



**UNIVERSIDAD NACIONAL DE LA DEFENSA
INSTITUTO DE INTELIGENCIA DE LAS FFAA
ESPECIALIZACION EN GESTIÓN DE INFORMACIÓN
MILITAR TERRESTRE**

Trabajo Final Integrador

TEMA:

Uso y Empleo de Tecnología en el Diseño de un Sistema de Medidas de Seguridad de Contrainteligencia.

TITULO:

Desarrollo de un Sistema Tecnológico de Control y Supervisión Aplicado a la Manipulación de Información Clasificada.

Autor: TP Juan Pablo LÓPEZ ACUÑA.

Director: CR (R) Augusto CAYO.

Diciembre 2022

“Las ideas expresadas sólo representan la postura personal del autor, por lo que son de su absoluta responsabilidad, no reflejando en consecuencia la opinión del Instituto de Inteligencia de las Fuerzas Armadas y de la Universidad de la Defensa Nacional.”

Resumen

El cumplimiento de las Medidas de Seguridad de Contrainteligencia se encuentra estrechamente ligadas a un proceso adaptativo constante como consecuencia de un escalonado crecimiento de los métodos y medios de procesamiento, almacenamiento de información, documentos o archivos en diversos dispositivos y servidores.

A tal efecto, contar con personal altamente capacitado para hacer frente a nuevos desafíos es el principal menester del Ejército Argentino. Así mismo, se requiere la elaboración de nuevos planes, actualización de sistemas, desarrollo de proyectos y establecimiento de nuevos procedimientos que permitan un adecuado cumplimiento de las necesidades surgidas de un estudio previo de vulnerabilidades.

El grado de urgencia de empleo es directamente proporcional a la creciente necesidad de obtención de información por diferentes motivos, ya sean colectivos o personales, como más adelante será desarrollado.

A lo largo de todo este trabajo se buscará poner en manifiesto; mediante definiciones, conceptos y ejemplos actuales; la imprescindible obligación del uso y empleo de tecnologías en el diseño de un sistema para perfeccionar las inermes Medidas de Seguridad de Contrainteligencia frente a la revolución tecnológica que atraviesan todos los países del mundo.

Palabras claves:

Análisis – Vulnerabilidades – Tecnologías – Infraestructura – Ciberseguridad – Seguridad – Fuga - Información – Digital – Contrainteligencia.

Índice

1.1 Introducción.....	4
1.2 Hipótesis:.....	6
1.3 Objetivos de la Investigación:.....	6
Capítulo 1 “La problemática vigente en la seguridad de la información en el Ejército Argentino”.....	8
2.1 Introducción.....	8
2.2 ¿Qué es la fuga de información?.....	9
2.3 La información como elemento de poder.....	10
2.4 La manipulación de la información en el Ejército Argentino.....	12
2.5 Alcance de las responsabilidades y las bases legales vigentes.....	15
2.6 Análisis de fugas de información recientes en las Fuerzas Armadas latinoamericanas.	20
2.7 Conclusiones Parciales.....	22
Capítulo 2 “Empleo de mecanismos y tecnologías a las Medidas de Seguridad de Contrainteligencia”.....	24
3.1 Introducción.....	24
3.2 Ciclo de la seguridad de la información.....	25
3.3 Mecanismos preventivos en la seguridad de la información.....	26
3.4 Mecanismos correctivos en la seguridad de la información.....	27
3.5 Mecanismos detectivos en seguridad informática y auditorías.....	28
3.6 Puesta en marcha en el desarrollo de nuevas tecnologías y aprovechamiento de los medios disponibles para brindar adecuadas Medidas de Seguridad de Contrainteligencia	30
3.7 Conclusiones parciales.....	31
4.1 Conclusiones Finales.....	32
Bibliografía.....	34

1.1 Introducción

El desarrollo de las nuevas tecnologías, la informática y las telecomunicaciones, supone un cambio trascendental en el trabajo, la economía, la administración y ocio entre algunos de los aspectos que están variando a pasos agigantados conformando un entorno mucho más globalizado e informatizado donde el Internet juega un papel trascendental como medio de transmisión e intercambio de todo tipo de información.

Las organizaciones, entre las cuales las militares no se encuentran excluidas, se enfrentan a una realidad digitalmente modificada, donde las nuevas tecnologías generan nuevos riesgos y necesidades de protección, siendo éste un medio el cual requiere una actualización permanente demandando reacciones rápidas para anticiparse a un incidente y una intensa conciencia para proteger la información.

Si bien la protección de la información hace referencia a una serie de propiedades, la principal de ellas es la confidencialidad. La fuga de información hace referencia a la pérdida de la misma, de forma que la información que solo debe ser conocida por un grupo de personas, en el ámbito de una Unidad táctica, termina siendo visible o accesible para otros.

Como cualquier otro incidente de seguridad, la propia existencia de una fuga de información posee un orígenes y causas determinadas. Y dicho hecho afectará no solo a la propia organización o Unidad, sino que también podrá tener impacto sobre grupos externos de personas o individuos que pudieran tener una relación directa o indirecta con la misma, o también así mismo a otras organizaciones.

Una de las grandes preocupaciones generadas a partir de la segunda década del siglo XXI, está centrada en el impacto y las consecuencias que surgen de éste tipo de incidentes, habiendo sido causa de numerosas recomendaciones por parte de las autoridades militares hacia las Unidades tácticas, ya que la filtración de información puede dañar su imagen pública y suponer un impacto negativo, además de generar desconfianza e inseguridad en la población en general al observar las vulnerabilidades de una organización cuyo significado es la protección los intereses nacionales.

También podría generar consecuencias a terceros, como en el caso de que la información filtrada haga referencia a individuo relacionado con la fuerza o no.

Es oportuno mencionar que las medidas de seguridad de contrainteligencia no contemplan la dificultad de ocultar estos incidentes, debido a la velocidad de su transmisión y que en un gran número de oportunidades los sucesos son difundidos en Internet y otros medios, los cuales no poseen la obligación jurídica de mantener la confidencialidad de la información al no ser responsables de la protección de esta. Es aquí donde la deficiencia de profesionalismo se refleja en la falta de compromiso por evitar la divulgación de información ante una fuga visible en la organización a la que muchos responsables pertenecen.

En la doctrina existen un conjunto de “Responsabilidades en el control de la información”, y una serie de advertencias a tener en cuenta en caso de una transgresión a las normas de seguridad donde se advierte la previsión de sanciones, sino también las penalidades contenidas en el Código Penal, ya que, en muchas ocasiones, estos incidentes terminan con la difusión o publicación de datos tanto institucionales o personales que cuentan con clasificación de seguridad.

Precisamente el temor a las posibles sanciones es en ocasiones, uno de los principales motivos para la ocultación de un incidente. Esta será una de las responsabilidades de las Unidades tácticas, destinada a decidir a quién se debe de informar y en qué orden (lo cual se encuentra descrito en el reglamento de medidas de seguridad de contrainteligencia), así como otros aspectos relativos a determinar si se hace público y la comunicación del suceso a los medios.

La frase «el enemigo está dentro» se popularizó hace ya unos años cuando los incidentes de seguridad cuyo origen estaba en el interior de las propias Unidades militares comenzaron a aumentar. Dicho aumento cambió la percepción y el concepto de protección, puesto que hasta entonces las medidas de seguridad se centraban en crear barreras para proteger a las mismas de las amenazas centradas en la seguridad física de la información.

Actualmente, el origen de las amenazas puede ser tanto externo como interno. En el caso del origen interno, aquellas personas del área de trabajo en la cual rescinde o de la cual deriva una determinada información, se ha convertido en uno de los principales focos de todo tipo de incidentes de seguridad.

Su finalidad puede ser la venta de información clasificada para la obtención de un beneficio económico, la venganza, el daño a la imagen, la utilización de determinada información para su aplicación en otro ámbito. Pero también pueden estar relacionados con la falta de conocimiento, formación o sencillamente errores. Éstos son algunos de los principales motivos detrás de una buena parte de los incidentes de seguridad en la fuga de información.

Desde el punto de vista de las amenazas externas podemos decir que el entorno ha cambiado enormemente en la última década, con la aparición de nuevos objetivos como cibercriminales o activistas, quienes han tomado Internet y lo han convertido en un medio en el que se desarrollan todo tipo de estrategias con diversos objetivos, como conseguir beneficio económico, llevar a cabo acciones de protesta o daño de imagen.

1.2 Hipótesis:

La concientización en la necesidad de actualizar los sistemas de seguridad de la información en las unidades tácticas impulsará la implementación de nuevas tecnologías aplicadas para reducir considerablemente las vulnerabilidades vigentes en las Medidas de Seguridad de Contrainteligencia.

1.3 Objetivos de la Investigación:

Objetivo General: Demostrar la urgente necesidad de implementar nuevas tecnologías al actual sistema de Medidas de Seguridad de Contra Inteligencia de las Unidades Tácticas para impedir la fuga de información.

Objetivo Especifico Nro 1: Analizar y determinar aquellas tecnologías que permitan reducir las vulnerabilidades en la fuga de información.

Objetivo Especifico Nro 2: Proponer el empleo de un plan de educación sobre amenazas, seguridad en la gestión de información y obligaciones en el marco legal vigente.

Capítulo 1 “La problemática vigente en la seguridad de la información en el Ejército Argentino”

“La seguridad de la información documentada es la resultante de aplicar un conjunto de medidas para alcanzar un nivel adecuado de confidencialidad, integridad, disponibilidad, no repudio y autenticación de la información clasificada durante todo el proceso de su gestión”¹

2.1 Introducción

La seguridad de la información es un tema que incluye a todos aquellos que son parte componente de cualquier sistema; entendiéndose como sistema a cualquier organismo o entidad pública o privada dependiente o en la cual se manipula información sensible. Pudiendo causar daños que afecten a la confidencialidad y/o integridad de una persona, como del elemento al cual pertenece.

La fuga de información es una falencia que afecta directa o indirectamente al Ejército Argentino, exponiéndose a amenazas cuyo origen pudieran ser internos o externos. Un adecuado análisis de riesgos permite minimizar el impacto que conlleva la fuga de información si se toman los controles preventivos, detectives y correctivos adecuados.

Pero el primer paso a analizar para brindar un correcto asesoramiento será el estudio de la problemática actual y el impulso de la aplicación de tecnología en las medidas de seguridad de contrainteligencia para abordar dicha problemática.

No es nada nuevo que uno de los activos más importantes para toda organización es la información. Hoy en día, el mundo atraviesa un periodo de conexión a través de la integración de la tecnología y esto incluye a los usuarios de cualquier dispositivo tecnológico en estrecha relación con la organización. Generando un alto riesgo para la confidencialidad, integridad y disponibilidad de la información.

El incremento experimentado en la fuga de información por parte de, no solo el Ejército Argentino, sino de otras fuerzas, entidades públicas y privadas en la actualidad es un claro ejemplo donde

¹ Art 7.003, Capítulo VIII - Medidas de Seguridad de Contrainteligencia (ROP-11-06).

documentos de carácter sensible son expuestos al exterior de las organizaciones. Algunos de estos ejemplos serán detallados en el presente trabajo.

Sin embargo, el desafío más grande en la fuga de información es el personal, ya que, en forma voluntaria o involuntaria, son la principal causa en la fuga de información. Y de este modo, se produce otro de los efectos de esta vulnerabilidad que es el deterioro de la imagen que bringa ante la sociedad a la cual sirve el Ejército Argentino, donde el ciudadano promedio podría cuestionar la incapacidad de controlar ataques o fugas de información crítica por parte de la institución que debe brindar seguridad a la Nación por excelencia.

La seguridad de la información depende de tres factores, las herramientas tecnológicas, los procesos y las personas. Siendo el segundo el de menor injerencia, las grandes empresas optan por realizar grandes inversiones en las herramientas que garanticen la protección de la información, debiendo aplicarse juntamente con sesiones de capacitación para concientizar a los usuarios que la manipulan.

2.2 ¿Qué es la fuga de información?

Antes de hablar de fuga de información, debemos saber que la protección de la información está determinada por tres aspectos básicos:

La confidencialidad: Este principio se refiere a que la información solo puede ser accedida por el personal autorizado.

La integridad de la información: Esto significa que la información es correcta, sin modificaciones o errores, ya que debemos tener en cuenta que la misma pudo haber sido cambiada intencionalmente o por error, y estaríamos en riesgo al emplear dicha información como cierta. Pudiendo llegar a generar diferentes grados de afectación, desde leves hasta gravísimos.

La disponibilidad de la información: Se refiere a la información a la que una persona o sistema autorizado pueda acceder cuando sea necesario.

Teniendo en cuenta lo anteriormente descrito, podemos decir que nos referimos a fuga de información cuando hablamos de una violación de la información como la pérdida de confidencialidad, dando acceso a personas no autorizadas a información con clasificación de seguridad o privilegiada.

Es así como las consecuencias de una fuga de información serán siempre negativas, en un aspecto tan importante como en la reputación del elemento militar del cual se haya producido la fuga como de la organización en su conjunto, ya que el conocimiento público de la existencia de una filtración de información dañará ésta imagen, impactando muy negativamente en la opinión social y generando desconfianza e inseguridad tanto a la población como a los mismos integrantes de la organización que de dicha seguridad dependen.

Cabe mencionar que lo más importante respecto al Data Leak (termino específico que hace referencia a la fuga de información y datos), es que comúnmente estos casos en su mayoría desencadenan una red de difusión o publicación de datos de carácter personal (como, por ejemplo: datos personales, unidad de destino, función y cargo e incluso en muchas oportunidades hasta datos concretos de la familia del personal perjudicado). Estas situaciones han dejado expuestos a personal de la fuerza en más de una oportunidad.

Siendo este uno de los aspectos más críticos de la gestión de fugas de información y será una de las responsabilidades de toda la cadena de comando del elemento en el cual se produce el quiebre decidir cómo manejar el incidente en términos de cumplimiento de las obligaciones legales, la imposición de medidas disciplinarias y, sobre todo, el manejo de los medios de comunicación institucional y de noticias.

2.3 La información como elemento de poder

Anteriormente hemos hecho referencia a la fuga de información como elemento crítico que podría perjudicar, con distinto grado de relevancia, al individuo en forma personal y/o profesional, a la organización como elemento de seguridad del estado. Pero ¿Qué hay de la información como elemento de poder? ¿En qué consisten las llamadas “Operaciones de Información”? ¿Se podría

ver afectada la Fuerza en estos términos como consecuencia de la pérdida de confidencialidad, integridad y disponibilidad de la información?

Desde el punto de vista de las Operaciones de Información (OI) proporcionan opciones más flexibles y no letales que podrían ser utilizadas en tiempos de paz para el estudio detallado del ambiente operacional y/o completamiento de la información sobre la propia organización, por una potencial amenaza o enemigo, ya sean estatales o no. Es importante no perder de vista que, si bien nuestro país no posee hipótesis de conflicto, no significa que otros países posean intereses diferentes. De esta manera se vuelve fundamental el conocimiento de los individuos que conforman una organización para determinar factores en su personalidad (sobre todo de un Comandante/Jefe) que bajo un exhaustivo análisis podría llegar a influir en las tácticas y procedimientos empleados por él en hipotéticas acciones.

La forma de manipulación y análisis de la información de un potencial enemigo es variable y el efecto a lograr estará determinado por la capacidad de este. Lo que se buscará con esta capacidad será la de producir un efecto en todos los niveles de la conducción, buscando sobre todas las cosas evitar la sorpresa y advertir como podría el adversario emplear sus medios disponibles, logrando el fin último que será evitar la amenaza.

La integración de la información debe incluirse en rigurosos procesos conjunto. Se debe elaborar medidas aprovechables para que sirvan de base en la toma de decisiones de las Operaciones de Información.

El emplear Operaciones de Información concentradas, integradas y sincronizadas para disuadir a un adversario mediante la manipulación de la información y medios de comunicación no constituye un acto bélico. No obstante, si bien no es un acto de guerra, tiene que ver con la adquisición de una posición ventajosa cuyo objetivo será lograr un efecto disuasivo deseado.

El ataque de redes informáticas implica el uso de redes informáticas para negar, interrumpir o degradar computadoras, redes informáticas o información establecida en cualesquiera de las mismas. En la actualidad, las tropas regulares e irregulares dependen cada vez más de computadoras y redes informáticas para facilitar el mando y control, transacciones que hacen posible el apoyo y la coordinación de medidas.

La falta de interés, conocimiento y/o capacitación sobre la importancia de la información radica en cuanto el individuo ignora su trascendencia y la capacidad de procesamiento, valoración e integración de la información para la obtención de un resultado concreto de mayor importancia.

Es así como el menosprecio de la importancia que obtiene la información manipulada por un individuo termina siendo la causa principal de la fuga de información provocada por la negligencia de este.

En este punto, es importante hacer entender que la información por sí misma sirve de poco cuando no es sometida a un riguroso procesamiento y, al mismo tiempo, asimilar y ver como real la existencia de un potencial oponente inteligente e intangible que se nutre de la información obtenida para lograr sus objetivos particulares en base a una estrategia mayor.

2.4 La manipulación de la información en el Ejército Argentino

Como se sabe en la mayoría de la reglamentación vigente, a la información oficial originada en organismos de defensa, Fuerzas Armadas, de inteligencia y/o privados, se les asignará la clasificación de:

- Estrictamente Secreto y Confidencial
- Secreto
- Confidencial
- Reservado
- Público Militar (Interno)
- Público

Así mismo, podemos definir el tratamiento de la información como “El conjunto de previsiones y procedimientos que se adoptan para evitar el riesgo de la difusión indebida de la información clasificada que emana de dichas fuentes, como también para evitar, neutralizar o disminuir las

posibilidades de reunión de información por parte del enemigo, a través de su espionaje (inteligencia) u otros procedimientos de obtención”.

El acceso a la información clasificada dentro de una computadora debe tener restricciones en función a los distintos niveles de acceso.

Si bien la responsabilidad, para determinar el acceso a la información, corresponderá al comandante, director o jefe, con el asesoramiento del oficial de inteligencia, también el personal es responsable de la protección de esta, relacionado con la generación y/o distribución de dicha información.

De esta manera podemos definir a la información como un activo. Para entenderlo mejor, diremos que se considera activo a aquellos bienes o derechos que tienen un beneficio o acción aplicable a futuro, en función al uso de su información.

En este caso, los activos como información son un recurso de propiedad de una Nación, que, a través de sus instituciones, al ser aplicados se obtienen beneficios a futuro. Por lo tanto, se considera un bien útil que deberá ser valorado, administrado y protegido.

En este punto es oportuno contextualizar el ambiente que rodea a la fuga de información. Hoy vamos a tratar un tema que todo el mundo sabe que existe, pero al que nadie se refiere.

Un informe consultado del Grupo Paradell del 2009 muestra que los canales más utilizados al surgir un hecho de fuga de información son correo electrónico (47%), dispositivos USB (28%), CD/DVD (13%), impresora (5%) y otros medios (7%). La constante indica que todos los comportamientos y prácticas de seguridad asociadas con el tema, tienen que ver con el recurso humano.

La fuga de información se asocia con tres elementos: personas, procedimientos y tecnología. Y aunque todos están unidos e interactúan de forma coordinada, la fuga de información se da primariamente por personas, impactando los procedimientos y la tecnología.

Como autor del presente trabajo final de investigación soy de opinión que todo radica en una falta de gobierno y de orientación sobre la administración de la información dentro del Ejército

Argentino en todos sus niveles. Los procesos y la tecnología son asuntos muy operativos que no siempre dependen de la estructura táctica y/o estratégica. Si en una organización no existe un adecuado gobierno con foco de cultura de control y de administración de riesgos, ni la tecnología ni los procesos van a funcionar de manera acorde, porque no se encuentran dentro de ese lineamiento organizacional. De los tres elementos planteados, el foco primario es el tema estructural que nace en una estructura de gobierno.

A nivel de la investigación después de sucedidos los hechos, se pueden determinar causantes de la fuga de información, fallas sistémicas de la organización, en lo que tiene que ver con las personas, fallas en los procesos y con debilidades en la tecnología, siempre dependiendo de la naturaleza de la fuga.

Porque muy probablemente hay fugas de información de carácter interno dentro de la organización relacionados con ataques o intrusiones externas teniendo en cuenta las vulnerabilidades de la organización o elemento, lo cual ocasiona la fuga.

Periódicamente en el Ejército Argentino se realizan recomendaciones mediante Mensajes Militares, Directivas, Memorándums, etc. pero se le ha dado más protagonismo a la información y, por supuesto, a la tecnología como herramienta de desarrollo. En tal sentido, se ha crecido y se ha evolucionado. Pero, en los asuntos de manejo, a sabiendas de qué es lo importante o lo confidencial y qué lo público, no se adoptan medidas preventivas y/o correctivas suficientes por quienes manipulan la información en forma negligente.

Otros estudios muestran estadísticas sobre la fuga de información y señalan que cerca del 80% de los eventos relacionados con la información son producidos por motivaciones sin intención, por no conocer qué pasa; por ignorancia o por aprovechamiento de otras personas que simplemente desconocen el funcionamiento y la importancia de la información, y permiten la fuga de esta.

Otro aspecto es el vengativo, es decir, criminal con un propósito negativo. Ahí hay una brecha muy grande para poder trabajar. ¿Cómo hago para educar a la persona que es el motivador, para que sepa qué es lo bueno y lo malo, qué se debe hacer y qué no? Teniendo claridad al respecto, entonces saldrán los procedimientos, la tecnología para moldear la organización.

Si bien se han tomado numerosas medidas para la prevención de ataques cibernéticos mediante la adquisición de diferentes sistemas con personal dedicado exclusivamente a detectar este tipo de delitos o filtraciones, es de público conocimiento en las Fuerzas Armadas y particularmente en el Ejército Argentino que no hemos podido aún con la fuga de información física que no contempla ningún aspecto tecnológico.

2.5 Alcance de las responsabilidades y las bases legales vigentes

La doctrina establece que *“La responsabilidad, para determinar el acceso a la información, corresponderá al comandante, director o jefe, con el asesoramiento del Oficial de Inteligencia y del responsable de la posesión de determinada información y no de quien hubiere de recibirla. Esta responsabilidad no eximirá a quien solicitare o recibiere el conocimiento correspondiente, de la obligación de hacer conocer su “NECESIDAD DE SABER”², antes de recibir dicha información...”³*

Generalmente, la fuga de información es endilgada a la Unidad dependiente por falta de aplicación de medidas de seguridad y/o de divulgación, ausencia de dispositivos de seguridad y la errónea clasificación de la información sensible.

Por otro lado, se ha evidenciado responsabilidad en aquellos que manipulan y gestionan determinada información sensible en las distintas áreas dentro de una Unidad táctica, ya sea por desconocimiento de las medidas de seguridad o por intenciones inequívocas de dar un uso inadecuado a la información, por exceso de confianza en el tema de seguridad y/o falta de interés en la protección de datos.

Los errores o la falta de conocimiento y formación son otra de las causas más comunes de la fuga de información. El personal que manipula información sensible debe utilizar los recursos que la

² “Concepto que indica que deberá proporcionarse (o hacer tomar conocimiento) una información militar, exclusivamente a la persona o elemento que poseyere la obligación de conocer dicha información...” Art 7.001, Capítulo VII – Inteligencia Táctica (ROD-11-01).

³Art 7.024, Capítulo VIII - Medidas de Seguridad de Contrainteligencia (ROP-11-06).

organización pone a su disposición de forma responsable, como en el caso del uso del correo electrónico, la navegación Web u otros servicios y, por otro lado, debe disponer de ciertos conocimientos y formación en relación con su actividad diaria, siendo responsabilidad de la organización proporcionar la información y la formación necesaria de manera que pueda desempeñar su función adecuadamente.

Es necesario implementar medidas que garanticen la protección de la información, como un software diseñado para ese fin, que envíe señales de alerta cuando se presenten incidentes y bloquee las acciones que no se encuentran permitidas. Los hallazgos encontrados nos permitirán corregir las falencias con la finalidad de evitar futuras pérdidas de información, sensibilizando a las personas sobre la fuga de información y las consecuencias de esta.

Las organizaciones no militares, cada vez es más habitual que durante el proceso de contratación de un empleado, se solicite por escrito la conformidad con diversas políticas de confidencialidad o de seguridad, entre otras, de manera que el futuro empleado, deja por escrito la aceptación de las condiciones correspondientes. Dicho procedimiento otorga no solo un acuerdo jurídico sino también un nivel mayor de compromiso por parte de este, lo cual es considerado un método efectivo al momento de incorporar personal militar en un área de conducción o sector donde la información adquiere mayor relevancia o sensibilidad al otorgarle un nivel de confidencialidad. Sin embargo, debido a la formación en lo que a valores morales y éticos respecta, esta acción es pasada por alto al suponerse una obviedad.

No es lo mismo leer un documento, que leerlo y posteriormente firmarlo. Como es el caso al tomar conocimiento con la doctrina que a “Medidas de Seguridad de Contrainteligencia” se refiere. El sentido y las consecuencias en ambos casos son muy distintos. Por otro lado, se cuenta con una legislación que permite establecer límites legales a las actividades de personal y que pueden ser utilizadas como mecanismos de disuasión para evitar un uso malintencionado de la información.

Uno de los mayores peligros son los *Malware*⁴, los cuales permiten automatizar una buena parte del proceso relacionado con la fuga de información y además, el diseño de muchos de estos

⁴Malware es un acrónimo del inglés de malicious software, traducido al español como código malicioso. Los malwares son programas diseñados para infiltrarse en un sistema con el fin de dañar o robar datos e información.

programas, incluye técnicas que permiten mantener oculto el código en un sistema, mientras recoge y envía información. Por lo cual es importante indicar que los sistemas y aplicaciones precisan de actualizaciones y revisiones constantes.

En el marco del cibercrimen como servicio o CaaS (del inglés *cybercrime-as-a-service*) hay organizaciones de delincuentes que ofrecen servicios de programas maliciosos ilegales en la nube (por ejemplo, para interrumpir operación, robar datos,) dando lugar al llamado Malware como servicio o MaaS (del inglés *Malware as a Service*). Estos servicios son accesibles desde cualquier lugar y son extremadamente fáciles de usar. Cualquiera los puede usar y por tanto se les pueda vender a cualquiera. Estos servicios son contratados por operadores externos.

Ejemplos típicos de estas actividades maliciosas son el robo de información (ej. troyanos), dañar o causar un mal funcionamiento el sistema informático, provocar un perjuicio económico, chantajear al propietario de los datos del sistema informático, permitir el acceso de usuarios no autorizados, provocar molestias o una combinación de varias de estas actividades.

En informática, se denomina caballo de Troya, o *troyano*⁵, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. Hay ciertas fuentes que lo descatalogan como malware debido a que aparentemente no causa daños en los sistemas, pero causan también otra clase de perjuicios, como el robo de datos personales.

La mayoría de las infecciones con troyanos ocurren cuando se ejecuta un programa infectado con un troyano. Estos programas pueden ser de cualquier tipo, desde instaladores hasta presentaciones de fotos. Al ejecutar el programa, este se muestra y realiza las tareas de forma normal, pero en un segundo plano y al mismo tiempo se instala el troyano. El proceso de infección no es visible para el usuario ya que no se muestran ventanas ni alertas de ningún tipo, por lo que evitar la infección de un troyano es difícil.

Llegados a este punto, conviene intentar determinar un concepto de delito informático.

⁵El término troyano proviene de la historia del caballo de Troya mencionado en la Odisea de Homero.

“Delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. Ante el extendido uso y utilización de las nuevas tecnologías en todas las esferas de la vida y el creciente número de usuarios, consecuencia de la globalización digital de la sociedad, la delincuencia también se ha expandido a esa dimensión. Gracias al anonimato y a la información personal que se guarda en el entorno digital, los delincuentes han ampliado su campo de acción y los delitos y amenazas a la seguridad se han incrementado exponencialmente.”⁶

Es sabido que la información ha adquirido un valor altísimo desde todo punto de vista, inclusive el económico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas (acceso ilegítimo, sabotaje o daño informático, espionaje informático, etc.) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales.

Ya con algún tiempo de vigencia, la Ley 26.388 incorpora al Código Penal delitos cometidos por medios informáticos. Donde define un documento como la representación de actos o hechos sin importar el soporte utilizado para almacenarlo o transmitirlo.

El Código Penal sanciona las siguientes conductas:

- Abrir o acceder indebidamente una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido.
- Apoderarse indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado.
- Suprimir o desviar de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.
- Interceptar o captar comunicaciones electrónicas o telecomunicaciones de carácter privado o de acceso restringido.

⁶Penal, 13° Congreso sobre Prevención del Delito y Justicia. «13° Congreso sobre Prevención del Delito y Justicia Penal, Doha, del 12 al 19 de abril de 2015». www.un.org. Consultado el 13 de junio de 2019.

La pena se agrava si el autor comunica o publica el contenido de la carta, escrito, despacho o comunicación electrónica y esto causa perjuicio.

Además, el Código Penal sanciona el acceso por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema informático de acceso restringido. La pena se agrava cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Referido al acceso de banco de datos se sanciona el acceder ilegítimamente a un banco de datos personales, proporcionar o revelar información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a guardar por ley, insertar o hacer insertar datos en un archivo de datos personales.

Donde en su Art 7 menciona:

“ARTICULO 7º — Sustituyese el artículo 157 del Código Penal, por el siguiente:

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 8º — Sustituyese el artículo 157 bis del Código Penal, por el siguiente:

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

- 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;*
- 2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.*
- 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.*

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.”⁷

Otro de los puntos importantes es que, en general, los delitos informáticos son anónimos, ya que Internet permite la posibilidad de crear identidades ficticias o porque el autor conoce la forma de ocultar su identidad. Esto trae aparejadas dificultades en momento de determinar el posible autor del ilícito, ya que muchas veces los dispositivos utilizados para la comisión del delito son de acceso compartido por varias personas.

Teniendo en cuenta lo anteriormente desarrollado, es importante no solo tener pleno conocimiento sobre aquellas personas que son incorporadas a las áreas de la conducción de las Unidades tácticas y otros sectores donde se manipule información sensible o clasificada, sino también la toma de medidas para minimizar o anular las posibilidades de fugas de información. Para ello, es indispensable un estricto control del cumplimiento de aquellas medidas descritas en la doctrina a la cual se hace referencia y la educación, preparación, capacitación continua en lo que a ello respecta. Razón por la cual adquiere importancia la constatación de estas actividades por medio de documentos para preservar la confidencialidad.

2.6 Análisis de fugas de información recientes en las Fuerzas Armadas latinoamericanas

A continuación, veremos los casos más recientes de fuga de información producidos en Fuerzas Armadas de países vecinos o latinoamericanos, sin hacer énfasis en las razones por las cuales se han producido los hechos, con la intención de poner en manifiesto la repercusión que han traído aparejadas las fugas en cuestión y así despertar el interés por la generación de un alto grado de conciencia organizacional e individual, pudiendo observar la necesidad de la implementación de tecnologías para la implementación de un sistema de control respecto a la problemática en cuestión.

⁷Ley 26.388. Reforma del Código Penal en materia de Delitos Informáticos. Deroega y modifica algunos incisos introducidos por el art. 32 de la Ley 25.326 al Código Penal.

Comenzando por el caso más reciente, iniciaremos con la noticia referida a documentos militares filtrados del Estado Mayor Conjunto de las Fuerzas Armadas (EMCO) de Chile. Donde se atribuye esta fuga al hackeo de correos electrónicos del EMCO en cuestión, donde habrían sido expuestos “Informes de estimación de riesgo de amenazas” enviado en el mes de abril del año 2022.

Más de 400.000 documentos con clasificación “reservado, secreto y ultrasecreto” fueron revelados. La filtración de estos archivos militares chilenos desnuda no sólo la vulnerabilidad del sistema informático de la defensa trasandina sino también la obsesión chilena por la actividad militar argentina.

Según la información brindada por los distintos medios de comunicación, revelan que uno de los documentos dice: *“El nuevo radar de vigilancia y control aéreo emplazado por Argentina en Río Grande (Tierra del Fuego) es motivo de preocupación y deberían arbitrarse los medios para su neutralización”*. Otro: *“Argentina acaba de anunciar oficialmente un plan para adquisición de municiones con previsiones para los próximos 10 años que se sostendrá con aportes de un fondo específico aprobado por el congreso”*⁸.

Otro de los párrafos del medio citado anteriormente menciona que “Dentro de los análisis de inteligencia con mayor clasificación de seguridad, se encuentran varios dossiers relacionados con la figura de Alberto Fernández y del “partido de gobierno””.

El siguiente ejemplo se basa en información clasificada expuesta del Ejército Peruano. La cual vale aclarar que fue obtenida presuntamente por un grupo de *Hacktivistas*⁹ por medio de vulnerabilidades en correos electrónicos, que si bien mencionamos al principio del apartado que no se haría hincapié en el medio por el cual se produjeron las fugas de información, es importante analizar el medio utilizado para la manipulación de información clasificada.

⁸ Según noticia publicada el 24 de septiembre del 2022 por el medio de comunicación Infobae en el siguiente link: <https://www.infobae.com/politica/2022/09/24/la-filtracion-de-archivos-militares-de-chile-revela-inquietud-y-un-prolijio-seguimiento-de-la-actividad-de-defensa-de-la-argentina/>

⁹ Definición de Hacktivismo y Hacktivista según el Instituto Lisa: “El hacktivismo se define como la realización de actos, normalmente maliciosos, en Internet para promover unas ideas políticas, religiosas o sociales. Los hacktivistas llevan a cabo acciones o ataques en el ciberespacio mediante dispositivos electrónicos con el fin de propagar y defender unas ideas o valores concretos”.

Así fue como se extrajeron se extrajeron 175 gigabytes de información desde los servidores del Ejército y del Comando Conjunto de las Fuerzas Armadas de Perú. Revelando mas de 283.000 correos electrónicos que quedaron exhibidos en dos bases de datos en internet.

Así se encontraron al menos tres planes de guerra ideados por los militares de ese país a implementar en caso de un conflicto armado con Chile. Dentro de ellos están las trayectorias que seguirían las unidades, hasta las estrategias de engaño que se implementarían para distraer a las fuerzas chilenas.

En dichos documentos fueron filtrados los análisis de inteligencia donde se detallan las capacidades de la 1ra Brigada Acorazada Coraceros y la Brigada Rancagua, de la Brigada Acorazada Cazadores, el Regimiento Huamachuco, entre otras Unidades militares. Habría también habría listas de posibles vulnerabilidades y fortalezas presentes en las infraestructuras chilenas y en la composición de sus fuerzas militares.

Tomando estos dos ejemplos de fuga de información de información clasificada, podríamos suponer que estos casos o similares, llegarían a afectar las relaciones bilaterales, tratados y/o negociaciones con los países en cuestión o terceros países que podrían verse influenciados de manera directa o indirecta por la documentación filtrada. Sin mencionar el sinnúmero de afecciones que traería aparejado este tipo de problemáticas.

2.7 Conclusiones Parciales

De acuerdo a las diferentes definiciones, conceptos, bases y ejemplos expresados previamente, permiten concluir que uno de los mayores problemas surgidos en la manipulación de información clasificada , posterior fuga de información y efectos aparejados a la misma es la falta de conciencia y capacitación profesional individual en el cumplimiento de las normas que establecen las bases legales vigentes, los reglamentos, directivas y mensajes militares que pautan el procedimiento a llevar a cabo para evitar negligencias de este tipo.

La fuga de información clasificada se ha vuelto un negocio cuya rentabilidad es directamente proporcional al valor de los documentos y archivos obtenidos. También se ve afectado por movimientos Hacktivistas que se encuentran en búsqueda del error humano y en sus sistemas que ocasionen la fuga para su posterior exposición con finalidades políticas o ideológicas.

Es por esto por lo que en la actualidad existe una lucha por el control de la información de la cual no se ha tomado noción por parte de la mayoría de los integrantes del Ejército Argentino y de esta manera generan una ventana de oportunidades a las amenazas latentes en esta segunda década del siglo XXI, caracterizada por su dependencia tecnológica.

Los cambios no solo se deben limitar al intento por generar mayor eficiencia laboral dentro del Ejército Argentino, sino que debe incluir a las Medidas de Seguridad de Contrainteligencia, principalmente en el esfuerzo de lograr un delicado control de la información.

Sin duda, ya estamos transitando una nueva sociedad a la cual muchos aún se resisten a la implementación de nuevas tecnologías en el ambiente laboral por falta de entendimiento. Pero en este novedoso escenario, no existe una mano invisible que haga que esta nueva forma de trabajo sea más segura y sustentable. Por el contrario, lo que se necesita es crear un tipo de ecosistema de políticas integradas y coherentes que acompañen el proceso de transición para lograr el diseño de un sistema de medidas de seguridad adecuadas a las épocas que se transitan.

Capítulo 2 “Empleo de mecanismos y tecnologías a las Medidas de Seguridad de Contrainteligencia”

“Aquel que puede modificar sus tácticas en función de su oponente y así conseguir la victoria podrá ser llamado capitán nacido del cuerno del cielo.”

(Sun Tzu)

3.1 Introducción

La capacidad de adaptación al cambio está dada por la flexibilidad institucional del Ejército Argentino, la cual es considerada como una de las ventajas competitivas en toda organización y resulta vital para el creciente desarrollo frente al mundo globalizado.

En así que para poder fomentar el comportamiento adaptativo y que exista una respuesta rápida frente a un cambio es necesario desarrollar nuevos procesos y cambiar los procesos existentes de forma rápida, segura y económica, flexibilizar el proceso de trabajo y estar dentro del objetivo final del proceso a lograr.

Ejércitos con mayor desarrollo tecnológico aseguran que solo aquellos que cuentan con un ambiente donde se asumen riesgos y donde no se ve el fracaso como un factor negativo pueden facilitar la innovación y la adaptación al cambio. Debido a que, al estar condicionada por estrategias en constante evolución, implica explorar nuevas prácticas y aportar nuevos recursos.

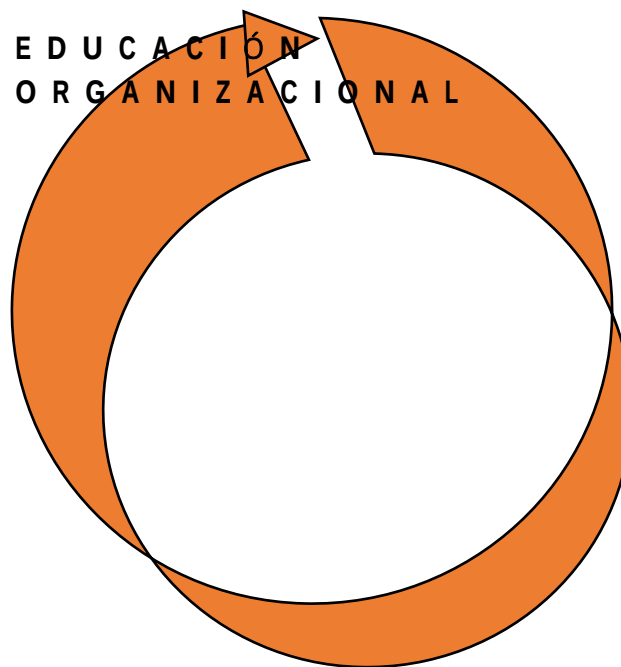
Hay un viejo refrán que dice: *“Es mejor prevenir que curar”*. El cerebro está mejor preparado para resolver situaciones problemáticas a medida que se presentan, antes que para anticiparse y realizar acciones preventivas que permitan evitar que los problemas ocurran. Por otro lado, la vida moderna exige mayor movimiento bajo la premisa de que hay que aprovechar el tiempo, y es por eso siente que cuando no se está haciendo algo, se está procediendo mal.

Es igualmente negativo es cuando se deja para más adelante algo que se debe hacer hoy. La causa es no saber separar lo urgente de lo importante, y cuando se percibe una oportunidad o una amenaza, el pensamiento deja la resolución para más adelante. Es por esto que en este capítulo se abordarán los aspectos a estudiar para evitar todo lo descripto en el capítulo anterior.

3.2 Ciclo de la seguridad de la información

El ciclo de la seguridad de la información se trata de un ciclo en el que se debe mantener una organización, para mitigar el riesgo, amenaza o pérdida de información como activos principales.

Consistirá en un principio fundamental que englobará la totalidad del ciclo que se define como “Educación Organizacional”. Y dentro de él se conciben cuatro pasos que se centran en las bases legales, reglamentaciones, directivas y mensajes emanados de la superioridad.



La evaluación consistirá en encontrar una metodología o una estrategia que le permite saber en qué estado está su seguridad, deberá ser un trabajo totalmente objetivo y específicas para cada sector de la organización. Así se podrán estudiar las vulnerabilidades encontradas, ver las prioridades para resolver y determinar si el estado de seguridad actual es suficiente, con el fin de tener una visión general.

El diseño estará orientado a la elaboración de una solución que corrija y mitigue los aspectos estudiados en el paso anterior, siendo coherentes con la prioridad establecida. Se establecerán también parámetros para indicar el nivel de éxito del nuevo software o tecnología empleada.

Ya con la nueva tecnología desarrollada, vendrá la implementación de ésta. Donde se ejecutarán todas las actividades propuestas en la evaluación para implementar todos los métodos de seguridad para que los sistemas sean más seguros. Los cambios, soluciones y aplicaciones realizadas serán siempre documentadas. Así se realizarán varias pruebas para comprobar el nivel de éxito analizado en el paso “*Diseño*”.

Durante la administración se deberá custodiar el soporte brindado para obtener una mejora constante en el proceso. Indicando el estado en que se encuentra y realizando nuevas evaluaciones que permitirán cerrar el ciclo y mantener la continuidad del perfeccionamiento de los sistemas empleados

Todo este ciclo se ve envuelto por la mayor de las consignas que será la educación organizacional. Si no se logra generar una conciencia colectiva de la seguridad de la información y la gravedad de una mala manipulación de esta, no se podrá llevar a cabo dicho ciclo en forma responsable y coordinada, lo cual podría llegar a desencadenar problemas aún mayores.

3.3 Mecanismos preventivos en la seguridad de la información

La definición de un mecanismo preventivo consta de revisiones diarias. Puede haber algunos cambios o mejoras en diversos aspectos de vez en cuando. Hardware, software o elementos que intervienen en sistemas y procesos. Por lo tanto, la revisión depende de los procesos de la empresa y de cada proceso individual. El mecanismo preventivo es en realidad a largo plazo por lo que la mayoría lo considera una pérdida de tiempo y dinero.

Puede compararse con los seguros médicos o vehiculares, los cuales se pueden pagar durante años y nunca tener un accidente, en primera instancia se podrá analizar que es algo muy bueno, pero después en algún momento se podrá pensar que es un desperdicio haber pagado tanto tiempo sin verse beneficiado directamente.

El principal obstáculo al que se enfrentan las organizaciones al querer aplicar los mecanismos preventivos es la aceptación y el compromiso de todos los involucrados, hacer entender que no es una carga, es parte de los procesos y de lo que se debe hacer bien en la organización.

Se podrán seguir los siguientes pasos como métodos preventivos de seguridad:

- Se deberá comprimir la información, que si bien no todo archivo se puede comprimir, se deberán hacer las valoraciones respectivas para determinar cuáles son aquellos archivos que si lo necesitan.
- Realizar un metodológico respaldo de la información es de los pasos más comunes realizados por toda organización y es característico de aquellas que poseen un grado de aceptación general al cambio. Debe haber un control detallado del tipo de archivo para su clasificación e integración con el resto de la información respaldada. Quizás algún tipo de inventario digital sea de ayuda para su control y supervisión.
- Seleccionar el horario de respaldo no será de menor importancia ya que se sugiere que se realice en horarios de menor tráfico de información y lo ideal es realizarlo una vez terminadas diferentes jornadas laborales.
- Por último y siendo el punto más crítico en estos pasos es el control de los medios. El cual se refiere a la capacidad de tener acceso a la información respaldada y comprimida. Lo cual es un aspecto para solucionar por su amplia peligrosidad pero que, mediante el empleo de barreras electrónicas, como por ejemplo de identificación, puede ser neutralizado el riesgo en gran medida.

Los pasos anteriormente descriptos son los más básicos a tener en cuenta. Por otro lado, debe ser tomada en cuenta la actualización de sistemas, antivirus, firewall, navegación por internet e intranet, gestión de contraseñas y control de accesos.

3.4 Mecanismos correctivos en la seguridad de la información

A diferencia de los métodos preventivos, estos se aplican después de un hecho sucedido y su principal función es la corrección de las consecuencias. Una forma de aplicación es mediante la asistencia inmediata de personal altamente capacitado o adquiriendo soluciones como softwares y parches de actualización que logran resolver los problemas. En estos casos el tiempo es un recurso de gran valor debido a que es escaso, por lo que es recomendable la adquisición o desarrollo de sistemas de rápido acceso que brinden soluciones inmediatas.

Los pasos para seguir para emplear mecanismos correctivos son:

- Primero se realizará la catalogación y asignación del problema, en los cuales se listan aquellos problemas a los que se pueden enfrentar, detectar y clasificar. Ésta es una forma que nos permitirá saber afrontar el problema y buscar la respuesta más adecuada.
- Luego se realizará el análisis del problema que se ha presentado, el cual deberá ser realizado en primera medida por expertos en caso de no contar con un sistema.
- Analizar la solución será el paso siguiente, donde antes de intentar solucionar un problema, se debe analizar la propuesta. No habrá muchas oportunidades de aplicar una correcta solución, por lo que la misma deberá de ser bien planteada y ejecutada, para intentar predecir lo que podría suceder.
- En este punto, es vital analizar la documentación, ya que los cambios a realizar posiblemente sean empleados con tiempo limitado y rápido, razón por la cual podría generar un error al saltar algún paso o cambios realizados.

3.5 Mecanismos detectivos en seguridad informática y auditorias

Ya sea que la posible fuga de información o problema en cuestión haya sido por una causa externa o interna de los usuarios al manipular en forma negligente información clasificada, será de gran importancia determinar el grado de intrusión o medio por el cual ha surgido el error o intrusión a un determinado recurso.

Los objetivos de este tipo de mecanismos serán:

- Detectar el punto exacto del error para poder llegar a una solución adecuada para su posterior recuperación.
- Detectar actividades sospechosas y conocer los eventos sucedidos, ya que, si no se encuentra la raíz del error, será necesario al menos saber lo que sucedió y partir desde este punto.

Un típico concepto relacionado a este tipo de mecanismos es la intrusión, las cuales son una secuencia de acciones deshonestas donde en la mayoría de los casos se busca acceder a un acceso no autorizado.

Los pasos básicos para detectar una intrusión son:

- Primero se debe revisar los patrones de acceso, donde se buscarán patrones de comportamiento como, por ejemplo, accesos a determinados horarios o usuarios que acceden a una misma información.
- Posteriormente se buscará revisar las transacciones. Es decir que mayormente las intrusiones irán acompañadas de al menos un intento de transacción de información, lo cual no es un hecho concreto que así suceda, pero es altamente probable.
- Muchos sistemas tienen incorporados sistemas de bloqueo de emergencia, los cuales podrían llegar a detener de forma drástica cualquier transacción no autorizada, evitando así el riesgo de que continúe la fuga de información.

En cuanto a las auditorías, existirán aquellas destinadas a mostrar las principales necesidades de protección de las herramientas utilizadas por la organización, para el posterior desarrollo de nuevas tecnologías (como ser softwares); como también aquellas realizadas para alertar sobre las preocupaciones relevantes de un proceso con el fin de garantizar la conformidad con las bases legales, directivas y mensajes emanados por la superioridad.

Las auditorías deberán ser realizadas a modo de inspección por personal altamente capacitado, el cual a su vez debe ser controlado y almacenado en lugares separados y con una alta clasificación de seguridad.

Así mismo, deben llevarse a cabo con el acuerdo de un órgano director de la superioridad. Se recomienda que la verificación sea de solo lectura y solo en casos particulares, deben ser generadas copias para su uso. Estas se aislarán y almacenarán en forma segura y eliminadas al final de la auditoría. Toda información debe ser puesta a disposición de la auditoría y serán identificados por la organización y todos los accesos deben ser controlados y registrados para posteriormente documentarlos.

3.6 Puesta en marcha en el desarrollo de nuevas tecnologías y aprovechamiento de los medios disponibles para brindar adecuadas Medidas de Seguridad de Contrainteligencia

El objeto del presente trabajo no es brindar un catálogo de tecnologías aplicadas a la seguridad de la información como Medida de Seguridad de Contrainteligencia, sino comentar algunas de sus características y consecuencias sobre la actividad. De hecho, en muchos casos las tecnologías de la seguridad se pueden considerar capaces de ser fusionadas con otras para configurar un sistema de última instancia de mayor nivel de seguridad (como, por ejemplo, las características del control de accesos reflejado en la reglamentación vigente de Medidas de Seguridad de Contrainteligencia).

El Ejército Argentino cuenta con una enorme cantidad de personal ampliamente capacitado para el desarrollo de sistemas que podrían funcionar en forma coordinada para mitigar al máximo las negligencias surgidas en la manipulación de la información que derivan comúnmente en la fuga de datos y recursos clasificados. Así como también el personal idóneo para llevar a cabo las auditorías descritas en títulos anteriores, tanto para la evaluación y desarrollo de mecanismos de seguridad de información, sino también para hacer cumplir el compromiso legal que norman las leyes vigentes para todo aquel personal con acceso a información clasificada.

De esta manera se presentan tres tipos de medidas a adoptar.

- Medidas organizativas:
 - Se deberá poner en marcha las prácticas para la gestión de fugas de información.
 - Habrá que definir una política de seguridad y procedimientos para todo el ciclo de vida de la información (datos).
 - Es necesario establecer sistemas integrados con niveles de accesos y roles específicos.
 - Se llevarán a cabo capacitaciones, formaciones y actualizaciones para el personal idóneo de cada región referido a ciberseguridad.
 - Se deberá implementar un sistema de gestión de seguridad adecuado a las necesidades particulares del Ejército Argentino en sus distintos niveles de conducción.

- Medidas técnicas:
 - Implementar o desarrollar sistemas de control de accesos e identidad para la manipulación de información clasificada con capacidad de registro de actividades.
 - Implementar tecnologías de bloqueo de emergencia sobre los sistemas que contienen información sensible.
 - Emplear softwares de control de tráfico y copias de seguridad.

- Medidas legales:
 - Se deberá realizar un documento legal de aceptación de la política de seguridad y conformidad por parte del personal que manipule información clasificada. El cual deberá estar previamente instruido sobre el funcionamiento y adecuado empleo de los sistemas.
 - Deberán elaborarse medidas de carácter disuasorio en base a las normas vigentes para el cumplimiento responsable de las funciones adoptadas.

3.7 Conclusiones parciales

De acuerdo con lo expuesto previamente a lo largo de todo el capítulo me permite concluir que las herramientas para la prevención de fallos en las Medidas de Seguridad de Contrainteligencia y el empleo de nuevas tecnologías se encuentra al alcance del Ejército Argentino. Sin embargo, es necesario un profundo estudio del caso, siguiendo los pasos descriptos, para lograr un acabado sistema de seguridad que logre contener cualquier fuga de información.

A su vez, la labor de generar una cultura de concientización y educación adaptada a las exigencias que revolución tecnológica ponen en juego es un factor determinante sin el cual no se podrá llegar a obtener resultados eficientes. Donde cualquier esfuerzo caerá en el vacío provocando grandes pérdidas de tiempo y dinero.

Así mismo, el tiempo es escaso mientras la tecnología, la conectividad y las amenazas avanzan a pasos agigantados. Y resulta imperante tomar cartas en el asunto de manera inmediata para transformar los desactualizados sistemas vigentes antes de que las consecuencias sean aún mayores o surja una pérdida irreparable del control de la información.

4.1 Conclusiones Finales

A lo largo de todo el trabajo se han presentado conceptos, definiciones y estudios de casos que nos permiten concluir sobre la necesidad del empleo de nuevas tecnologías aplicadas a las Medidas de Seguridad de Contrainteligencia para el adecuado control de una problemática vigente que ha tenido grandes repercusiones en el año en curso, como es la fuga de información clasificada.

En el primer capítulo se pudieron observar definiciones, conceptos, empleo de la información en el Ejército Argentino, normativas legales y ejemplos actuales de filtraciones de documentos de enorme relevancia internacional, que han afectado el tablero geopolítico. Permitiendo introducirnos de lleno en una problemática presente en el Ejército Argentino de la cual todos somos testigos.

El segundo capítulo se basó en una presentación de una metodología de empleo respecto a los procedimientos necesarios para mitigar las causas y efectos derivados de aquellos aspectos descriptos en el capítulo anterior. Donde se expuso el diseño de un sistema basado en la aplicación de nuevas tecnologías a desarrollar o adquirir, que generaría una solución rentable a la problemática vigente de las Medidas de Seguridad de Contrainteligencia en el Ejército Argentino.

Se pudo observar que dicha problemática también se presenta en otros países sudamericanos que poseen vulnerabilidades similares a las propias. Así también, se pudo analizar como las consecuencias pueden trascender, por ejemplo, a un plano geopolítico e influir en las relaciones internacionales dependiendo de la sensibilidad de la información filtrada.

Basados en estos ejemplos, fue posible inferir que la adaptación a las nuevas tecnologías y el aprovechamiento eficiente del tiempo para la aplicación de medidas o gestión de desarrollo de proyectos es fundamental para lograr estar a la altura de las circunstancias que exigen los tiempos

modernos. Y que la resistencia al cambio o el retroceso en los métodos de empleo no son una opción viable.

Así mismo, es imposible concebir cualquier reforma o actualización de los procedimientos empleados a las medidas de seguridad sin un esquemático plan de capacitación y educación periódica y responsable, el cual irá de la mano con la aplicación de esporádicas auditorias que permitan culminar un ciclo de estudio y perfeccionamiento de los sistemas vigentes. No debemos olvidar que la responsabilidad del usuario que manipula información clasificada forma parte del sistema de medidas de seguridad y como tal debe ser consciente de sus obligaciones ante las normas vigentes, las cuales deberán ser consumadas.

Para finalizar es necesario entender el poder que la información adquiere en las manos adecuadas, brindando una posición estratégica ventajosa a aquel que la posea. Donde, hoy más que nunca, se alza no solo un comercio ilegal y altamente rentable, sino también el popularizado surgimiento de un sinnúmero de movimientos de activistas digitales que ponen en riesgo la seguridad nacional. Por ende, no hay razón para no poner en marcha todos los recursos físicos e intelectuales disponibles para generar un sistema lo mejor diseñado posible aplicado a las Medidas de Seguridad de Contrainteligencia.

Bibliografía

- Sphera Pública. (2003). *La guerra en la era de la información: Propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación*. Obtenido de <https://elcomercio.pe/mundo/actualidad/la-primavera-arabe-la-primera-revolucion-del-smartphone-y-las-redes-sociales-facebook-twitter-blackberry-noticia/>
- Fernando Morales (24 de septiembre de 2022). *Infobae*. Obtenido de: <https://www.infobae.com/politica/2022/09/24/la-filtracion-de-archivos-militares-de-chile-revela-inquietud-y-un-prolijo-seguimiento-de-la-actividad-de-defensa-de-la-argentina/>
- Infobae. (22 de septiembre de 2022). *Infobae* . Obtenido de: <https://www.infobae.com/america/america-latina/2022/09/22/se-filtraron-documentos-militares-chilenos-en-los-que-hablan-de-argentina-y-alberto-fernandez/>
- Adam Saunders. (Marzo de 2018). *BBVA*. Obtenido de: <https://www.bbvaopenmind.com/wp-content/uploads/2018/03/BBVA-OpenMind-Adam-Saunders-El-impacto-de-la-tecnologia-en-el-crecimiento-y-el-empleo.pdf>
- La Nación. (23 de septiembre de 2022). *La Nación*. Obtenido de: <https://www.lanacion.com.ar/el-mundo/filtran-documentos-militares-chilenos-en-los-que-acusan-a-alberto-fernandez-de-tener-la-costumbre-de-nid22092022/>
- Nicolas Massai D. y Nicolas Sepúlveda. (06 de octubre de 2022). *Ciper*. Obtenido de: <https://www.ciperchile.cl/2022/10/06/peru-files-hackeo-al-ejercito-peruano-desnuda-sus-planes-de-guerra-en-caso-de-un-ataque-desde-chile/>
- Lisa Institute (14 de julio de 2021). *Lisa Institute*. Obtenido de: <https://www.lisainstitute.com/blogs/blog/hacktivismo-definicion-tipos-modus-operandi-motivaciones>
- Diego Vera (22 septiembre de 2022). *Bio Bio Chile*. Obtenido: <https://www.biobiochile.cl/noticias/nacional/chile/2022/09/22/hackeo-al-estado-mayor-conjunto-defensa-anuncia-sumario-y-presenta-denuncia-ante-justicia-militar.shtml>
- Mariela Molina, Natalia Benítez, Christoph Ernst (2018). *Organización Internacional del Trabajo*. Obtenido de: <file:///C:/Users/Usuario/Desktop/MILITAR/11.%20TFI/2.%20TFI%20L%C3%93PEZ%20ACU%C3%91A/cambios%20tecnol%C3%B3gicos%20y%20laborales.pdf>
- Ing. Arsenio Antonio Aguirre Ponce (2017). *Universidad de Buenos Aires*

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería. Obtenido de:

file:///C:/Users/Usuario/Desktop/MILITAR/11.%20TFI/2.%20TFI%20L%C3%93PEZ%
20ACU%C3%91A/NUEVOS%20DOCUMENTOS/TESIS%20INFRAESTRUCTURA%
20CRITICA%20DE%20LA%20INFORMACION.pdf

Juan Fernando Ormachea Montes (2019). *ESTRATEGIAS INTEGRADAS DE*

CIBERSEGURIDAD PARA EL FORTALECIMIENTO DE LA SEGURIDAD NACIONAL.

Obtenido de:

[http://repositorio.caen.edu.pe/bitstream/handle/20.500.13097/156/TESIS%20para%20opt
ar%20Grado%20de%20DOCTOR_Juan%20ORMACHEA%2016_07_20.pdf?sequence=](http://repositorio.caen.edu.pe/bitstream/handle/20.500.13097/156/TESIS%20para%20opt
ar%20Grado%20de%20DOCTOR_Juan%20ORMACHEA%2016_07_20.pdf?sequence=)