Controles de Seguridad propuesta inicial de un Framework en el Contexto de la Ciberdefensa.

Pablo Gastón Sack , Jorge S Ierache.

Facultad de Informática Ciencias de la Comuicación y Técnicas Especiales
Universidad de Morón Cabildo 134 Morón Argentina
jierache@unimoron.edu.ar

Abstract.: El presente trabajo explora un conjunto de definiciones de ciberespacio, ciberguerra, ciberdefensa, y de características de controles de seguridad a fin de realizar una propuesta inicial de un Framework que facilite la gestión y diagnóstico de seguridad en el contexto de la ciberdefensa.

Keywords: Ciberespacio, Ciberguerra, Ciberdefensa, Seguridad Informática, Controles de Seguridad.

1 Introducción

La constante evolución humana ha llevado a la generación de un nuevo espacio artificial que resulta transversal a los espacios naturales (terrestre, marítimo, aéreo, espacial) en los que la humanidad se desarrolla naturalmente. El nuevo ambiente o espacio denominado ciberespacio está plenamente integrado en las actividades humanas, no reconoce fronteras físicas ni estados naciones, permite la evolución de las operaciones en términos de interoperabilidad de los sistemas en los distintos ambientes naturales. En la Primera Guerra Mundial se introdujeron los aviones, una nueva forma de sorprender y atacar a las fuerzas en oposición, algo similar (salvando las distancias tecnológicas) ocurre en la actualidad con el ciberespacio. Desde este nuevo espacio artificial se presenta un campo de batalla , presente en la puerta de cada computadora infectada por un software malicioso (malware) puede ser un elemento de ataque a gran escala a un país/agencia o empresa sin que su dueño esté enterado. Internet no es un lugar seguro, ya que hay personas que buscan delinquir en la red ya sea por diversión, por dinero, por motivos políticos, etc. El ciberespacio se presenta como el nuevo ambiente artificial creado por el hombre, que actúa como integrador de los ambientes naturales donde actúa la humanidad. Desde el principio de la historia de la humanidad, los conflictos y las guerras, aumentaron sus alcances y efectos acompañados por los avances científicos tecnológicos. El hombre ha luchado entre sí por diferencias culturales, disputas territoriales, políticas, por recursos, sometimiento, hoy lucha por el dominio del ciberespacio. Se presenta en la Fig. 1 la integración de ambientes a través del ciberespacio, se detalla a continuación cada uno de ellos: a) Tierra (1) y Mar (2): Con el paso del tiempo el hombre ha ampliado y dominado nuevos campos de batalla, siendo sus primeros comienzos el campo terrestre y marítimo; b) Aire (3): Con la llegada de la Primera Guerra Mundial se comenzó con

el dominio aéreo teniendo una vital importancia para la Segunda Guerra Mundial cambiando drásticamente la forma de hacer una guerra; c) Espacio (4): Ya avanzada la década del 60 fue el auge de la carrera espacial dominando así un nuevo campo de batalla muy diferente a los anteriores los cuales están definidos en gran medida por la geografía o radio de operación; d) Ciberespacio (5): Con el advenimiento de Internet desde hace varias décadas, los países (principalmente los desarrollados) se han volcado de lleno a esta nueva era digital en la que todo está interconectado con todo.

Fig. 1. Integración de Dominios

1.1 Ciberespacio

La palabra ciberespacio surge de la conjunción de la palabra "cibernao" -proveniente del griego que significa "pilotear una nave" y es utilizado comúnmente en el ámbito de las redes -, y espacio dando así la idea de estar piloteando o navegando sobre un mundo virtual. Éste término fue utilizado por primera vez en la década de los '80 por el escritor William Gibson para describir una red de computadoras ficticia que contenía enormes cantidades de información que podría explotarse con el fin de adquirir riquezas y poder [1]. En la actualidad el ciberespacio se le da un significado más amplio al que se lo aglomera en la conjunción de toda la información disponible (digitalmente) junto con el intercambio de la información y las comunidades electrónicas que surgen en base al uso de esa información [2]. El ciberespacio no debe confundirse con el Internet real, el término se refiere a menudo a los objetos e identidades que existen dentro de la red informática. Esto quiere decir que una página Web (por ejemplo), se encuentra en el ciberespacio. Según esta interpretación, los acontecimientos que tiene lugar en Internet no están ocurriendo en los países donde los participantes o los servidores se encuentran físicamente, sino en el ciberespacio [3]. Otro punto de vista que vale la pena mencionar es una definición de ciberespacio que abarca todo el espectro electromagnético y propagación de energía. En otras palabras, todo lo que fluya a través del espectro electromagnético (como celulares, Internet, etc); Si emite, transmite, usa el ciberespacio. En septiembre de 2006, Jefes de Estado Mayor de los Estados Unidos lo definieron como "dominio caracterizado por el uso de electrónica y espectro electromagnético para el almacenamiento, modificación e intercambio de información vía sistemas en red e infraestructuras físicas asociadas" [4]. El ciberespacio sobrepasa los límites de cómo

y cuándo interactuar. Entre las características del ciberespacio están las siguientes [5]: a) Identidad, flexibilidad y anonimato: La falta de interacción física cara a cara causa un impacto en cómo la gente presenta su identidad o quizás quedarse en el anonimato, incluso se puede tener una identidad imaginaria o falsa; b) En el ciberespacio todos tenemos la misma oportunidad de comunicación; c) Trasciende los límites espaciales: Las distancias geográficas no limitan quién pueda comunicarse con quién; d) Tiempo extendido y condensado: puede haber una comunicación cualquiera vía Internet, pueden haber varias personas sentadas en su computadora al mismo tiempo. Este tipo de comunicación crea un espacio temporal donde el estar, como tiempo interactivo se extiende. Es decir, se tiene tiempo para pensar cosas y dar una respuesta. El Ciberespacio en el contexto del campo de batalla ha ido creciendo y convirtiéndose en algo más difícil de definir y defender, su ámbito de actuación propio de Internet proveyó un mecanismo de acción que incrementa la velocidad, difusión y poder en un ataque [6], a diferencia de nuestro entendimiento histórico de la guerra, el ciberespacio como campo de batalla posee ventajas asimétricas a favor del atacante. En este orden resulta oportuno considerar que: a) La inteligencia y engaño serán los principios críticos de la guerra en el ciberespacio; b) El ciberespacio es vasto y es fácil de esconderse en el mismo; c) Los efectos de los ataques son desproporcionados a los costos de los mismos; d) El uso del ciberespacio no requiere un uso intensivo de materiales o capital; e) Se puede lanzar ataques desde cualquier parte del mundo, incluso el mismo país o red del atacado proporcionando un anonimato. Éste punto representa una dificultad extra ya que no es fácil ubicar al agresor e incluso pueden ser grupos independientes (no gubernamentales) o incluso mismos ciudadanos; f) El atacante puede tomarse todo el tiempo necesario para la adquisición de recursos u oportunidades para garantizar la conquista de su objetivo. Diferentes definiciones del Ciberespacio se pueden presentar. En este orden la **Real Academia Española** lo define como el: Ámbito artificial creado por medios informáticos. Esto quiere decir que para implementar el ciberespacio se necesita de una infraestructura física de computadoras y líneas de comunicaciones que las mantengan interconectadas. Para el **National Institute of Standards and Technology (NIST)** Ciberespacio se define como **el** dominio global dentro del entorno de la información que consta de redes interdependientes de infraestructuras de sistemas de información que incluyen: internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores. Para la **Unión Europea** se define como el: espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo. Para la **Unión Internacional de Telecomunicaciones** se define como: un lugar creado a través de la interconexión de sistemas de ordenador mediante Internet. **España** lo define como el: Conjunto de medios físicos y lógicos que conforman las infraestructuras de los sistemas de comunicaciones e informáticos. **Estados Unidos** (DoD) lo define como: un dominio global dentro del entorno de la información, consistente en la red interdependiente de las infraestructuras de tecnología de la información incluida la Internet, redes de telecomunicaciones, sistemas informáticos, los procesadores y controladores embebidos. **Estados Unidos** (National Military Strategy for Cyberspace Operations) lo define como: El dominio que se caracteriza por el uso de la electrónica y el espectro electromagnético para

almacenar, modificar e intercambiar datos a través de sistemas de redes e infraestructuras físicas asociadas. Para **Alemania** el ciberespacio se define como: espacio virtual de todos los sistemas informáticos vinculados a nivel de datos a escala global. La base para el ciberespacio es el Internet como una red de conexión y transporte universal y accesible al público que puede ser complementada y más expandido en cualquier número de redes de datos adicionales. Sistemas de informáticos en un espacio virtual aislado no son parte del ciberespacio.. Para el **Reino Unido**: Todas las formas de actividades en redes digitales; esto incluye el contenido y acciones realizadas a través de redes digitales. En una visión particular de **ciberespacio** por parte de los autores propone como definición del ciberespacio: al ámbito artificial transversal a los ambientes naturales (terrestre, marítimo, aéreo y espacial) que conforma el espacio virtual de interacción en el que se desarrollan actividades propias de humanos y máquinas relacionadas con la creación, procesamiento, publicación, almacenamiento, modificación y explotación de datos, información y conocimiento digitales, en un contexto distribuido (computación en nube) a través de redes interdependientes e interconectadas globales, públicas, privadas, híbridas, software y firmware de máquinas, cuyo carácter distintivo está dado por el empleo de las tecnologías de información y comunicaciones.La **ciberguerra** es definida por Richard Clarke como las acciones realizadas por un estado Nación que penetra computadoras o redes de otras naciones con el propósito de causar daño o ruptura de las mismas. Wisegeek la define como la forma de guerra que toma lugar en las computadoras e Internet a través de mecanismos electrónicos por sobre los físico. **China** define Ciberguerra como: las acciones adoptadas para lograr la superioridad de información al afectar la información adversario, sus procesos basados en la información, sistemas de información y redes informáticas, mientras que se realiza la defensa de la propia información, los procesos basados en la información, sistemas de información y redes informáticas.**Estados Unidos (DoD)** Cyber warfare (CyW) — Cualquier acto destinado a obligar a un oponente para cumplir nuestra voluntad nacional , ejecutado contra el software de control de procesos dentro del sistema de un oponente. CYW incluye los siguientes modos de ataque cibernético : la infiltración cibernética , la manipulación cibernética , asalto cibernético, y la incursión cibernética..La **Ciberdefensa** es definida por La OTAN como: El desarrollo de la capacidad de prevenir, detectar, defenderse y recuperarse de los ataques cibernéticos. Por lo tanto, la defensa se centra en el uso de métodos tecnológicos para identificar una intrusión no autorizada, localizar el origen del problema, evaluar los daños, evitar la propagación de los daños dentro de la red, y en la medida necesaria, la reconstrucción de los datos y de los equipos que se encontraban dañados. Defensa implica [7] la capacidad de colocarse en el camino de penetración, identificar tal intento, y frustrar a través de la interrupción y suspensión de la tareas. Para este propósito, los sistemas informáticos se utilizan para supervisar las actividades y las comunicaciones; bloquear vías de acceso; limitación de permisos; verificación de identidad; proporcionar cifrado y habilitar la copia de seguridad y recuperación de desastres. Para **Colombia Ciberdefensa se define como la:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional. Para **Estados Unidos**

(Comprehensive National Cybersecurity Initiative (CNCI)): La defensa de todo el espectro de amenazas mediante la mejora de las capacidades de contrainteligencia de EEUU y el incremento de la seguridad de las cadenas claves de suministro de información.

2 Controles de Seguridad

En el contexto de la Ciberdefensa para su estudio se propone armar una base sólida y progresiva de controles de seguridad tomando como esqueleto y estructura el documento "The Critical Security Controls for Effective Cyber Defense" [8]. Complementar la base de controles de seguridad con lo planteado en "Strategies to Mitigate Targeted Cyber Intrusions" [9] y en el documento de "Security and Privacy Controls for Federal Information Systems and Organizations (800-53 Rev.4)" [10]. Se toma como punto de partida y de referencia el documento "Framework for Improving Critical Infrastructure Cybersecurity" de National. [11]

2.1 The Critical Security Controls for Effective Cyber Defense

El documento de Critical Security Controls for Effective Cyber Defense [8], fue realizado por una comunidad de más de 100 agencias gubernamentales, compañías privadas y expertos. Estos controles actúan como una plataforma sólida para construir otros estándares, puede ser utilizado para crear un mapa de ruta o punto de partida para quienes no saben por dónde empezar. El objetivo principal de este documento es reducir los ataques iniciales incrementando los niveles de seguridad al configurar los dispositivos, la identificación de dispositivos comprometidos, la interrupción del control de los atacantes sobre el código malicioso implantado y encontrar la forma de que todo esté integrado en un circuito de retroalimentación (evolución continua). Los principios críticos en que se basa este documento son: a) La ofensiva informa a la defensa: Usar el conocimiento de ataques actuales para aprender de estos eventos y construir defensas más efectivas; b)Priorizar: Invertir en controles que proveerán un mayor grado de reducción de riesgo; c) Métricas: Establecer sistemas de medición comunes que puedan dar un lenguaje común para la gerencia, los auditores, el grupo de informática y el grupo de seguridad de la organización; d) Diagnóstico: llevará a cabo mediciones continuas para evaluar y validar la efectividad de las mediciones de seguridad actuales; e)Automatización: Automatizar defensas para que las organizaciones puedan obtener mediciones confiables, escalabres y continuas .Por otro lado, este documento está divido en veinte controles críticos de seguridad que contienen a su vez un grupo de subcontroles. Dichos subcontroles se categorizan con el fin de implementar controles de manera progresiva y escalonada de la siguiente forma: a) **Logros Rápidos**: Estos subcontroles ofrecen una gran reducción del riesgo sin grandes inversiones financieras, de arquitectura o técnicas (orientado a ataques comunes); b) **Medidas de Visibilidad y Atribución**: Estos subcontroles ofrecen mejorar el proceso, la arquitectura y las capacidades técnicas de las organizaciones para monitorear sus redes y sistemas informáticos con el objetivo de detectar intentos

de ataque, localizar puntos de entrada, identificar dispositivos ya comprometidos, interrumpir actividades de atacantes infiltrados y obtener información sobre las fuentes del ataque; c)**Mejora de la Configuración de Seguridad de la Información**: Estos subcontroles ofrecen reducir el número y magnitud de las vulnerabilidades de seguridad y mejorar las operaciones de los sistemas informáticos en red; d) Subcontroles Avanzados: Estos subcontroles son usados en nuevas tecnologías o procedimientos que provee máxima seguridad pero son difíciles de implementar, más caro o requiere de personal altamente capacitado.

2.2 Strategies to Mitigate Targeted Cyber Intrusions [9]

El documento Strategies to Mitigate Targeted Cyber Intrusions" [9] está dividido en tres documentos desarrollados por el Departamento de Defensa de Australia y se compone de la siguiente manera: a) Mitigation Strategies 2014: contiene una breve introducción y un poster con el resumen de las treinta y cinco estrategias para mitigar ciberataques; b)Mitigation Strategies 2014 Details: Describe cada una de las treinta y cinco estrategias para mitigar ciberataques. Se menciona un código de control recomendado; c)Information Security Manual 2014 Control: Describe los códigos de controles mencionados en el documento anterior. Si bien este documento plantea treinta y cinco estrategias para la mitigación de los ciberataques remarca que como paso primordial es la de desarrollar y aplicar las primeras cuatro estrategias a las que denominan como esenciales. Dichas estrategias consisten en la generación de listas blancas de aplicaciones, parches de aplicaciones, parches de vulnerabilidades de sistemas operativos y restricción de privilegios de administrador.

2.3 Security and Privacy Controls for Federal Information Systems and Organizations

El documento "Security and Privacy Controls for Federal Information Systems and Organizations (800-53 Rev.4)" [10], forma parte de un "ciclo de vida de la seguridad" propuesto por NIST formando un marco de trabajo de gestión de riesgos. El "ciclo de vida de la seguridad" propuesto está compuesto por seis etapas con su correspondiente documento: a) Categorizar Sistemas de Información: 800-60; b) Seleccionar Controles de Seguridad: 800-53 Rev.4, c) Implementar Controles de Seguridad: 800-160; d) Evaluar Controles de Seguridad: 800-53A; e) Autorizar Sistemas de Información: 800-37; f) Monitorear Estado de Seguridad: 800-137.

2.4 Framework for Improving Critical Infrastructure Cybersecurity

Este marco de trabajo denominado como "Framework for Improving Critical Infrastructure Cybersecurity" de National" [11], provee un lenguaje común para el entendimiento, gestión, expresando el riesgo en la ciberseguridad, tanto interna como externa. Este marco de trabajo está compuesto por tres partes: a) **Núcleo**: Está compuesto por un conjunto de actividades de ciberseguridad, resultados deseados y referencias aplicables que son comunes en todos los sectores de infraestructuras

críticas. Se compone de cinco funciones concurrentes y continuas: **Identificar, Proteger, Detectar, Responder y Recuperar**. Dichas funciones proveen una vista estratégica del ciclo de vida de la gestión de riesgos de ciberseguridad de una organización. A su vez, cada una de estas funciones principales se dividirán en Categorias, Subcategorias y Referencias informativas; b) **Niveles de Implementación:** Proporcionar un contexto sobre cómo una organización ve los riesgos de ciberseguridad y los procesos para gestionar ese riesgo. Se compone de cuatro niveles: **Parcial, Riesgo Informado, Repetible y Adaptativo.** Estos niveles reflejan una progresión de respuestas informales y reactivas a enfoques ágiles y riesgo informado. c) **Perfiles:** Representa los resultados en base a las necesidades del negocio que una organización ha seleccionado de las categorías y subcategorías del marco de trabajo. Pueden ser utilizados para identificar las oportunidades para mejora la postura de ciberseguridad mediante la comparación de un perfil "actual" con un perfil "objetivo. Para el desarrollo de un perfil, una organización puede revisar todas las categorías y subcategorías y, basándose en los objetivos del negocio y una evaluación del riesgo, determinar cuáles son los más importantes.

3 Modelo de Framework propuesto

Sobre la base de controles y el marco de trabajo presentados en la sección anterior, se presenta a continuación la propuesta de un Modelo de Framework que facilite la implementación de controles de manera progresiva y realice un seguimiento de avance a través de las métricas en cada uno de los controles, ofreciendo documentos de consulta por cada control involucrado y links sugeridos. Para esto utilizaremos la **división de los controles de seguridad** propuestos en Framework for Improving Critical Infrastructure Cybersecurity [11]. Dicho documento plantea una división de los controles de seguridad propuestos en cinco fases. Estas fases aglutinarán controles de seguridad que cumplan con el objetivo de cada fase (ver Fig. 2).

Fig. 2. Fases del "Framework for Improving Critical Infrastructure Cybersecurity

3.1 Iteraciones dentro del marco de trabajo

Adicionalmente a la **división de los controles de seguridad** en cada una de las fases, el marco de trabajo constará de **cuatro iteraciones** que cruzarán todas las fases del mismo (ver Fig. 3). Estas iteraciones tendrán como objetivo lo descripto en la categorización de los subcontroles comentados en la sección anterior del documento

The Critical Security Controls for Effective Cyber Defense [8], logrando así la conformación de una grilla que permitirá ubicar los controles de acuerdo a la fase (Identificar, Proteger, Detectar, Responder, Recuperar) e iteración. Las cuatro iteraciones se clasifican como: a) **Logros Rápidos** (primera iteración): Controles, Métricas y recomendaciones para brindar protecciones inmediatas sin un mayor costo o cambio de infraestructura; b) **Medidas de Visibilidad y Atribución** (segunda iteración): Mayores controles, métricas y recomendaciones para monitorear y controlar la efectividad de dichos controles; **Mejora de la Configuración de Seguridad de la Información (**tercera iteración): Reducir prácticas débiles de seguridad, vulnerabilidades y sus impactos, mantenimiento y configuración apropiada de los controles; d) **Subcontroles Avanzados** (cuarta iteración): Minimizar posibilidades de éxito de atacantes con determinación, instalación de controles de alto costo.

Fig. 3. Secuencia a seguir para el marco de trabajo propuesto

3.2 Función del Marco de Trabajo

Cada cuadrícula conformada entre una fase y una iteración contendrá una "X" cantidad de controles a implementar y cumplir. La sumatoria del cumplimiento de cada uno de los controles dará el grado de cumplimiento de cada cuadrícula. El Marco de trabajo también tendrá la posibilidad de calcular el grado de cumplimiento no sólo de cada cuadricula sino también por fase e iteración. La Fig. 4 muestra un ejemplo de la interfaz propuesta, donde se pueden apreciar una categorización por colores que indican los grados de cumplimiento.

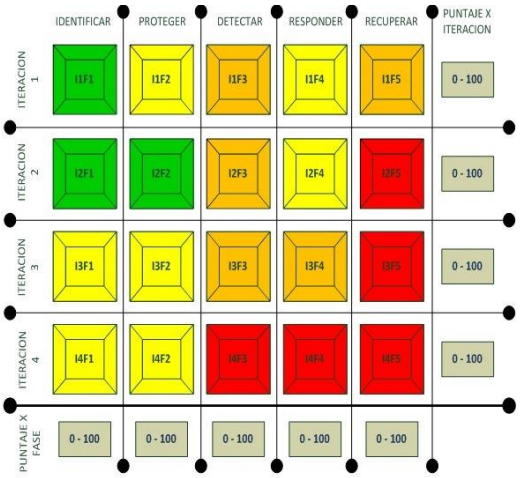

Fig. 4. Interfaz de explotación del Framework propuesta

3.3 Funcionamiento de la interfaz de carga.

Como se explicó anteriormente, cada cuadrícula estará compuesta por un listado de controles en la interfaz de carga. Dicha interfaz mostrará por cada control de seguridad un link a una documentación de ayuda y referencia para poder dar un valor de cumplimiento del control como así también links de sitios recomendados para mayor información. La interfaz de carga facilita parametrizar cada uno de los controles para la necesidad de cada usuario modificando la columna de Obligatorio / Recomendado, la ponderación que el usuario asigne o considere apropiada, como así también asignar un puntaje de cumplimiento. En la Fig. 5 se puede ver un ejemplo de la cuadrícula correspondiente a la fase 1 e iteración 1. Recordemos que el objetivo de la fase 1 corresponde a identificar "recursos permitidos de la empresa (SW, HW, PC's, etc.) y la iteración 1 corresponde a controles, métricas y recomendaciones para brindar protecciones inmediatas sin un mayor costo o cambio de infraestructura. El usuario al acceder a la interfaz de carga se encontrará con el listado de controles correspondientes a esta cuadrícula con una parametrización estándar recomendada que podrá ser modificada según la necesidad particular del mismo. El primer paso del usuario es considerar que controles son obligatorios y cuales son recomendados. Posteriormente se deberá asignar una ponderación de cada control y el valor a elegir estará contenido entre 0 y 1. Con respecto al puntaje el usuario irá completando el grado de cumplimento del control y el valor a ingresar estará contenido entre 0 y 100. El cálculo del total de la cuadrícula se determina de la siguiente manera: a) se calculará el Subtotal máximo de cada control de seguridad: Subtotal (Máximo) = Ponderación Ingresada X 100, b) se calculará el Subtotal real de cada control de seguridad: Subtotal = Ponderación Ingresada X Puntaje otorgado .c) Siendo el total de la cuadrícula igual a la relación entre la sumatoria de los subtotales y la sumatoria de los subtotales máximos, multiplicado por 100 para obtener el porcentaje. Siguiendo

con el ejemplo de la Fig. 5 el total de la cuadrícula sería igual a: Total Cuadricula (407,60/462)* 100= 88,22%.

INTERFAZ DE CARGA
PRIMERA ITERACIÓN, PRIMERA FASE

CONTROLES, MÉTRICAS Y RECOMENDACIONES PARA BRINDAR PROTECCIONES INMEDIATAS SIN UN MAYOR COSTO O CAMBIO DE INFRAESTRUCTURA

N.U.C.	NOMBRE DEL CONTROL	OBLIGATORIO / RECOMENDADO	PONDERACION	PUNTAJE	SUBTOTAL
I1F1-CCS01-01	Generar Inventario preliminar de dispositivos	OBLIGATORIO	0,7	80	56
I1F1-CCS01-02	Complementar el inventario preliminar de dispositivos con información DHCP	OBLIGATORIO	0,3	100	30
I1F1-CCS01-03	Automatizar la actualización del inventario de dispositivos	OBLIGATORIO	0,35	100	35
I1F1-CCS01-04	Cantidad de dispositivos no autorizados conectados en la red	RECOMENDADO	0,2	100	20
I1F1-CCS01-05	Tiempo de detección de nuevos SW instalados (min).	OBLIGATORIO	0,4	50	20
I1F1-CCS01-06	Tiempo de envío de alertas a los administradores por instalación de SW no autorizados(min).	RECOMENDADO	0,5	100	50
I1F1-CCS02-07	Tiempo para alertar que una aplicación de SW fue descubierta (min).	RECOMENDADO	0,49	100	49
I1F1-CCS02-08	Cantidad de aplicaciones de SW no autorizadas están instaladas en la red.	RECOMENDADO	0,27	100	27
I1F1-CCS02-09	Tiempo promedio para eliminar aplicaciones de SW no autorizadas.(min)	OBLIGATORIO	0,3	100	30
I1F1-CCS02-10	Es la política por defecto denegación de ejecución e un software (si o no)	OBLIGATORIO	0,51	60	30,6
I1F1-CCS02-11	Las carpetas de los ejecutables tienen restricciones de acceso a escritura (si o no)	OBLIGATORIO	0,6	100	60

Fig. 5. Interfaz de carga

4 Conclusiones y futuras líneas de trabajo

Se realiza un proceso exploratorio en término a las definiciones de ciberespacio, ciberguerra, ciberdefensa. Se propuso armar una base sólida y progresiva de controles de seguridad tomando como base inicial diferentes documentos de seguridad a fin de generar una propuesta inicial de un Framework de explotación, que facilite la gestión y diagnóstico de seguridad en el contexto de la ciberdefensa. En futuras líneas de trabajo se pretende articular la valoración de los controles y su análisis con el empleo de sistemas basados en conocimiento que asistan a la determinación del diagnóstico de seguridad de una unidad en el marco de la ciberdefensa.

5 Referencias

1. Gibson, W. (1984). Neuromancer. Ace Books(Gibson, 1984).
2. Umphress, T.C. (2007). Air&Space Power Journal. Obtenido de: “El Ciberespacio: ¿Un Aire y un espacio Nuevo? http://www.airpower.au.af.mil/apjinternational/apj-s/2007/3tri07/umphress.html
3 Gonzalez, J.A. (06/03/2010) Obtenido de: http://es.scribd.com/doc/32463107/grupo-de-el-ciberespacio

4.Wynne, H.M. (01/03/2007). *Air&Space Power Journal*. Obtenido de Flying and Fighting in Cyberspace: http://www.airpower.au.af.mil/airchronicles/apj/apj07/spr07/wynnespr07.html

5 ND. (2012). *La enciclopedia cubana en la red*. Obtenido de Ciberespacio: http://www.ecured.cu/index.php/Ciberespacio

6. Geers, K. (2010). A Brief Introduction to Cyber Warfare. *Common Defense Quarterly*, 16-17

7 Tabansky, L. (May de 2011). Basic Concepts in Cyber Warfare. Obtenido de INSS, The Institute for National Security Studies:http://www.inss.org.il/index.aspx?id=4538&articleid=2351

8 The Critical Security Controls for Effective Cyber Defense. Version 5 (CSC-5) del "Council on CyberSecurity. https://www.sans.org/media/critical-security-controls/CSC-5.pdf

9 Strategies to Mitigate Targeted Cyber Intrusions" del "Department of Defense – Intelligence and Security of Australian Government.http://www.asd.gov.au/infosec/mitigationstrategies.htm

10 Security and Privacy Controls for Federal Information Systems and Organizations (800-53 Rev.4) de National Institute of Standards and Technology (NIST).http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

11 Framework for Improving Critical Infrastructure Cybersecurity de National Institute of Standards and Technology (NIST).http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf