INGENIERÍA SOCIAL Y SUS IMPLICANCIAS EN LAS OPERACIONES MILITARES: UN ANÁLISIS DESDE LA PERSPECTIVA DE LA CIBERSEGURIDAD MILITAR

Social engineering and its implications in military operations: an analysis from the perspective of military cybersecurity

Mayor Carlos Bustamante Quintero[1]

Resumen

La ingeniería social (IS) constituye una amenaza latente para las operaciones militares, enfocándose en explotar las vulnerabilidades humanas para acceder a información sensible o interrumpir sistemas. A diferencia de los ataques técnicos, la IS manipula el comportamiento humano, haciendo difícil de contrarrestar. Las consecuencias de estos ataques pueden ser devastadoras, comprometiendo la seguridad y la capacidad operativa de las fuerzas armadas. Para mitigar los riesgos asociados a ataques mediante IS, se requiere un enfoque integral que combine capacitación continua del personal, implementación de tecnologías de seguridad avanzadas y la creación de políticas de seguridad dinámicas. Solo a través de la conciencia, la preparación y la adaptación constante, las fuerzas armadas podrán fortalecer su ciberseguridad y proteger sus sistemas críticos contra las amenazas de IS.

Palabras clave: Ingeniería social, operaciones militares, ciberseguridad, vulnerabilidades humanas.

Abstract

Social engineering (SE) is a latent threat to military operations, focusing on exploiting human vulnerabilities to access sensitive information or disrupt systems. Unlike technical attacks, SE manipulates human behavior, making it difficult to counter. The consequences of these attacks can be devastating, compromising the security and operational capabilities of the armed forces. To mitigate the risks posed by being attacked through SE, a comprehensive approach is required that combines continuous training of personnel, implementation of advanced security technologies, and the creation of dynamic security policies. Only through awareness, preparedness, and constant adaptation will the armed forces be able to strengthen their cybersecurity and protect their critical systems against SE threats.

Keywords: Social engineering, military operations, cybersecurity, human vulnerabilities.

[1] Oficial de Estado Mayor del arma de Ingenieros, Especialista en inteligencia militar en el Ejército de Chile e inteligencia policial en Carabineros de Chile, Magister en Relaciones Internacionales, Seguridad y Defensa en la Academia Nacional de Estudios Políticos y Estratégicos y Licenciado en ciberseguridad en la Universidad Mayor. Correo electrónico: carlos.bustamante.quintero@gmail.com

Introducción

El advenimiento de la era digital ha modernizado el campo de batalla, trasladando las hostilidades al ciberespacio. En este nuevo escenario, las organizaciones militares se enfrentan a una amplia gama de amenazas cibernéticas que ponen en peligro la confidencialidad, integridad y disponibilidad de sus sistemas y datos. Entre estas amenazas, los ataques que emplean ingeniería social (IS), emergen como uno de los más sofisticados y difíciles de contrarrestar, explotando las vulnerabilidades psicológicas del ser humano para obtener información confidencial o acceso a sistemas restringidos, pudiendo comprometer a las instituciones de la defensa, afectando de esta forma a las operaciones militares.

La IS, puede definirse como *"el acto de manipular a una persona para que lleve a cabo una acción "que puede ser o no" lo más conveniente para el objetivo"* (Hadnagy C. , 2011, pág. 37), una definición más detallada indica que la IS puede entenderse como *"el conjunto de técnicas de tipo social que pueden usar ciertos individuos, grupos u organizaciones de cualquier tipo para manipular o persuadir a objetivos humanos, con la intención de que realicen acciones, tomen decisiones o revelen información valiosa para el atacante, en forma voluntaria"* (Ramos, Barbero, Marugan, & González, 2015, pág. 17).

Para los efectos de este artículo, y con la finalidad de mejorar el entendimiento a un nivel menos técnico, se definirá la IS como la manipulación psicológica de individuos para que revelen información confidencial o realicen acciones que comprometan la seguridad. Independiente a las definiciones, es indudable que la IS se ha convertido en un arma poderosa en el arsenal de los ciber atacantes. A diferencia de los ataques que explotan vulnerabilidades de hardware (físicas) o de software (lógicas), la ingeniería social se centra en el factor humano, aprovechando la confianza, la curiosidad y el miedo de las personas.

De acuerdo con lo anterior se plantea que el factor humano, debido a sus inherentes vulnerabilidades psicológicas, tales como la tendencia a apoyar o a servir, representa el eslabón más débil en la cadena de ciberseguridad militar. La IS, al explotar estas vulnerabilidades, y ser utilizadas como parte de un ataque mayor, constituye una amenaza significativa para las operaciones militares, poniendo en riesgo la confidencialidad de la información clasificada, la integridad de los sistemas de mando y control, y la disponibilidad de las infraestructuras críticas.

El presente artículo pretende reflexionar sobre la amenaza que la IS representa en las operaciones militares cuando es utilizada como parte de un ataque mayor y dar respuesta a la pregunta ¿Qué medidas pueden adoptar las organizaciones de la

defensa, especialmente chilenas, para fortalecer la ciberseguridad frente a las amenazas de la IS y proteger así la información clasificada, las operaciones militares y la reputación de las fuerzas armadas?

Para dar cumplimiento a lo anterior, en la primera parte se abordará la IS y sus tácticas, donde se analizarán las diferentes técnicas utilizadas por los ciber atacantes, como el *Phishing,* el *Tailgating* y el *Pretexting,* así como los objetivos y motivaciones de estos ataques, seguidamente se reflexionará sobre el factor humano como factor débil, donde se explorarán las vulnerabilidades psicológicas que hacen a las personas susceptibles a la manipulación social, y cómo estas pueden ser explotadas en el contexto militar. Posteriormente se abordará el impacto de la IS en las operaciones militares, donde se abarcarán las consecuencias de estos ataques en diferentes áreas de las operaciones militares, como la inteligencia, las comunicaciones y el mando y control y finalmente se presentarán algunas estrategias de mitigación, que propondrán medidas para fortalecer la ciberseguridad militar frente a las amenazas de la IS, incluyendo la concientización y capacitación del personal, el desarrollo de tecnologías de seguridad y la implementación de políticas y procedimientos de seguridad.

La ingeniería social y sus tácticas

La ingeniería social, son técnicas que explotan las vulnerabilidades psicológicas del ser humano y se ha convertido en una de las principales amenazas para la ciberseguridad militar, cuando son utilizadas como parte de un ciberataque o un ataque físico. Los atacantes emplean una variedad de técnicas sofisticadas para manipular a las personas y obtener acceso a información confidencial o sistemas restringidos.

Tal como ya se ha señalado en la introducción del presente artículo, la IS utiliza al factor humano de una organización, para lograr sus objetivos, valiéndose de diferentes tácticas, a diferencia de los ataques cibernéticos tradicionales que se centran en vulnerabilidades técnicas, la IS explota la confianza, la curiosidad y el miedo de las personas.

Para lograr un mejor entendimiento, se describirán algunas de las tácticas de IS más utilizadas:

Phishing y Spear Phishing

El *Phishing* consiste en el envío masivo de correos o mensajes, en los que se les solicita a los receptores, que ingresen a una página haciendo click en un link, todo lo anterior a través de una historia ficticia haciendo alusión a un premio, solicitud de información por parte de una entidad bancaria, posibilidad de corte de algún servicio por no pago, etc.

En el caso del *Spear Phishing*, se utiliza la misma táctica, sin embargo, esta no es masiva, se dirige a un objetivo específico, por lo que la historia ficticia que se utiliza para generar el ingreso al sitio web, es mucho más preparada y enfocada al objetivo.

En ambos casos, una vez dentro del sitio previamente generado, el cual cuenta con una estructura similar al original, se le puede solicitar al objetivo "…*datos financieros, datos confidenciales, militares, o cualquier tipo de información que se encuentre dentro de una organización o empresa"* (Ramos, Barbero, Marugan, & González, 2015, pág. 95). También se pueden solicitar datos personales que posteriormente son utilizados para generar otras credenciales como parte de un mayor ataque.

Tailgating

El *Tailgating* es una táctica de IS bastante simple pero efectiva, que consiste en que un intruso no autorizado siga de cerca a una persona autorizada para acceder a un área restringida, aprovechando la apertura de puertas o torniquetes. Para esta técnica podría utilizarse algún tipo de indumentaria que hiciera "normal" su ingreso, de esta forma podría acceder a áreas donde se almacena información clasificada, equipos sensibles o sistemas de control, lo que podría permitirle obtener información valiosa, sabotear equipos o incluso llevar a cabo actos de espionaje. *Esta táctica se aprovecha de la "predisposición a sujetar la puerta al que viene detrás por motivos educacionales"* (Ramos, Barbero, Marugan, & González, 2015, pág. 29)

De igual forma una vez ingresando a un área que cuente con servidores, o computadores conectados a los sistemas de defensa, pueden conectarse dispositivos que, aprovechando alguna brecha de seguridad, puedan causar el robo de información o la vulneración de algún sistema para un ataque a mayor escala posterior.

Pretexting

El *Pretexting* es una táctica de IS donde un atacante crea una historia falsa o un escenario convincente (pretexto) para manipular a una víctima y obtener información confidencial. *"Es más que simplemente producir una mentira; en algunos casos puede ser crear una identidad totalmente nueva y utilizarla para manipular al receptor de la información"* (Hadnagy C., 2023, pág. 91). Para el caso particular de las organizaciones militares, alguien podría hacerse pasar por un mando, un compañero de trabajo o incluso un proveedor para convencer a un funcionario de revelar datos confidenciales, como contraseñas, números de identificación o detalles sobre proyectos clasificados.

Las tácticas expuestas anteriormente solo son algunas de las muchas que pueden afectar las organizaciones, teniendo como denominador común, el aprovechamiento de las vulnerabilidades que presenta el ser humano para el logro de sus fines. Algo que hace aún más complicada su mitigación es que muchas de las cualidades que hacen vulnerable al ser humano, son aquellos valores y virtudes que son fomentadas en la vida en sociedad, tales como la confianza, el respeto hacia los adultos, la bondad, etc. Derivado de lo anterior la concientización y formación, son imprescindibles para mitigar los riesgos que atacan al factor humano de una organización.

El factor humano como eslabón débil

"El Ingeniero social, o atacante diestro en el arte del engaño, se alimenta de las mejores cualidades de la naturaleza humana: nuestra tendencia a servir de ayuda y apoyo, a ser educado, a colaborar y el deseo de concluir un trabajo" (Mitnick & Simon, 2006, pág. 299)

Una de las razones por las cuales la IS es tan efectiva, es la naturaleza misma del ser humano. Nuestras predisposiciones psicológicas, como la confianza, la reciprocidad y la urgencia, pueden ser explotadas por los atacantes para lograr sus objetivos. Tal como se mencionaba anteriormente, las vulnerabilidades que presenta el ser humano frente a los ataques que emplean IS no deben confundirse con deficiencias, sólo cuando se carece de una formación orientada a la seguridad, políticas adecuadas, además de un apoyo tecnológico suficiente, los valores y virtudes que posee el ser humano y que son aquellos que nos permiten vivir en sociedad, se transforman en vulnerabilidades, que aprovechadas por la IS, se transforman en amenazas a las organizaciones, en este caso particular, de defensa.

La confianza constituye un pilar fundamental en las interacciones humanas, pero en el ámbito de la ciberseguridad se erige como una vulnerabilidad explotable. Los atacantes suelen aprovechar la credibilidad que las personas depositan en entidades reconocidas para perpetrar engaños. Como acertadamente señala Kevin Mitnick, "*establecer la credibilidad es el primer paso en la mayoría de los ataques de ingeniería social"* (2006, pág. 314). Al cultivar una apariencia de cercanía y confianza, los atacantes logran manipular a sus objetivos para que revelen información sensible o concedan accesos que, a priori, parecen inofensivos. Sin embargo, estos datos suelen ser piezas clave en un rompecabezas más amplio, permitiendo a los atacantes escalar sus operaciones o validar hipótesis cruciales para sus organizaciones.

La confianza y el principio de reciprocidad constituyen dos pilares fundamentales de las relaciones humanas que, paradójicamente, se erigen como vulnerabilidades significativas en el ámbito de la ciberseguridad. Los atacantes, conscientes de esta dinámica, explotan hábilmente estas tendencias para manipular a sus víctimas y lograr sus objetivos maliciosos. Como señala Hadnagy (2023, pág. 131), al ofrecer un beneficio previo, como información gratuita o un favor, los ciberdelincuentes incrementan considerablemente la probabilidad de que sus solicitudes sean atendidas. Este mecanismo psicológico, conocido como reciprocidad, funciona como un ciclo vicioso: al conceder algo, el atacante genera en la víctima una sensación de deuda, lo que facilita que esta acceda a posteriores peticiones, impulsada por el deseo de equilibrar la balanza. Para explotar eficazmente esta vulnerabilidad, los atacantes suelen identificar o generar una necesidad específica en sus objetivos, estableciendo al mismo tiempo un lazo de confianza que les permita posicionarse como la solución a dicho problema. De esta manera, los cibercriminales pueden llevar a cabo sus ataques de manera más sutil y efectiva, aprovechando la predisposición humana a devolver favores.

Por otro lado, la urgencia y el miedo son emociones poderosas que pueden nublar el juicio de las personas. “*Nuestro cerebro está condicionado para reaccionar rápidamente ante una amenaza, el miedo es una de nuestras emociones básicas y, sin duda, nos lleva a tomar muchas decisiones”* (Deutsch, 2022, pág. 20). Los atacantes a menudo crean un sentido de urgencia o miedo para presionar a las víctimas a tomar decisiones apresuradas y sin pensar en las consecuencias. Por ejemplo, un mensaje que advierte sobre una cuenta bancaria bloqueada puede llevar a una víctima a revelar su contraseña sin verificar la autenticidad del mensaje.

Además de la confianza, la reciprocidad y el miedo, existen otras vulnerabilidades psicológicas que pueden ser explotadas por los atacantes, como:

- La autoridad, donde las personas tienden a obedecer a figuras de autoridad, incluso cuando las órdenes son claramente erróneas, es un principio psicológico que los atacantes aprovechan. De igual manera, la escasez, que genera una urgencia debido a que los recursos son limitados o alguna oferta tiene una duración determinada, puede llevar a las personas a tomar decisiones impulsivas y poco racionales.

- Por otro lado, la simpatía, ese sentimiento que nos inclina a ayudar a aquellos que percibimos como similares a nosotros o que se encuentran en una situación difícil, también es una herramienta poderosa en manos de los ciberdelincuentes. Al generar empatía, los atacantes pueden manipular a sus víctimas para que revelen información confidencial o realicen acciones que beneficien al atacante. Estos principios psicológicos, cuando son explotados de manera estratégica, pueden convertirse en poderosas armas en el arsenal de los cibercriminales, facilitando la ejecución de ataques de ingeniería social altamente efectivos.

Los sentimientos, principios y características humanas antes mencionados, normalmente son identificados como valores o virtudes, y no nos equivoquemos, lo son, sin embargo, cuando se carece del conocimiento, las políticas y la tecnología, pueden transformarse en el punto de entrada de un atacante. Las instituciones armadas o relacionadas a la defensa, no se encuentran ajenas a estos ataques que, de ser exitosos, pueden afectar gravemente a las operaciones militares.

Impacto de la ingeniería social en las operaciones militares

Los objetivos de los ataques de IS en el ámbito militar son diversos y pueden incluir el robo de información clasificada, el sabotaje de sistemas, el espionaje, la desinformación y la propaganda. Estos ataques pueden tener consecuencias devastadoras para las operaciones militares y la seguridad nacional.

La IS, lejos de ser una amenaza exclusiva del ámbito civil, ha penetrado profundamente en el dominio militar, con consecuencias potencialmente catastróficas para las operaciones. Los atacantes, ya sean actores estatales, no estatales o cibercriminales, emplean tácticas de IS para infiltrarse en redes militares, robar información clasificada, sabotear sistemas críticos y, en última instancia, socavar la capacidad de respuesta y la toma de decisiones de las fuerzas armadas.

Uno de los impactos más directos de la ingeniería social en el ámbito militar es la pérdida de información clasificada. A través de técnicas como el *phishing* y el *spear phishing*, los atacantes pueden engañar a miembros del personal militar para que

revelen contraseñas, credenciales de acceso o información sensible sobre operaciones en curso. Esta filtración de información puede comprometer misiones, poner en peligro vidas y dañar la reputación de una nación (Ross & Pillitteri, 2024).

Un ejemplo paradigmático de cómo la IS se ha utilizado como arma en conflictos contemporáneos lo encontramos en los ciberataques sufridos por Georgia durante el conflicto con Rusia en las regiones separatistas de Osetia del Sur y Abkhazia. Si bien los ataques a los sitios web del gobierno georgiano, que resultaron en su indisponibilidad o en la manipulación de su contenido para propagar desinformación, pueden parecer meramente técnicos, es fundamental comprender que detrás de ellos se esconden sofisticadas estrategias de IS. Al privar a la población de información veraz y confiable, los atacantes buscaron sembrar la confusión, erosionar la confianza en las instituciones gubernamentales y manipular la opinión pública, lo que a su vez debilitó la capacidad de respuesta del gobierno georgiano ante la crisis. Estos ataques no solo tuvieron un impacto directo en la infraestructura digital del país, sino que también representaron una forma de guerra psicológica, donde la información se convirtió en un arma de doble filo (Diaz del Río, 2011)

Los sistemas de mando, control, comunicaciones, computación e inteligencia (C4I)[2] son fundamentales para las operaciones militares modernas. Al infiltrarse en estos sistemas, los atacantes pueden causar disrupciones significativas, como la interrupción de las comunicaciones, la pérdida de datos críticos o el control remoto de sistemas de armas. (Marowski, 2018, pág. 122)

Un ejemplo notable es el ataque Stuxnet, que utilizó un malware altamente sofisticado para sabotear las centrifugadoras de enriquecimiento de uranio en Irán, en este ataque se utilizó un pendrive[3], la cual contenía un malware[4], este al ser instalado en el sistema produjo una lectura errónea de las revoluciones de las turbinas que enfriaban el agua del reactor, lo que generó un sobrecalentamiento y su inutilización. (Silva, 2018, pág. 304)

[2] Por sus siglas en Inglés *Command, Control, Communications, Cumputers* e *Intelligence,* El término **C4I** abarca las tecnologías y estrategias que ayudan a coordinar, comunicar, y controlar las fuerzas militares, integrando datos de inteligencia para apoyar la toma de decisiones en tiempo real. Es un componente clave en las operaciones militares modernas, permitiendo una comunicación y análisis efectivo en el campo de batalla y mejorando la eficiencia y efectividad de las misiones (Marowski, 2018)

[3] Memoria Extraíble

[4] Software de índole malicioso, como un virus, gusano, caballo de troya, etc.

Lo más interesante de este caso es la sofisticada combinación de ingeniería social y ciberataque. Para llevar a cabo la infección inicial, los atacantes explotaron una vulnerabilidad humana fundamental, la curiosidad. Mediante la IS, lograron obtener información crucial sobre el software utilizado en el sistema de control de las turbinas. Posteriormente, un dispositivo de almacenamiento infectado (un pendrive) fue estratégicamente dejado en un lugar accesible para los operadores de la planta, con la esperanza de que alguien lo conectara a un equipo de control. Al hacerlo, el malware contenido en el dispositivo se propagó por el sistema, manipulando las lecturas de las turbinas y provocando su sobrecalentamiento. Este ejemplo ilustra cómo la IS puede servir como la puerta de entrada para ciberataques altamente destructivos, donde la explotación de la confianza y la curiosidad humanas se convierte en un elemento fundamental del ataque.

La IS también se utiliza para difundir desinformación y propaganda entre las fuerzas armadas y la población civil. Los atacantes pueden crear cuentas falsas en redes sociales, difundir noticias falsas o manipular la opinión pública para sembrar la discordia y socavar la moral. Este tipo de ataques pueden tener un impacto psicológico significativo en las tropas y afectar su cohesión, logrando el objetivo que es afectar al factor humano en las operaciones, disminuyendo el apoyo a las operaciones por parte de la población y con esto afectando la voluntad política. Uno de estos casos se vivió en la operación Tormenta del Desierto, donde el Ejército Estadounidense logra interceptar las comunicaciones de los comandantes del Ejército Iraquí, enviando mensajes que los desconcertaban y evidenciaban la mala seguridad de sus sistemas, haciendo decaer la moral en las tropas que podían escuchar como los soldados norteamericanos hablaban en sus frecuencias y detectaban sus movimientos (Mitnick & Simon, 2006, pág. 338).

Estrategias de mitigación

La IS cuando es utilizada como parte de un ciberataque o ataque físico, representa una amenaza constante y evolutiva para las organizaciones militares. Para hacer frente a esta amenaza, es necesario implementar una serie de medidas de seguridad que abarquen tanto el aspecto humano como el tecnológico. A continuación, se detallan tres estrategias de mitigación clave: capacitación y formación, uso de tecnologías y elaboración de políticas.

Como señala el NIST (National Institute of Standards and Technology)[5] en su publicación 800-171, la capacitación debe ser continua y adaptada a las nuevas amenazas emergentes (NIST, 2021), es por esto por lo que la **capacitación y formación del personal,** son elementos fundamentales para fortalecer la resistencia ante los ataques de ingeniería social. Un programa de capacitación efectivo debe incluir la concientización sobre las tácticas de ingeniería social, derivado de esto, es necesario que todo el personal que se emplea en los organismos de la defensa sea consciente de las técnicas más comunes utilizadas por los atacantes, esto implica la realización de academias (charlas, exposiciones, etc.) que permitan conocer las tácticas y técnicas más utilizadas por los atacantes que emplean la IS para llevar a cabo sus objetivos.

Otra forma de implementar medidas que cooperen en la mitigación de ataques de IS son las simulaciones y ejercicios prácticos, estos permiten al personal poner en práctica los conocimientos adquiridos y desarrollar habilidades para identificar y responder a situaciones de riesgo, lo anterior sumado a pruebas de penetración, ayudan a identificar las vulnerabilidades humanas y técnicas de una organización, permitiendo así tomar medidas correctivas.

Si bien es imposible eliminar por completo las vulnerabilidades humanas, existen medidas que pueden ayudar a reducir el riesgo de ser víctimas de ataques de ingeniería social, este es el caso de la verificación de la información, la cual consiste en verificar la autenticidad de la fuente antes de hacer clic en un enlace, descargar un archivo o proporcionar información confidencial. Otra forma de mitigación de las vulnerabilidades humanas es la desconfianza saludable, donde lo importante es ser escépticos ante cualquier solicitud que parezca sospechosa. Todas estas medidas solo pueden implementarse con una adecuada capacitación y formación del personal que maneja o tiene acceso a información que pueda ser explotada por un atacante mediante el empleo de IS.

Para garantizar la seguridad de una organización es fundamental comprender cómo la seguridad tecnológica interactúa con otras estrategias de seguridad (Avigilon, 2024). En este sentido, las tecnologías de la información desempeñan un papel crucial en la mitigación de los riesgos asociados con la ingeniería social. Una de las medidas más comunes es el empleo de filtros de correo electrónico, capaces de identificar y bloquear correos electrónicos sospechosos antes de que lleguen a las bandejas de entrada de los usuarios. Asimismo, los sistemas de detección de

[5] El Instituto Nacional de Estándares y Tecnología (NIST) fue fundado en 1901 y ahora forma parte del Departamento de Comercio de Estados Unidos. NIST es uno de los laboratorios de ciencias físicas más antiguos del país.

intrusiones juegan un papel fundamental al monitorear continuamente las redes en busca de actividades anómalas. Finalmente, la autenticación multifactorial añade una capa adicional de seguridad, exigiendo a los usuarios que presenten múltiples credenciales para acceder a los sistemas. Al combinar estas tecnologías, las organizaciones pueden crear una defensa en profundidad que dificulta significativamente el éxito de los ataques de ingeniería social.

No obstante, como acertadamente señala Kevin Mitnick y Simon (2006), “una compañía puede gastar cientos de miles de euros en firewalls, sistemas de cifrado y demás tecnologías de seguridad, pero si un atacante engaña a un empleado, todo ese dinero no habrá servido para nada”. Esta afirmación, aunque pueda parecer contradictoria a la luz de lo expuesto anteriormente, resalta un hecho innegable, el ser humano sigue siendo el eslabón más débil en cualquier cadena de seguridad. Por ello, resulta fundamental complementar las medidas tecnológicas con una sólida estrategia de concientización y formación de los empleados. La elaboración, implementación y seguimiento de políticas de seguridad sólidas constituye el pilar fundamental de cualquier programa de ciberseguridad, ya que proporciona un marco de referencia claro y conciso para guiar las acciones de todos los miembros de la organización.

A juicio de este autor, para que una política de seguridad sea efectiva, debe contar con al menos cuatro factores interrelacionados que la conviertan en un ciclo virtuoso. En primer lugar, es necesario definir claramente los roles y responsabilidades de cada miembro del personal en materia de seguridad. Posteriormente, se deben establecer procedimientos detallados para la gestión de incidentes, la respuesta a emergencias y la recuperación ante desastres. Estos procedimientos deben ser claros, concisos y fácilmente accesibles. En tercer lugar, es fundamental promover una cultura de seguridad en toda la organización. Esta cultura debe arraigarse en todos los niveles, desde la alta dirección hasta los empleados de primera línea. Finalmente, las políticas de seguridad deben ser revisadas y actualizadas periódicamente para adaptarse a los cambios constantes en el entorno de amenazas cibernéticas.

FIGURA N° 1

Ciclo Política de Seguridad

Nota: Elaboración propia.

Conclusión

El análisis de la ingeniería social (IS) y sus implicancias en las operaciones militares desde la perspectiva de la ciberseguridad, revela una amenaza multifacética y persistente que se centra en el eslabón más débil de la seguridad, el factor humano. La IS explota las vulnerabilidades psicológicas inherentes al ser humano, como la confianza, la reciprocidad y el miedo, utilizando técnicas sofisticadas como el *phishing*, el *tailgating* y el *pretexting* para obtener acceso a información confidencial o sistemas restringidos. A diferencia de los ataques que explotan vulnerabilidades técnicas, la IS se focaliza en manipular el comportamiento humano, lo que la convierte en una de las amenazas más difíciles de contrarrestar dentro del ciberespacio militar.

Uno de los aspectos más preocupantes es que los ataques de que emplean IS no solo buscan la obtención de información, sino que también pueden tener un impacto devastador en las operaciones militares. La pérdida de información clasificada, la disrupción de sistemas de mando y control, y la propagación de desinformación y propaganda son algunos de los efectos que pueden comprometer gravemente la capacidad operativa y la seguridad de una nación. Ejemplos como el ataque Stuxnet o los ciberataques en el conflicto entre Georgia y Rusia demuestran cómo la IS

puede ser empleada para sabotear infraestructuras críticas y desestabilizar a las fuerzas armadas a través de la manipulación del factor humano.

Ante esta realidad, la mitigación de los riesgos asociados a la IS en el contexto militar requiere un enfoque integral que abarque tanto la capacitación y concientización del personal como el desarrollo e implementación de tecnologías de seguridad robustas y la elaboración de políticas de seguridad rigurosas. La capacitación continua del personal es crucial para que los individuos sean conscientes de las tácticas utilizadas por los atacantes y puedan reconocer y resistir intentos de manipulación. Las simulaciones y ejercicios prácticos también juegan un papel esencial en el fortalecimiento de la resiliencia ante ataques de IS, permitiendo al personal experimentar escenarios de riesgo en un entorno controlado y desarrollar habilidades de respuesta efectiva.

Desde un punto de vista tecnológico, el uso de herramientas como filtros de correo electrónico avanzados, sistemas de detección de intrusiones y autenticación multifactorial son medidas esenciales para reducir la exposición a ataques de IS. Estas tecnologías actúan como barreras adicionales que dificultan la ejecución de tácticas de IS y protegen la información sensible al exigir múltiples capas de verificación y monitoreo constante de actividades sospechosas.

Finalmente, las políticas de seguridad deben ser claras, exhaustivas y dinámicas, adaptándose continuamente a las nuevas amenazas emergentes. Estas políticas no solo deben establecer protocolos de acción en caso de un ataque, sino también fomentar una cultura de seguridad en toda la organización, donde la ciberseguridad sea vista como una responsabilidad compartida por todos los miembros de las fuerzas armadas.

En conclusión, los ataques que emplean la ingeniería social representan una amenaza significativa para las operaciones militares, pero con un enfoque multidimensional que combine la capacitación, la tecnología y las políticas adecuadas, es posible fortalecer la ciberseguridad y proteger la integridad y disponibilidad de los sistemas y datos militares. La naturaleza evolutiva de las amenazas cibernéticas exige una constante adaptación y mejora de las estrategias de defensa, asegurando que las fuerzas armadas estén preparadas para enfrentar los desafíos del ciberespacio en un entorno cada vez más complejo y hostil.

Referencias

Avigilon. (2024). *Guía Tecnológica de Seguridad: Tendencias del sector para el 2024.* Obtenido de Tendencias en tecnologías de seguridad: https://www.avigilon.com/es/blog/security-technology

Deutsch, V. (2022). *Ciberseguridad Para Directivos*. España: Almuzara.

Díaz del Río, J. J. (2011). *La Ciberseguridad en el Ámbito Militar*. Cuadernos de Estrategia N°149, 215.256.

Díaz, H. (2018). *Infraestructura Crítica Vulnerable a la Ciberguerra*. La Ciberguerra, Sus Impactos y Desafíos, 45-58.

Equipo CEEAG. (2018). *Desafíos Para Afrontar la Ciberguerra*. La Ciberguerra, Sus Impactos y Desafíos, 147-164.

Hadnagy, C. (2011). *Ingeniería Social: El Arte Del Hacking Personal*. Madrid: ANAYA.

Hadnagy, C. (2023). *Ingeniería Social, La Ciencia de la Piratería Humana*. Madrid: ANAYA.

Marowski, C. (2018). *Efectos de los Riesgos y Amenazas de la Ciberguerra en la Infraestructura Crítica*. La Ciberguerra, Sus Impactos y Desafíos, 107-128.

Mauricio, F. (2023). *Cyberceo, Una Visión Estratégica de la Ciberseguridad*. España: Marcombo.

Mitnick, K., & Simon, W. (2006). *El Arte de la Intrusión, La Verdadera Historia de las Hazañas de Hackers, Intrusos e Impostores*. Madrid: RA-MA.

Mitnick, K., & Simon, W. (2013). *Un Fantasma en el Sistema.* Madrid: Capitán Swing Libros.

Mitnick, K., & Vamosi, R. (2023). *El Arte de la Invisibilidad*. Madrid: ANAYA.

Ramos, A., Barbero, C., Marugan, D., & González, I. (2015). *Conoce Todo Sobre Hacking con Ingeniería Social: Técnicas para Hackear Humanos*. Madrid: RA-MA.

Ross, R., & Pillitteri, V. (2024). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. USA: NIST.

Silva, F. (2018). Stuxnet - *El Software como Herramienta de Control Geopolítico*. Revista PUCE (106), 297-314.