MEDICIÓN DE LA CULTURA DE CIBERSEGURIDAD MEDIANTE SIMULACIONES CONTROLADAS DE ATAQUES CON MALWARE

MEASURING CYBERSECURITY CULTURE THROUGH CONTROLLED MALWARE ATTACK SIMULATIONS

Alex Ricardo Álvarez Paredes[1*]

[1] Fuerza Aérea Ecuatoriana. Licenciado en Administración Aeronáutica Militar. Master en Ciberseguridad. ORCID: https://orcid.org/0009-0003-2311-5441. Correo: zahid1102@hotmail.com

Christian Daniel Cortez Viteri[2]

[2] Docente Instituto Superior Tecnológico Tungurahua. Ing. En Administración de Empresas. Magister en Administración de Empresas. ORCID: https://orcid.org/0000-0002-7338-5074 Correo: ccortez.istt@gmail.com

Pedro Renato Araujo Fierro[3]

[3] Fuerza Aérea Ecuatoriana. Licenciado en Administración Aeronáutica Militar, Máster en Gerencia y Liderazgo Educacional, Máster en Gerencia de Seguridad de Riegos, Master en relaciones internacionales y diplomacia mención en movilidad humana. ORCID: https://orcid.org/0009-0000-7196-7516. Correo: goriluec@yahoo.com

Cristian Fabricio Moreno Proaño[4]

[4] Fuerza Aérea Ecuatoriana, Licenciado en Administración Aeronáutica Militar. Master en desarrollo del talento humano, Master en dirección de personas y del talento humano. ORCID: https://orcid.org/0009-0001-7463-5338. Correo: cristianfmorenop@gmail.com

*** Autor para correspondencia:** ccortez.istt@gmail.com

Resumen

La Fuerza Aérea Ecuatoriana (FAE) enfrenta crecientes amenazas cibernéticas que ponen en riesgo la seguridad nacional, la integridad de sus operaciones y la confidencialidad de su información, con el avance de las tecnologías de la información y comunicaciones (TIC), el ciberespacio se ha convertido en un nuevo teatro de guerra donde las ciberamenazas pueden afectar el funcionamiento de la institución, en este contexto, la FAE creó una unidad de Ciberdefensa con el objetivo de proteger su infraestructura digital, gestionando

incidentes de seguridad de manera proactiva y reactiva, este estudio tiene como objetivo medir el nivel de cultura de ciberseguridad en la FAE, utilizando una metodología experimental para evaluar la respuesta del personal ante ciberataques controlados mediante malware embebido en una aplicación que firma documentos digitalmente. La investigación se basa en un enfoque cuantitativo, con encuestas y análisis de datos estadísticos obtenidos de las pruebas experimentales, los resultados permitirán identificar patrones de conocimiento y comportamientos del personal frente a amenazas cibernéticas, proporcionando información valiosa para fortalecer la ciberseguridad en la Fuerza Aérea Ecuatoriana y orientar futuras intervenciones en este ámbito.

Palabras clave: ciberseguridad; malware; fuerza aérea ecuatoriana; ciberdefensa

Abstract

The Ecuadorian Air Force (FAE) faces growing cyber threats that jeopardize national security, the integrity of its operations, and the confidentiality of its information. With the advancement of information and communication technologies (TIC), cyberspace has become a new battlefield where cyber threats can affect the institution's functioning. In this context, the FAE created a Cyber Defense unit with the objective of protecting its digital infrastructure by managing security incidents both proactively and reactively. This study aims to measure the level of cybersecurity culture within the FAE, using an experimental methodology to assess the personnel's response to controlled cyberattacks through malware embedded in an application that digitally signs documents. The research is based on a quantitative approach, using surveys and statistical data analysis obtained from the experimental tests. The results will help identify patterns of knowledge and behavior in the personnel regarding cyber threats, providing valuable information to strengthen cybersecurity in the Ecuadorian Air Force and guide future interventions in this field.

Keywords: *cybersecurity; malware; ecuadorian air force; cyber defense*

Fecha de recibido: 12/02/2025
Fecha de aceptado: 22/04/2025
Fecha de publicado: 30/04/2025

Introducción

La creciente importancia de la ciberseguridad en un mundo cada vez más digitalizado ha llevado a numerosas investigaciones y estudios sobre la protección de infraestructuras críticas frente a ciberamenazas. En particular, las organizaciones gubernamentales y las fuerzas armadas, como la Fuerza Aérea Ecuatoriana (FAE), se enfrentan a la necesidad urgente de fortalecer su cultura de ciberseguridad para hacer frente a las amenazas cada vez más sofisticadas, como los ataques de malware, el phishing y otras técnicas de ingeniería social.

El planteamiento del problema se basa en la necesidad de determinar el nivel de conciencia y preparación en ciberseguridad de los miembros de la FAE. Las investigaciones previas (Ganuza, 2020; Denning, 2012) sugieren que el factor humano sigue siendo el eslabón más débil en la cadena de defensa cibernética, pues la mayoría de los ataques exitosos se deben a errores humanos, como el clic en un enlace malicioso o la ejecución de un archivo infectado. Sin embargo, aún persiste una falta de estudios que midan el impacto de ataques controlados de malware sobre las instituciones de seguridad nacional, particularmente en el contexto ecuatoriano.

Las interrogantes clave que motivan esta investigación son: ¿Cuál es el nivel de cultura de ciberseguridad en la Fuerza Aérea Ecuatoriana? ¿Cómo reaccionan los miembros de la institución ante ataques simulados mediante malware? ¿Qué acciones de mitigación deben implementarse para mejorar este nivel? Estas preguntas orientaron el trabajo, que busca medir la respuesta del personal militar y administrativo ante un ataque controlado de malware y evaluar los resultados obtenidos a partir de una encuesta de sensibilización en ciberseguridad.

El objetivo de este estudio es evaluar el nivel de cultura de ciberseguridad en la Fuerza Aérea Ecuatoriana mediante la aplicación de ciberataques controlados con malware, a fin de generar métricas que reflejen la eficacia de la formación en ciberseguridad. El enfoque adoptado es experimental y se centra en la simulación de ataques a través de phishing, con el objetivo de evaluar las respuestas de los usuarios ante la amenaza cibernética.

La ciberseguridad y la ciberdefensa son campos multidisciplinarios que buscan proteger la información y las infraestructuras de las organizaciones frente a ciberamenazas. Diversos estudios (Granados, 2018; Pollit, 1998) han abordado la relevancia de la ciberdefensa en el ámbito militar, señalando que la seguridad de las infraestructuras críticas depende no solo de las herramientas tecnológicas, sino también de la cultura de ciberseguridad adoptada por los usuarios. El concepto de "ciberarmas", como el malware, ha sido fundamental en el desarrollo de ciberataques, que se valen de técnicas como el phishing para engañar a los usuarios y comprometer los sistemas de la organización (Joint, 2016).

Se revisan estudios previos en el campo de la ciberdefensa y la ciberseguridad en contextos militares, destacando los avances de otros autores que han trabajado en la implementación de medidas de protección a infraestructuras críticas y en la evaluación de la cultura de ciberseguridad mediante pruebas controladas. El presente trabajo justifica su necesidad, dado el creciente número de ciberataques en América Latina y la falta de investigaciones específicas que aborden la situación en la Fuerza Aérea Ecuatoriana.

Los resultados obtenidos a partir de los ciberataques simulados y las encuestas fueron analizados mediante técnicas estadísticas para determinar el nivel de conciencia en ciberseguridad dentro de la institución. Se compararon las respuestas correctas de la encuesta con los datos de interacción obtenidos durante los ataques, identificando patrones de comportamiento que reflejan el grado de preparación de los usuarios ante amenazas cibernéticas.

Materiales y métodos

La investigación se basa en un enfoque cuantitativo, utilizando herramientas como encuestas y análisis de datos estadísticos para evaluar el nivel de cultura de ciberseguridad en la Fuerza Aérea Ecuatoriana, a través de estas herramientas, se recopilan datos de las pruebas experimentales realizadas con malware embebido, lo que permite medir la capacidad de respuesta del personal ante amenazas cibernéticas, el estudio tiene un carácter exploratorio, ya que su objetivo principal es identificar patrones y entender el estado actual de la cultura de ciberseguridad dentro de la institución, esta metodología facilita la recolección de información detallada, que puede orientar en el diseño de futuras estrategias y medidas de ciberseguridad, como parte de la técnica empleada, se realizan encuestas para evaluar el nivel de conocimiento del personal en este ámbito, complementadas con pruebas experimentales que simulan ataques cibernéticos para medir la efectividad de las respuestas frente a dichos incidentes. Este enfoque integral contribuye a obtener una visión clara del panorama actual y permite comparar los resultados obtenidos con los objetivos de la investigación.

Desarrollo del Malware se utiliza Kali Linux como plataforma para el desarrollo del malware, específicamente un servidor cliente-servidor que facilita la creación de puertas traseras en los dispositivos infectados. El malware se desarrolla en lenguaje C utilizando la librería socket.h, que permite la creación de conexiones TCP (Sockets) para la interacción entre el servidor y las víctimas. (Luz, 2022).

Simulación de los ataques, los ataques controlados se llevan a cabo mediante técnicas de ingeniería social, como el phishing, que tiene como objetivo engañar a los usuarios para que ejecuten el archivo infectado. El malware se encuentra encapsulado en el archivo "FIRMAEC", con la finalidad de evitar su detección por software antivirus. Para esto, se emplean técnicas de ofuscación y ocultación de código (Ranchal, 2018; Microsoft, 2012). Las técnicas de phishing y su efectividad en la propagación de malware han sido documentadas por varios autores, como Ganuza (2010), quien argumenta que los ciberdelincuentes explotan las vulnerabilidades humanas para llevar a cabo ataques exitosos.

Pruebas y medición, se realizaron pruebas utilizando un servidor en la nube con una base de datos que almacena información sobre las interacciones de las víctimas. Estas métricas se analizan a través de la recopilación de datos como fecha, hora y nombre del usuario, lo que permite generar indicadores clave de rendimiento (KPI) sobre el nivel de cultura de ciberseguridad dentro de la institución (Fortinet, 2022). La implementación de este tipo de sistemas para la medición del impacto de los ataques es fundamental para evaluar las capacidades de defensa ante ciberamenazas (León, 2021).

Para complementar los resultados obtenidos mediante los ataques simulados, se realizó una encuesta a 300 empleados de la FAE para medir su nivel de conocimiento sobre ciberseguridad. Los resultados de la encuesta son comparados con el impacto de los ataques controlados para evaluar la efectividad de la formación en ciberseguridad (Klimburg, 2017). Según Denning (2012), la educación y la sensibilización del personal son fundamentales para prevenir infecciones de malware, ya que la mayoría de los incidentes ocurren debido a errores humanos.

La elección de Kali Linux como plataforma y el uso de técnicas como el phishing se justifican por su relevancia en el ámbito de ciberseguridad y su capacidad para simular de manera realista los ataques que podrían ocurrir en un entorno operativo real (Ganuza, 2020). El empleo de la herramienta FIRMAEC y su combinación con el malware permite simular un ataque real sin causar daño a los sistemas. Las encuestas

complementan los resultados de las pruebas, ofreciendo una visión integral sobre el nivel de cultura de ciberseguridad de los participantes (Pollit, 1998).

Resultados y discusión

Tabla 1. Que contienen los típicos intentos de Phishing

Opción	Respuesta	Frecuencia
a	Si uso un programa antivirus estaré protegido contra los intentos de Phishing	3
b	Normalmente piden información personal como nombres de usuario, contraseñas y números de la tarjeta de crédito	295
c	Normalmente el remitente pide que se le responda en un plazo de días	2
d	Todo lo anterior	0

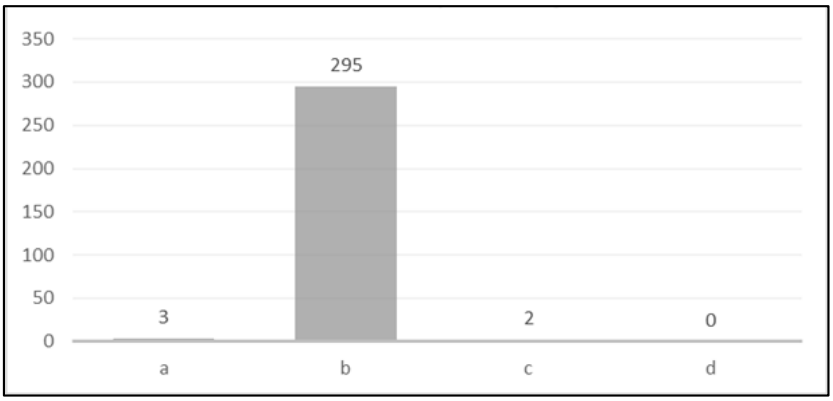

Figura 1. Que contienen los típicos intentos de Phishing

Análisis: la mayoría de las personas pueden reconocer un ataque de phishing, como lo demuestra la alta proporción de respuestas que indicaron que estos ataques suelen solicitar información personal como nombres de usuario, contraseñas y números de tarjetas de crédito, esto muestra que los encuestados tienen una comprensión adecuada de los métodos más comunes empleados en estos ataques, los cuales buscan recopilar datos sensibles, además, el hecho de que pocos hayan optado por respuestas que indican que los antivirus son suficientes para prevenir phishing sugiere que los participantes son conscientes de que este tipo de ataques va más allá de las medidas de seguridad tradicionales. Sin embargo, el bajo porcentaje de respuestas relacionadas con tácticas como la urgencia temporal en los correos de phishing revela que no todos los usuarios están

familiarizados con estos métodos específicos, la mayoría tiene noción de los riesgos del phishing, aún existen áreas de mejora en la conciencia sobre otras técnicas utilizadas en estos fraudes.

Tabla 2. Cuál de las siguientes amenazas es la más peligrosa para la información de su empresa

Opción	Descripción	Respuestas
a	Los competidores, porque la competencia es muy fuerte en este mercado	39
b	Los empleados, porque podrían filtrar información intencionada o no intencionadamente	217
c	Ninguna	26
d	No lo sé	18

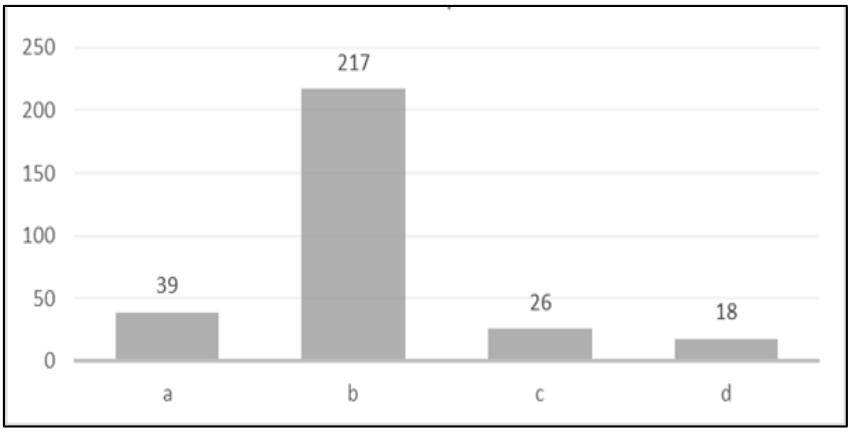

Figura 2. Amenazas es la más peligrosa para la información de su empresa

Análisis: los resultados reflejan una clara preocupación sobre los factores internos y externos que pueden afectar la seguridad y la competitividad en el mercado, de las respuestas obtenidas, 39 personas mencionan que la competencia es muy fuerte, lo que implica que los competidores pueden representar una amenaza significativa para la empresa, ya sea a través de estrategias agresivas o el robo de información clave, por otro lado, 217 personas señalan a los empleados como el principal riesgo, ya sea por filtración de información de manera intencionada o no, lo que sugiere una alta conciencia sobre los peligros internos, como la falta de control sobre el acceso a datos sensibles, esta respuesta es acertada, ya que los empleados tienen acceso privilegiado a información clave y, en ocasiones, pueden verse tentados o involucrados en la filtración de

datos, la opción "Ninguna" fue seleccionada por 26 personas, lo que podría reflejar una falta de conciencia sobre los riesgos o una percepción de que estos factores no aplican a su contexto, finalmente, 18 personas indicaron no tener conocimiento sobre el tema, lo que resalta la necesidad de mejorar la capacitación y sensibilización respecto a la seguridad en el entorno laboral, aunque hay una clara preocupación por la competencia y los empleados, se evidencia que la falta de conocimiento y la subestimación de ciertos riesgos internos podrían comprometer la seguridad y el bienestar de la organización.

Tabla 3. Quién conoce la contraseña que se utiliza para acceder a los datos de su empresa

Opción	Descripción	Respuestas
a	Sólo usted	271
b	Sólo unos cuantos colegas	0
c	Sólo un administrador del sistema	29
d	Miembros de la familia	0

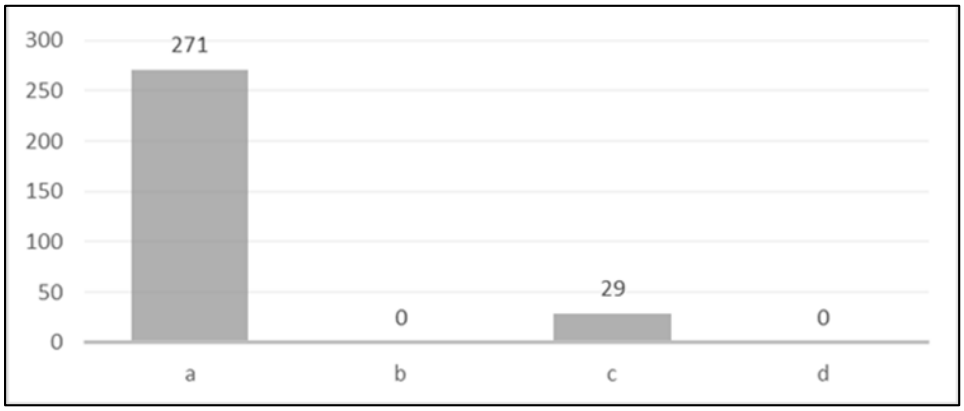

Figura 3. Quién conoce la contraseña que se utiliza para acceder a los datos de su empresa

Análisis: Se observa que 271 personas indican que solo el propietario del equipo conoce la contraseña de acceso a los datos de la empresa, lo que refleja una alta reserva de las credenciales. Por otro lado, 29 personas mencionan que tanto el propietario como un administrador del sistema tienen acceso a la contraseña, lo que indica un modelo de seguridad compartido en situaciones específicas. Las opciones restantes no recibieron respuestas, lo que sugiere que la política de control de acceso es estricta y centralizada. En general, los resultados evidencian que la empresa mantiene un enfoque prudente y seguro sobre el manejo de credenciales, limitando su conocimiento solo a las personas clave, lo que reduce los riesgos de vulnerabilidad.

Tabla 4 . Utiliza su dirección electrónica privada en su actividad profesional

Opción	Descripción	Respuestas
a	Nunca	9
b	A veces	145
c	Con frecuencia	83
d	Todos los días	63

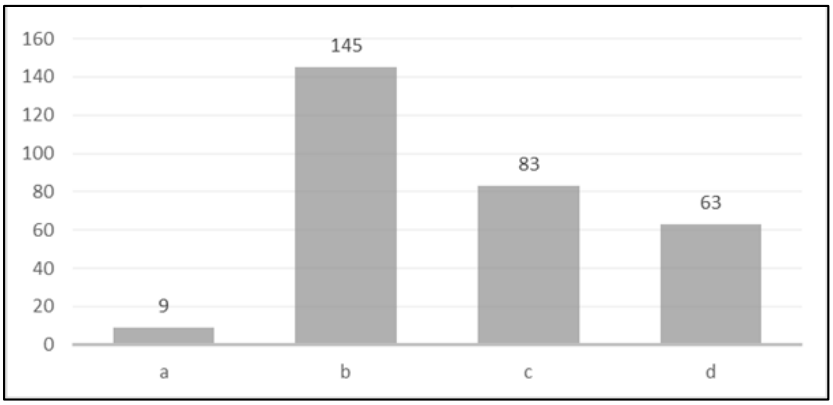

Figura 4. Utiliza su dirección electrónica privada en su actividad profesional

Análisis: se observa que un total de 9 personas afirman que "nunca" utilizan su correo personal para actividades institucionales, lo que podría indicar una estricta separación entre sus asuntos personales y laborales, por otro lado, 145 personas indican que "a veces" usan su correo personal en actividades relacionadas con la institución, lo que sugiere una tendencia a utilizarlo ocasionalmente, posiblemente en situaciones informales o cuando el correo institucional no está disponible, un total de 83 personas manifiestan que "con frecuencia" emplean su correo personal, lo que podría reflejar una mayor dependencia de este medio en sus labores cotidianas, finalmente, 63 personas informan que "todos los días" usan su correo personal para actividades de la institución, lo que plantea preocupaciones sobre la posible falta de una infraestructura de comunicación institucional adecuada o la preferencia por la comodidad del correo personal, este patrón resalta la necesidad de revisar las políticas de comunicación institucional para garantizar la seguridad y eficiencia en el manejo de la información.

Conclusiones

La realización de la presente investigación determina los componentes fundamentales de la ciberguerra, así como el alcance de las operaciones ciberespaciales y las ciberarmas utilizadas para llevar a cabo ciberataques. Se ha identificado que el factor humano es el eslabón más vulnerable en materia de ciberseguridad, dado que el desconocimiento, la excesiva confianza, la ignorancia o incluso la actuación deliberada permiten la

infiltración de malware en la infraestructura crítica de la institución, esta situación pone de manifiesto que la institución está expuesta a diversos tipos de ciberataques debido a la falta o ausencia de una cultura sólida en ciberseguridad. Así, se destaca la urgente necesidad de fortalecer la formación y conciencia en ciberseguridad entre los empleados, para prevenir riesgos y proteger los activos digitales de la organización frente a posibles amenazas.

La implementación de soluciones informáticas para detectar y neutralizar ciberamenazas en los sistemas y/o dispositivos debe ir más allá de la tecnología, acompañándose de un proceso continuo de capacitación, concientización y sensibilización de las personas. Es fundamental que todos los empleados mantengan buenas prácticas de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información. El desconocimiento, el exceso de confianza, la ignorancia o incluso la actuación deliberada pueden poner en riesgo la infraestructura crítica de la institución. Por lo tanto, una cultura de ciberseguridad sólida, que involucre tantas herramientas tecnológicas como un cambio en la mentalidad de los colaboradores, es esencial para proteger adecuadamente los recursos y activos digitales frente a las crecientes amenazas cibernéticas.

Referencias

Denning, D. (2012). activism, hacktivism, and cyberterrorism: the internet as a tool for influencing foreign policy. Networks and Netwars: The Future of Terror, Crime, and Militancy, 239-280.

Fortinet. (1 de Septiembre de 2022). Fortinet: Latinoamérica sufre 137 mil millones de ciberataques en 2022. Obtenido de Fortinet: Latinoamérica sufre 137 mil millones de ciberataques en 2022: https://thestandardcio.com/2022/09/01/fortinet-latinoamerica-sufre-137-mil-millones-de-ciberataques-en-2022/

Ganuza Artiles, N. (2010). Ciberseguridad, retos y amenazas a la seguridad en el ciberespacio. Madrid: Instituto Español de Estudios Estratégicos.

Ganuza, N. (2020). Guía de Ciberdefensa. Canadá: Junta Interamericana de Defensa.

Joint, P. 1.-0. (2016). Department of Defense Dictionary of Military and Associated Terms. Estado Unidos: Joint Publication.

Klimburg, A. (23 de Noviembre de 2017). The-darkening-web-the-war-for-cyberspace. Obtenido de https://ikindlebooks.com/best-sellers/the-darkening-web-the-war-for-cyberspace

León, Á. D. (18 de Junio de 2021). blog.infranetworking.com. Obtenido de https://blog.infranetworking.com/que-es-apache-servidor/

Luz, S. D. (16 de Octubre de 2022). Redeszone.net. Obtenido de https://www.redeszone.net/tutoriales/configuracion-puertos/que-es-socket-tcp-udp-diferencias-puertos/

Microsoft. (2012). Microsoft_Security_Intelligence_Report_Special_Edition. Obtenido de Microsoft_Security_Intelligence_Report_Special_Edition: https://www.microsoft.com/en-us/download/details.aspx?id=29046

Pollit, M. (1998). Cyberterrorism — fact or fancy? Computer Fraud and Security, 8-10.

Ranchal, J. (25 de Octubre de 2018). https://www.muycomputer.com/. Obtenido de https://www.muycomputer.com/2018/10/25/consola-de-windows-guia/redhat. (8 de Mayo de 2020). redhat.com. Obtenido de https://www.redhat.com/es/topics/api/what-is-a-rest-api