CIBERSEGURIDAD Y CIBERDEFENSA, UN NUEVO CAMPO DE BATALLA QUE EMERGE AL MUNDO

Segura Rivera Edwin Julián.
edwin801@hotmail.com
Universidad Piloto de Colombia
2015

Resumen - Este artículo muestra dos temas muy importantes que hoy en día son tratados por distintas naciones, uno de ellos es la ciberseguridad y otro la ciberdefensa. La idea este documento es dar a conocer estos dos temas, dar el concepto de cada uno de ellos, indicar distintas vulnerabilidades latentes en la red y por las cuales se puede generar un ataque cibernético, exponer los programas y políticas que los países diseñan para evitar ataques cibernéticos como también ataques que han recibido, y en la actualidad qué está desarrollando Colombia para ser lo menos vulnerable posible en materia de seguridad en la red.

Índice de Términos-Ciberseguridad, ciberdefensa, ciberguerra, ciberespacio, mecanismos de defensa,

Abstract—this article demonstrates two very important issues today are treated by different nations; one of them is another cybersecurity and cyber defense. The idea this document is to present these two issues, to the concept of each indicate different latent vulnerabilities in the network and which can generate a cyber attack, exposing the programs and policies designed to prevent countries cyber attacks as well as attacks they have received, and currently being developed by Colombia to be the least vulnerable possible security on the network.

Index Terms-cybersecurity, cyber defense, cyber warfare, cyberspace, defense mechanisms,

I. INTRODUCCIÓN

Normalmente conocemos distintos campos de batalla como lo son por aire, mar y tierra. Sin embargo en la actualidad y debido a los acontecimientos actuales, hemos evidenciado ataques cibernéticos que nos llevan a una especulación acerca de si el mundo se encuentra en un nuevo campo de batalla que muchas personas del común no conocen, y las principales dudas que esto genera es, qué puede repercutir este tipo de batalla, a quienes puede afectar, como nos podemos defender ante estos ataques y como se encuentra nuestro país en materia de seguridad y defensa.

Últimamente se ha observado como el mundo de la tecnología de la información avanza, transformado procesos e introduciendo importantes cambios en la infraestructura que utilizamos. Es por esta razón que el mundo es cada vez más dependientes de la tecnología, donde el punto focal es el internet, lo cual genera que un país sea cada vez propenso y vulnerable a recibir ciberataques que pueden comprometer la infraestructura crítica, comprometer seriamente a la población civil sin necesidad de utilizar armamento y no siendo menos importante, también se compromete su parte militar.

El idea de este artículo, es demostrar cómo la ciberseguridad y la ciberdefensa permiten demonstrar que en el ciberespacio existen amenazas que atentan contra la seguridad de un país o una organización como tal. También la idea de este artículo busca brindar una definición de cada uno de estos términos explicado de la manera más simple para que el lector de este trabajo conozca este nuevo mundo de ciberataque. Por lo anterior, éste artículo brindará en primera parte terminología sobre lo que es ciberseguridad, ciberdefensa, distintos métodos que se utilizan en la red ya sea para realizar ataques o defendernos de los mismos.

Por otra parte, el artículo data sobre los distintos ataques cibernéticos que se han ejecutado en diferentes países, cómo operaron estos ataques y qué medidas tomaron estos países para prevenir y estar preparado ante otros posibles ataques que comprometan su ciberespacio.
Otro tema que tratará el artículo es sobre cómo esta Colombia a nivel de ciberataques, que medidas hay para prevenir este tipo de ataques.

II. DEFINICIONES

Para abordar y entender el tema, es necesario entender los conceptos tratados en el documento, para ello se van a dar unas definiciones pero sin ir a fondo puesto que no es el enfoque central del documento.

Ciberseguridad: Es el conjunto de acciones, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías de carácter preventivo que pueden utilizarse para proteger a los usuarios en un entorno, proteger activos de una organización y negarlos a terceros. [1]

Ciberdefensa: Conjunto de acciones de defensa, tanto preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al terceros.

Ciberespacio: es la dimensión generada por una persona durante el tiempo de interconexión y operatividad a través de internet, como por ejemplo visualizar emails, realizar video conferencias entre varias personas, comunicarse a través de redes sociales, etc. [2]

Ciberguerra: Básicamente es la guerra que se desata a través del ciberespacio.

III. PUNTOS DE VULNERABILIDAD DE INTERNET

Esta parte del documento es importante puesto que se describirán algunas de las vulnerabilidades por las cuales se pueden generar diversos ciberataques.

La SANS Institute (System Administration, Networking, and Security Institute) y el FBI, han venido publicando una extensa lista con las vulnerabilidades más explotadas en la mayoría de los ataques de las cuales solo se describen algunas de ellas a continuación:

Instalaciones por defecto de sistemas y aplicaciones, la filosofía de los fabricantes es que resulta mejor habilitar funciones que no son utilizadas que hacer que el usuario instale funciones adicionales a medida que las vaya requiriendo. Esta aproximación, aunque conveniente para el usuario, genera la mayoría de las vulnerabilidades de seguridad debido a que los usuarios no mantienen activamente o aplican los parches a los componentes de software que utilizan. Más aún, muchos usuarios no son conscientes de lo que está realmente instalado en sus propios sistemas, dejando peligrosos programas de demostración en ellos por el simple hecho de que no saben que están ahí. Aquellos servicios a los que no se les han aplicado los parches proveen rutas para que los atacantes puedan tomar el control de las máquinas.

Cuentas sin contraseña o contraseñas débiles, la mayoría de los sistemas se encuentran configurados para usar contraseñas secretas como primera y única línea de defensa. Los nombres de usuario (user IDs) son relativamente fáciles de conseguir y la mayoría de las compañías tienen accesos telefónicos que se saltan los cortafuegos. Es por esto que si un atacante puede determinar el nombre de una cuenta y su contraseña correspondiente, él o ella pueden entrar en la red.

Gran número de puertos abiertos, tanto los usuarios legítimos como los atacantes se conectan a los sistemas por medio de puertos. Cuantos más puertos se encuentren abiertos más formas hay para que alguien se conecte. Por lo tanto, es importante mantener abiertos sólo los puertos imprescindibles para que el sistema funcione correctamente. El resto de los puertos deben ser cerrados.

*Respaldos (backu*ps) incompletos o inexistentes, Cuando ocurre un incidente (y va a ocurrir en casi todas las organizaciones), la recuperación requiere respaldos actualizados y métodos probados para

restaurar la información. Algunas organizaciones hacen respaldos diarios, pero nunca verifican que éstos se encuentren realmente funcionando. Otros definen políticas de respaldo, pero no políticas o procedimientos de restauración. Tales errores son usualmente descubiertos después de que un atacante ha entrado en los sistemas y ha destruido o arruinado la información.

IV. MEDIDAS DE SEGURIDAD PARA PREVENIR ATAQUES

Utilice contraseñas más fuertes. Escoja aquellas que sean difíciles o imposible de suponer.

Póngale contraseñas diferentes a cada una de las cuentas. Realice respaldos regulares de datos críticos. Estos respaldos deben hacerse por lo menos una vez al día en el caso de usuarios o empresas pequeñas. Para organizaciones más grandes y complejas, deben realizarse respaldos completos por lo menos una vez a la semana, y respaldos incrementales todos los días.

Utilice un antivirus monitoreando toda actividad de archivos, actualizándolo periódicamente (sugerido una vez a la semana, lo ideal es diariamente).

Utilice cortafuegos como barrera entre su computadora e Internet. Los cortafuegos normalmente son productos de software. Ellos son esenciales para aquéllos que poseen enlaces de banda ancha con conexiones las 24 horas (DSL, cable módem, etc.), y muy recomendados para todos los que utilicen Internet, aún a través de la línea telefónica.

No deje que las computadoras sigan en línea cuando no están en uso. Físicamente desconéctelas de la conexión de Internet si fuera necesario.

No abra bajo ningún concepto, adjuntos en el correo electrónico que venga de extraños, sin importar lo que mencione su asunto o el archivo adjunto. Sospeche siempre de cualquier adjunto de alguien conocido, que le envía un adjunto que usted no solicitó. Esa persona podría estar infectada, y enviar el correo infectado sin siquiera percatarse del error. Sospeche de cualquier adjunto no esperado, de alguien que usted conoce porque se puede haber enviado sin el conocimiento de esa persona desde una máquina infectada.

Baje e instale regularmente los parches necesarios a medida que estos vayan apareciendo.

En concreto, estas pocas vulnerabilidades son la base de la mayoría de los ataques exitosos, que suelen aprovecharse de las brechas más conocidas con las herramientas de ataque más efectivas y fáciles de conseguir. La mayoría de los atacantes, simplemente se aprovecha de quienes no actualizan su software, casi siempre por pereza.

Según el FBI y SANS, la oportuna instalación de parches largamente anunciados, hubiera prevenido la mayoría de los ataques exitosos.

Para que esta omisión no sea por ignorancia, la presente lista debería servir de claro punto de referencia. [3]

Estas fueron solo algunas medidas de seguridad que pueden prevenir ciberataques hacia una organización, existen muchas medidas que se pueden tomar en cuenta para prevenir desastres, no en un 100% de prevención, pero por lo menos se podrían detectar a tiempo y poder aplicar las correcciones necesarias para no entrar en riesgo.

V. ATAQUES Y VIRUS QUE SE PUEDEN PRESENTAR EN UN CIBERATAQUE

DDoS: es uno de los ataques más letales que existe, consiste en denegar los servidores web de una institución u otros servicios hasta el punto de que esta misma colapse.

Botnets: son redes de diversas computadoras utilizadas para dirigir ataques de denegación de servicios, cuando una persona del común abre un correo basura, este correo se encuentra infectado de virus haciendo que la maquina se infecte y quede en manos de terceros. Dicho ataque es uno de los más utilizados para espiar instituciones gubernamentales.

Zeus: es un virus más conocido como troyano que se encarga de ingresar a las computadoras de los usuarios con el fin de obtener contraseñas de diferentes paginas ya sean de redes sociales, bancarias, entre otras, esto con el fin de realizar acciones de suplantación y robos de productos bancarios.

VI. ATAQUES DIRIGIDOS A DISTINTOS ESTADOS Y SUS TOMAS DE ACCIÓN PARA MITIGARLOS

ALEMANIA: recibió miles de intentos de espionaje comercial por parte de hackers chinos, que en algunos casos llegaron a bloquear páginas web gubernamentales por varias horas. Adicionalmente recibe constantes ataques por parte de hackers rusos a su red eléctrica y ferroviaria.
Las acciones tomadas por este país surgieron en el 2009, cuando estableció su primera unidad exclusivamente dedicada a la guerra cibernética, esta unidad está conformada por 60 oficiales y suboficiales de todas las fuerzas y está comandada por un General del Ejército Alemán.

AUSTRALIA: en múltiples ocasiones, hackers norcoreanos y chinos han ingresado y bloqueado páginas web del gobierno. En noviembre de 2008, el sitio del primer ministro fue desconectado completamente por dos días.
Ellos crearon el centro de operaciones cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio. Por otro lado, en el libro blanco de defensa de 2009, se definió a la ciberseguridad como una de las capacidades esenciales y principales a fortalecer en los próximos 20 años.

CHINA: se ha embarcado en una serie de asaltos informáticos a naciones occidentales como Corea del Sur, Alemania, Australia, Reino Unido y especialmente Estados Unidos.
Tiene una capacidad bien conformada y hombres entrenados dentro del comando cibernético conjunto (militar y civil). Ha desarrollado una red operativa muy segura para sus sistemas gubernamentales y militares, haciendo sus redes impenetrables y con un poderío ofensivo que está en posición de demorar o interrumpir el despliegue de tropas de otros países.

COREA DEL NORTE: a pesar de haber sido acusada de numerosos asaltos informáticos, Corea del Norte no ha aceptado oficialmente que dichos asaltos provengan de organismos oficiales.
La toma de acción de este país es que tiene operando desde hace aproximadamente 8 años una unidad de guerra cibernética, especializada en hackear las redes militares surcoreanas y norteamericanas para extraer información y examinar sus vulnerabilidades.

COREA DEL SUR: sus redes informáticas civiles y militares están bajo continuo ataque; se reporta que mensualmente sufren alrededor de 10.500 intentos de ingresos piratas y de 81. 700 contagios con virus informáticos. En 2004, hackers chinos y norcoreanos robaron información ultra secreta de sistemas de diferentes agencias gubernamentales.
Dicho país planea la creación de un comando conjunto unificado de guerra cibernética para 2012 con el fin de enfrentar la amenaza creciente de ataques a sus redes informáticas gubernamentales y militares. Las entidades civiles también han desarrollado un fuerte mecanismo privado de defensa a los ataques, dada la poca eficiencia de las acciones adelantadas en este sentido por parte del estado.

ESTADOS UNIDOS: en enero de 2009, hackers robaron información ultra secreta del Joint Strike Fighter ó F – 35 (el proyecto de un sistema de armas más costoso en la historia de Estados Unidos). Adicionalmente el 4 de julio de 2009, deshabilitaron las páginas web del departamento del tesoro y de estado, de la comisión federal de comercio, del pentágono y de la casa blanca.
La acción tomada por este país, creó un centro de cibercomando unificado que depende de la agencia de seguridad nacional (NSA, por sus siglas en inglés). Este centro optimiza los esfuerzos hechos por parte de las fuerzas militares y otras agencias, y provee al país con la capacidad de defender la infraestructura tecnológica y de conducir operaciones ofensivas.

ESTONIA: el caso de éste país lo vamos a ilustrar más puntualmente puesto que a la fecha ha sido uno de los ataques cibernéticos más fuertes que ha ocurrido en la historia, Dicho ataque ocurrió en el año 2007.

En Abril 15, el Gobierno de Estonia, decide remover del centro de Tallin, el Monumento del soldado de Bronce, lo cual genera un fuerte enfrentamiento diplomático con Rusia. En Abril 26 el ataque cibernético empezó a las 10 p. m; al final de esa primera semana, todas las páginas web gubernamentales y de los diferentes partidos políticos habían sido bloqueadas. En Mayo 2 la segunda semana, todos los medios de comunicación quedaron completamente desconectados, haciendo imposible que se le informara al mundo lo que estaba ocurriendo. En Mayo 09, a medianoche, ocurrió el ataque más fuerte, los hackers desconectaron todo el sistema bancario, bloquearon sus páginas web y los cajeros electrónicos dejaron de funcionar. En mayo 15, durante tres semanas, los sitios web del gobierno, los bancos, medios de comunicación y todas las universidades fueron sistemáticamente atacados y desconectados. En Mayo 19, los ataques se detuvieron y la primera ciberguerra llegó a su fin. Estonia inmediatamente acusó al gobierno de Rusia, pero nada ha podido ser demostrado a la fecha.

La acción tomada por éste país fue en 2008 cuando creó conjuntamente con varios países de Europa, la OTAN y EE.UU el centro internacional de análisis de ciberamenazas. En este centro trabajan 30 personas, entre personal técnico y administrativo. Su presupuesto proviene de los países participantes de manera compartida.

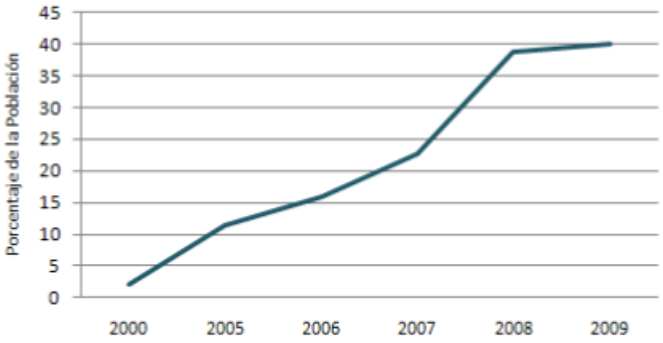
FRANCIA: En enero de 2009, aviones de combate franceses no pudieron despegar de su portaviones al ser desactivado, por medio de un virus informático, lo cual ocasionó una intermitencia en su sistema electrónico.

Creó la agencia de seguridad para las redes e información (FINSA), que vigila las redes informáticas gubernamentales y privadas con el fin de defenderlas de ataques cibernéticos. Esta agencia depende directamente del ministro de seguridad nacional. También lidera la unidad de ciberseguridad y ciberdefensa en la OTAN. [4]

VII. ESTADO DE COLOMBIA EN CIBERSEGURIDAD Y CIBERDEFENSA

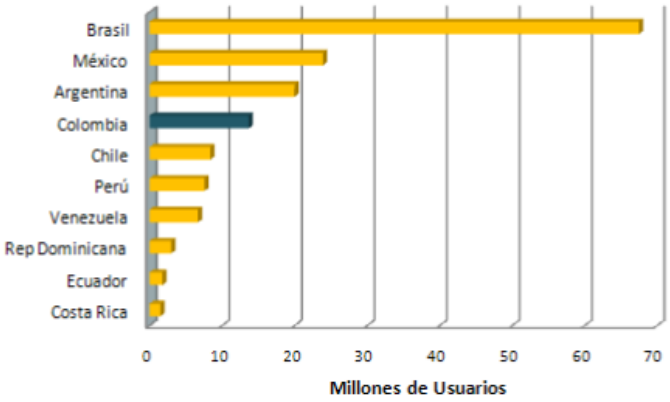
De acuerdo a los estudios realizados por el ministerio de defensa nacional de Colombia, a través de la dirección de estudios sectoriales (2009), para el año 2000 tan solo el 2% de la población tenía acceso a Internet; actualmente el 40% hace uso constante de este medio (ver figura No. 1), ubicando al país en el cuarto lugar en el ranking de usuarios de América Latina (ver figura No. 2) y en el puesto 24 del mundo.

Imagen No. 1
Crecimiento del uso de internet en Colombia, periodo 2000 al 2009



Fuente: Ministerio de Defensa Nacional de Colombia

Imagen No. 2
Países según su uso de internet (2009)



Fuente: Ministerio de Defensa Nacional de Colombia

De acuerdo a este estudio realizado, desde el año 1999 se han reportado numerosos ataques a dominios colombianos; para el año 2002 el sitio http://attrition.org/ reportó 50 ataques a diferentes sitios oficiales. En el 2009, la cantidad de ataques aumentó exponencialmente; el sitio www.zone-h.org reportó una veintena tan solo en el mes de agosto.

También ocurren ataques más sofisticados como el que ocurrió en el primer semestre de 2009, cuando el sistema financiero vio comprometidos alrededor de 50 millones de dólares que desaparecieron de las cuentas bancarias de personas naturales y jurídicas.

En términos generales, de enero a julio de 2009 la Policía Nacional ha atendido 836 casos relacionados con amenazas cibernéticas, que van desde el robo de identidad, hasta los hurtos electrónicos, accesos abusivos a sistemas informáticos y pérdida de información sensible en las organizaciones.

En los últimos años, se han detectado múltiples intentos de ataque a la infraestructura crítica del país. Estos intentos han sido neutralizados exitosamente hasta el día de hoy, sin embargo, su nivel de sofisticación cada vez es mayor y, por lo tanto, se requiere un equipamiento de última tecnología y una excelente preparación del personal a cargo de la seguridad nacional de Colombia. [5]

Desde el año 2005 se creó un grupo de inteligencia liderado por el Ministerio de Relaciones Exteriores, en conjunto don el ministerio del interior y de justicia, el ministerio de defensa nacional y posteriormente el ministerios de las tecnologías de la Información y las telecomunicaciones (TIC's) y entidades relacionadas con este tema, decidieron que quien 26 levaría las riendas de la ciberseguridad y la ciberdefensa de Colombia seria el ministerio de defensa nacional.

De este trabajo asociado entre las instituciones anteriormente relacionadas se gesta en 2009 el ColCERT (equipo de respuesta a emergencias informáticas de Colombia), "cuya función principal es la de coordinar las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano, frente a emergencias cibernéticas que atenten o comprometan la seguridad y defensa nacional". De acuerdo con este informe el trabajo va en caminado en tres ejes temáticos principales:

En primera instancia se enfoca en el fortalecimiento jurídico e institucional, el cual se refiere a la adaptación del sistema de legislativo y judicial para los temas de ciberseguridad. En segundo término plantea los asuntos internacionales como plano de vital importancia para los intereses colombianos, esto se traduce en una misión de observación de los casos internacionales y que tendencias se marcan en el ámbito de la ciberseguridad y ciberdefensa en cuanto a medidas a preventivas que lleven a una minimización del riesgo de sufrir ataques cibernéticos, así como implementación de acuerdos sobre la materia que pueda asumir el estado ya sea bilateral o multilateralmente. En tercer lugar se encuentran las medidas contra el delito cibernético. Con ello se refieren a las capacidades que puede adquirir en cuanto a sistemas de defensa que mediante el ColCERT se ponen en marcha para mitigar potenciales ataques. En cuanto al ColCERT, se enfatiza que es importante trabajar de mano de las entidades privadas para obtener financiación y de ese modo se pueda evolucionar en el fortalecimiento de esta entidad y que no quede como un proyecto inconcluso.

En la actualidad esta entidad a través de su página en Internet www.colcert.gov.co, brinda información acerca de foros mundiales sobre seguridad informática, así como asesorías y actualizaciones de seguridad para sistemas operativos y de ese modo reducir la vulnerabilidad de los ordenadores (ver imagen No. 3). [6]

Imagen No. 3
Países según su uso de internet (2009)

Fuente: Portal Web ColCERT, www.colcert.gov.co. [7]

VIII. NOTICIA IMPORTANTE DEL DIARIO PORTAFOLIO EN COLOMBIA

El Gobierno Nacional, ha sido consciente del aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, aprobó, mediante el documento Conpes, unos lineamientos para llevar adelante la política de ciberseguridad, basados en tres acciones principales: I) adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar, generar recomendaciones para afrontar las amenazas y los riesgos que se presenten; II) brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberdefensa y ciberseguridad, y III) fortalecer la legislación en estas materias, la cooperación internacional y adelantar la adhesión de Colombia a los diferentes instrumentos internacionales.

En la parte institucional se diseñaron las siguientes entidades: Comisión Intersectorial, presidida por el Presidente de la República, Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), Comando Conjunto Cibernético de las Fuerzas Militares (Ccoc) y el Centro Cibernético Policial (CCP).

Es importante aclarar que el Conpes no creó estas entidades porque no tiene facultades para ello, simplemente recomendó su constitución al Ministerio de Defensa en el presente año.

Queda pendiente ver si el Ministerio tiene facultades ordinarias para hacerlo o si su creación podría caber dentro de las precisas facultades extraordinarias que tiene el gobierno Nacional para modificar la estructura de la administración nacional.

La capacitación especializada en seguridad de la información será gradual. Inicialmente se capacitará a los funcionarios que estén directamente involucrados en la atención y manejo de incidentes cibernéticos y luego se extenderá a otras instituciones del Gobierno y al sector privado, para lo cual se requerirá la colaboración de los ministerios de educación y de las tecnologías de la información.

El objetivo para fortalecer la legislación en materia de ciberseguridad y ciberdefensa busca desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos cibernéticos, no sólo a nivel nacional, sino internacional.

La meta es que Colombia se posicione como líder regional en el área de seguridad cibernética a través del intercambio de buenas prácticas, conocimiento y experiencias, prestando especial atención a la promoción de la experiencia nacional en el proceso de desarrollo de esta política.

Queda una ardua tarea que desarrollar que requerirá, para llevarla adelante, un gran apoyo del sector privado y de las universidades. [8]

IX. CONCLUSIONES

Las nuevas tecnologías de información y telecomunicaciones han avanzando a un ritmo cada vez más rápido al pasar de los días, para los hackers y crackers permitiendo que ellos también avancen al ritmo de nuevas tecnologías, por ello, es importante estar a la vanguardia de los mecanismos de defensa, no solo la información sensible de los pobladores de un estado o una organización, o el ataque a una página oficial, sino también tener sistemas de defensa que permitan proteger las infraestructuras críticas que con el paso del tiempo son más dependientes del ciberespacio; también es importante que cada especialista de seguridad informática continúe en aprendizaje tanto de las nuevas tecnologías que se pueden usar como de los nuevos intentos de ataques que se pueden generar hoy en día.

El campo de la investigación acerca del ciberespacio para diseñar políticas en ciberseguridad y ciberdefensa ha sido importante con el pasar del tiempo, pues ha sido evidente que existe un nuevo campo de batalla en el ciberespacio, razón por la cual, es importante fomentar la investigación de este tema entre los estudiantes de

diversas ramas de la ciencia, solo en la ingeniería, en la cual deben trabajar conjuntamente para lograr estar a la vanguardia y conocer que este tema a futuro va con más fuerza y concientizarlos en que la seguridad debe ser un tema conocido y manejado por todos.

Los años de análisis sobre este tipo de cambios en la seguridad que empezaron años atrás y que en los últimos años hemos venido anticipando, nos han permitido profundizar sobre los riesgos inminentes que se filtraban sobre nuestro día a día de los cuales no éramos conscientes de la necesidad de entender y prevenir los riesgos y adicionalmente convertirlos en oportunidades para generar en nuestro entorno un cambio que se pudiera poner a disposición de las organizaciones y de las personas que posibilitaran la percepción de la seguridad como un elemento importante de nuestro día a día.

Para todo caso se requiere revisar el análisis de riesgo de los nuevos escenarios críticos a los que nos enfrentamos día a día, y es importante tomar rápidamente decisiones correctivas que mitiguen el impacto de los riesgos y nos permitan salir lo antes posible de un escenario de crisis, esto es fundamental, pues nos estamos acostumbrando a convivir con un nivel de riesgo, es claro que la seguridad total no existe y el grado de complejidad de las tecnologías de la información y las comunicaciones ha aumentado y cada vez es más difícil de administrar y por lo tanto es difícil controlar el riesgo.

REFERENCIAS

[1] Definiciones relativas a la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación. Available: http://www.itu.int/net/itunews/issues/2010/09/20-es.aspx

[2] Ciberdefensa-Ciberseguridad Riesgos y Amenazas. Available: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

[3] Vulnerabilidades más críticas por internet. Available: http://www.vsantivirus.com/20vul.htm

[4] Contexto internacional, países atacados. Available: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

[5] Crecimiento del uso de internet en Colombia, periodo 2000 al 2009. Available: http://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

[6] lineamientos de política para ciberseguridad y ciberdefensa, conpes. Available: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[7] Grupo de respuestas a emergencias cibernéticas de Colombia. Available: http://www.colcert.gov.co/

[8] Política de ciberseguridad y ciberdefensa. Available: http://www.portafolio.co/columnistas/politica-ciberseguridad-y-ciberdefensa

Autor

Edwin Julián Segura Rivera
Ingeniero de Sistemas
Universidad Piloto de Colombia
2015