollado herramientas informáticas para automatizar el proceso de reflejo de las metodologías, como por ejemplo Threat modeling tool, de Microsoft (antes conocida como SDL Threat modeling tool); ThreatModeler, de MyAppSecurity; securiCARD, de foreseeti; SD Elements, de Security Compass; y Irus Risk, de Continuum Security.

PASTA es una metodología, como tantas otras. Se vale de una serie de vocablos que tienen un significado y relevancia particular, por lo que antes de adentrarnos en PASTA, es necesario especificarlos y definirlos brevemente.



Taxonomía de términos

Activo: es un recurso de valor. Puede ser tangible como un escritorio, o intangible, como la información o la reputación.

Amenaza: es un evento no deseado. Una ocurrencia potencial usualmente descripta como el efecto que puede dañar o comprometer un activo u objetivo.

Vulnerabilidad: es una imperfección en el código del software del sistema, red u otro nivel que hace posible una explotación.

Ataque (o explotación): es una acción tomada que utiliza uno o más vulnerabilidades para materializar una amenaza.

Contramedida: acciones tomadas para reducir la probabilidad de ataques o el impacto de las amenazas. No apuntan directamente a las amenazas, sino que apuntan a los factores que las promueven.

Caso de uso: funcional, una función diseñada de una aplicación.

Caso de abuso: acción deliberada que excede el caso de uso para producir resultados no intencionados.

Vector de ataque: punto y canal por donde los ataques se conducen [lector de tarjetas, campos de formularios, proxy de una red, etc.]

Superficie de ataque: área lógica expuesta a amenazas y patrones de ataque subyacentes.

Actor: individuo u organización legítima o adversaria de casos de uso o abuso.

Impacto: valor negativo sostenido por ataques exitosos.

Árbol de ataque: diagrama de relaciones entre activo-actor-caso de uso-caso de abuso-vulnerabilidad-explotación-contramedida.

PASTA se compone de una serie de actividades realizadas en cada uno de los 7 niveles de los procesos que se detallan a continuación:

Cómo es centralizado en el riesgo, el objetivo es mitigar lo que importa

Modelado de amenazas basado en evidencia

- Reúne inteligencia de amenazas para apoyar motivaciones de amenazas
- Impulsa los datos de amenazas para apoyar patrones previos de amenazas

Enfoque basado en el riesgo que se focaliza bastante en la probabilidad de ataques, posibilidad de ataques, riesgo inherente e impacto de compromiso

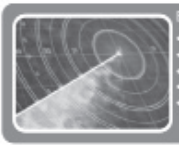
Si hay poco o ningún impacto, ¿para qué gastar tiempo/dinero en seguridad?"

Colaborativo

Modelo de priorización que debería definir cuándo y qué aplicaciones pasan al modelo de amenazas

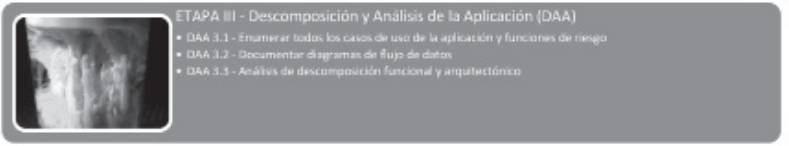
ETAPA I - Definición de Objetivos (DO)

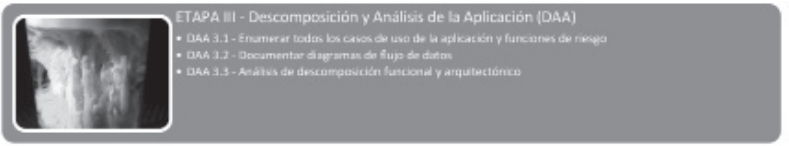
- DO 1.1 - Documentar los requerimientos del negocio
- DO 1.2 - Definir los requerimientos de seguridad/cumplimiento
- DO 1.3 - Definir el impacto del negocio
- DO 1.4 - Determinar el perfil del riesgo

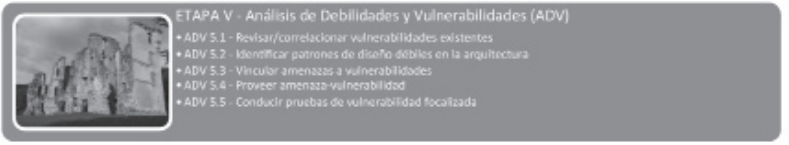


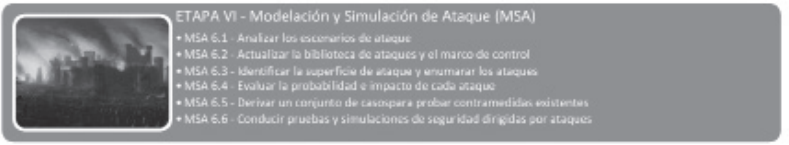
ETAPA II - Definición del Alcance Técnico (DAT)

- DAT 2.1 - Enumerar los componentes del software
- DAT 2.2 - Identificar actores y fuentes/repositorios de datos
- DAT 2.3 - Enumerar servicios a nivel de sistema
- DAT 2.4 - Enumerar infraestructura de terceros
- DAT 2.5 - Asegurar completitud del diseño técnico seguro









Estas enseñanzas no solamente afianzan lo que estoy aprendiendo, sino que además me preparan para responder a una amenaza. Debo internalizarlas, hacerlas propias, sentirlas, vivirlas y repetirlas, para responder naturalmente si un evento negativo se ocurriera.

De la misma manera que una aplicación informática tiene que seguir un proceso y una secuencia segura determinada para poder ser

seguro, pero en el caso de aplicaciones cerradas (enlatadas) como sistemas operativos, sistemas de gestión de base de datos, servidores web, aplicaciones web, sistemas de comunicaciones, sistemas criptográficos, etc., se utilizarán técnicas de caja cerrada.

Cada etapa que se pasa en este proceso de desarrollo seguro, donde se hacen pruebas, donde si los resultados son positivos se pasa a la siguiente etapa, es decir que paso a un nuevo cinturón, me gradúo, me puedo defender mejor, pero el camino sigue y la cuesta es cada vez más difícil.

Este el momento del proceso de crecimiento más largo, más arduo, que requiere más práctica, más tiempo, más correcciones, más repeticiones, más retroalimentaciones, más opiniones, más derrotas, más desafíos, más dolor. Pero el progreso es una recompensa.

Ver la flecha antes de que salga del arco

Se dice que un samurái ve la pelea antes que se desenvaine la katana. El nivel de conciencia y comprensión de las técnicas de defensa y ataque es tal que la intuición, la tendencia de que todo estímulo tiene una respuesta, y las acciones que se desencadenan a partir del conflicto llevan a un solo resultado: la victoria. Ya sea bloquear, esquivar, derivar o absorber; siempre la vista está puesta en el objetivo: desactivar el origen del ataque.

La inteligencia de amenazas es el estudio, análisis, conclusión y prognosis sobre las vulnerabilidades que pueden ser explotadas por diversos actores, que de acuerdo a sus finalidades, pueden afectar la integridad, disponibilidad y confidencialidad de la información, alterando el normal funcionamiento de equipamiento, programas, sistemas o procesos interconectados.

Y de la misma manera en que se realiza la inteligencia tecnológica al tomar posesión de un armamento o dispositivo del adversario para ver sus fortalezas y vulnerabilidades que minimicen las primeras y potencien las segundas generando contramedidas que mitiguen los riesgos, obtener la tecnología detrás de un ciberata-

que, también denominado operación cibernética, puede vislumbrar el grado de avance y conocimiento de la contraparte.

Para finalizar, es necesario establecer una estrategia de ciberdefensa, que debe ser definida por las máximas autoridades gubernamentales, con base en experiencias de otras naciones, buscar el apoyo regional, compartir información entre organismos, alinearse con el marco normativo vigente y se debe escuchar a los expertos.

Pero para tener una estrategia, debemos primero delinear una misión, que debe ser maximizar las capacidades de defensa de la infraestructura crítica del sistema de Defensa Nacional donde los procesos y objetivos generales y particulares sean apoyados por sistemas informáticos y de comunicaciones.

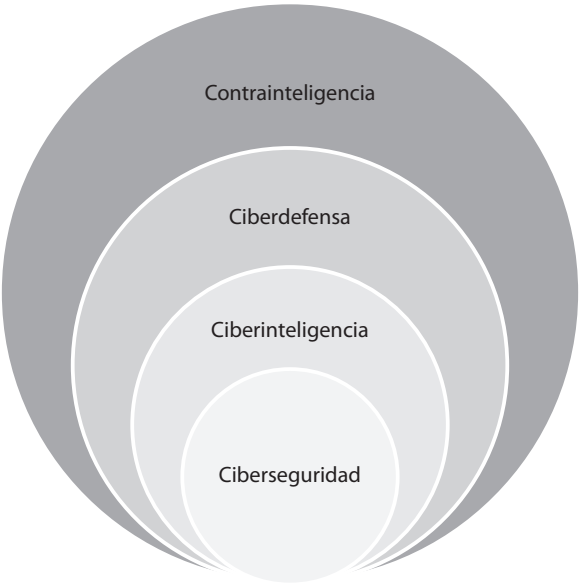
Sin embargo, el verdadero punto de partida es la visión. Y con ello cerramos el ciclo que iniciamos en el comienzo de estas palabras. ¿Cerramos? No, retroalimentamos.

Todo cinturón negro ve que a medida que va avanzado y alcanza nuevos danes, estos se imprimen en el mismo cinturón, que sufre desgaste, y que con el paso del tiempo, parece volverse blanco, pero eso no significa que no se ha aprendido, sino que, en realidad, es momento de mirar hacia atrás, ver el camino recorrido y sentir regocijo.

Es entonces que la visión es en realidad ese anhelo que debemos proponernos cuando vamos a encaminarnos por un trecho que desconocemos, pero aunque no veamos el horizonte, sí sabemos que debemos llegar a destino.

Nuestra visión sobre la ciberdefensa será una idea que atienda la necesidad que nuestros recursos incrementan sus funcionalidades cuando las TICs son incluidas y comprender que en un mundo interconectado, todos los actores son parte de la solución y parte del conflicto.

Es así que cuando hablamos de la visión que debemos tener sobre la ciberdefensa, creemos que significa proveer el mejor servicio con contrainteligencia digital.



Además de esta situación, es necesario conocer las amenazas para poder desarrollar las contramedidas necesarias, y por ende, tener capacidades propias. Por ello, es crítico que en el campo de la investigación y producción para la Defensa se trabaje en forma conjunta, para coordinar proyectos tendientes a la detección de vulnerabilidades de los sistemas propios y de aquellos adquiridos de terceros.

Bibliografía

Caralli, R. et al, (2007) Introducing OCTAVE *Allegro: improving the information security risk assessment process.* Recuperado de. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf (consultado el 12 de septiembre de 2018).

Dantu, R. et al. (2008). *Network risk management using attacker profiling. Wiley InterScience*. Recuperado de http://cangussu.com/site/publications/PAPERS/SCN09.pdf

Simeonova, S. (2016) *Threat modeling in the enterprise (parts 1-3).* Recuperado de https://securityintelligence.com/?s=threat+modeling (consultado el 12 de septiembre de 2018).

Uceda Vélez, T; Morana, M. (2015). *Risk centric threat modeling. Process for attack simulation and threat analysis,* Wiley, Nueva Jersey, Estados Unidos

Yourdon, E. (1993). *Análisis Estructurado Moderno*. Prentice-Hall Hispanoamericana, México.