MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
EJÉRCITO NACIONAL
CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA DE EDUCACIÓN

INFORME DE GESTIÓN No. 008

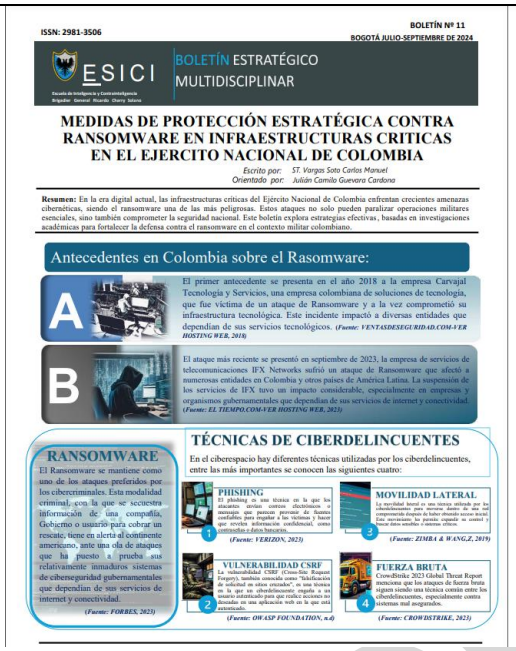
Bogotá, Septiembre 2024

1. No. DEL CONTRATO	CONTRATO No. 206
2. FECHA SUSCRIPCIÓN CONTRATO	1 de febrero 2024
3. POLIZA DE SEGUROS	No. De póliza: 14-46-101107444 Aseguradora: Seguros del Estado S.A. Fecha oficio aprobación: 19 de enero de 2024 Aprobado por: TC. ANDRÉS AUGUSTO POLANCO VALENCIA Ordenador del Gasto- CENAC-EDUCACIÓN
4. CRP	No. 7024 Fecha expedición: 6 de febrero de 2024 Unidad/Sub-unidad ejecutora: 15-01-03-088 CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA DE EDUCACIÓN Dependencia: 088 - CENTRAL ADMINISTRATIVA Y CONTABLE ESPECIALIZADA EDUCACIÓN Posición catálogo de gasto: A-02-02-02-009-002 SERVICIÓS DE EDUCACIÓN Fuente: Nación 10 Recurso: 10 Valor total: $38.000.000
5. FECHA INICIO EJECUCIÓN CONTRACTUAL	6 de febrero 2024
6. CONTRATISTA	Nombre completo: JULIAN CAMILO GUEVARA CARDONA Identificación: No. 1002397365, expedida en BOGOTA Nacionalidad: colombiana Dirección-ciudad de residencia: **CRA 74 #160-83** Teléfono de contacto: **3008873305** E-mail de contacto: julian.guevara@esici.edu.co
7. SUPERVISOR	Nombre completo: C.T SARA LIA BARRERO MORENO Cargo: OFICIAL DECTID Resolución de Nombramiento: No. 207 del 1/29/2024
8. OBJETO CONTRACTUAL	PRESTACIÓN DE SERVICIOS COMO ASESOR EN LOS PROCESOS DE INVESTIGACION DE LA ESCUELA DE INTELIGENCIA Y CONTRAINTELIGENCIA
9. OBLIGACIONES CONTRACTUALES	1. Cumplir a cabalidad el cronograma de investigación propuesto por el Departamento de Ciencia Tecnología Investigación y Doctrina “DECTID” en la vigencia 2024. 2. Elaborar dos capítulos del libro en coordinación con las demás escuelas del Ejército de acuerdo con las directrices que le sean emitidas por parte del DECTID. 3. Elaborar, dos artículos “Tipo B” relacionado con la línea de investigación "ESTADO SEGURIDAD Y DEFENSA MULTIDIMENSIONAL”, y/o cualquier otro tema afín que sea indicado por el DECTID, entregándolos con la sesión de derechos al DECTID. En total dos (2) durante la vigencia del contrato. 4. Mantener actualizado el CvLAC personal, alimentando la base de datos con los distintos productos obtenidos durante la vigencia del contrato, aportando al DECTID los soportes mediante correo electrónico institucional de extensión “esici.edu.co”, que será asignado al contratista durante la vigencia del contrato por parte de la sección de telemática de la ESICI, todos los 25 del mes, relacionando eventos, publicaciones u otras actividades científicas, además de los certificados o publicaciones en formato pdf a fin de mantener actualizada la base de datos.

CENACEDU

	5. Gestionar, la publicación de dos (2) artículos escritos por personal externo para la revista “Perspectivas en Inteligencia”. 6. Participar como ponente, en mínimo 02 ponencias, en eventos académicos con entes externos. 7. Organizar, participar e invitar representaciones de la comunidad educativa nacional a los encuentros de semilleros, foros, ponencias según requerimiento del DECTID. 8. Revisar, asesorar, formular estrategias y retroalimentar mediante un informe al DECTID los días 25 de cada mes, según el avance de los semilleros de investigación, convocados en los cursos militares, para aportar de forma significativa a los proyectos de investigación en desarrollo e innovación (i+d+i). De acuerdo con las líneas de investigación de la ESICI. 9. Aplicar y dar cumplimiento a lo estipulado en el sistema integrado del Ejército Nacional (proceso, procedimientos y formatos), soportando todas sus reuniones asesorías y capacitaciones con los formatos ordenados por Ejército. 10. Las demás funciones que sean asignadas por la autoridad competente, de acuerdo con la naturaleza y el área de desempeño del cargo. 11. Asistir a las reuniones que sea convocado. 12. Cumplir ampliamente con idoneidad el objeto del contrato. 13. Guardar absoluta reserva de la información que en desarrollo del contrato llegue a conocer. 14. Realizar informe los días 25 de cada mes sobre las actividades desarrolladas durante el lapso. 15. Realizar transferencia de conocimiento a partir de videos e instructivos de las diferentes metodologías y software utilizados durante su contrato. 16. Apoyar con la elaboración de documentos y asesorías, en las diferentes actividades institucionales relacionadas con acreditaciones, condiciones institucionales, renovaciones de los registros calificados de los pregrados y posgrados ofertados por la IES ESICI, u otras que surgieren en el transcurso del contrato. 17. Dar cumplimiento al sistema de gestión documental SICDI, garantizando con ello la seguridad de la información y la trazabilidad de los procesos, de acuerdo a lo establecido en la ley 1581 de 2012 y la ley 1621 de 2013, en tal virtud el rendimiento de informes de contrato, avances de proyectos de investigación, productos finales y demás labores encomendadas dentro de su marco de obligaciones contractuales deben presentarse de manera documental por medio de la plataforma en los tiempos pactados. 18. El contratista debe custodiar los medios entregados y a la terminación del presente contrato devolver los insumos, suministros herramientas, dotación, implementación, inventarios y/o materiales que sean eventualmente y por la necesidad del cumplimiento del objeto contractual, puestos a su disposición para la prestación del servicio objeto de este contrato, en caso de pérdida o daño le serán aplicables las disposiciones pertinentes contenidas en la ley 1476 de 2011, en concordancia con ello se entenderá que la información es material de consulta y base para desarrollo de investigación (datos, bases de datos, proyectos estudiantiles u otros), obtenidos por intermedio de la Escuela de Inteligencia y Contrainteligencia BG. Ricardo Charry Solano (ESICI), de manera directa o indirectamente deberán ser empleados para el cumplimiento de las obligaciones específicas de este contrato en la vigencia establecida, por lo tanto no podrán ser usados o empleados con posterioridad ni a nombre propio sin previa autorización escrita y explicita de la ESICI, atendiendo a la reserva de la información y a la protección de la propiedad intelectual. 19. En concordancia con la cláusula Quinta “Lugar de Ejecución del Contrato” Escuela de Inteligencia y Contrainteligencia BG. Ricardo Charry Solano (ESICI), la última semana del mes en día hábil, se deberá entregar por parte del contratista al supervisor del contrato un Backup de la información generada en desarrollo del contrato en formato Word, Power Point, Excel o como originalmente haya sido generado, de igual forma dicha información deberá tener concordación con la desarrollada y contenida en la carpeta compartida asignada para tal fin, la mensajería electrónica requerida entre contratista y ESICI deberá ser enviada mediante el correo institucional de extensión “esici.edu.co”, que será asignado al contratista durante la vigencia del contrato por parte de la sección de telemática de la ESICI. 20. Dar cumplimiento al cronograma de actividades establecido con el supervisor, en el cual hace parte integral del contrato de prestación de servicios y contendrá la medición en alcance e impacto del producto que desarrollará el objetivo estratégico de la dependencia

	en consideración a sus misiones y capacidades. Mencionado cumplimiento se debe dejar como obligación del contratista para que en caso que este sin acudir causa que lo justifique, se abstenga de entregar los informes o los documentos requeridos para el cumplimento de los requisitos legales de ejecución del contrato, dentro del plazo establecido para ello se pueda aplicar la cláusula resolutoria y disolver el contrato, finalmente se clarifica que cualquier tipo de prorroga a los tiempos pactados no se podrá genera de manera unilateral por parte del contratista. 21. En el cumplimiento al objeto contractual, se podrán establecer requerimientos para el desarrollo de productos de propiedad intelectual, que en tal caso serán de propiedad del Ejército Nacional y no podrán reclamarse como derechos de autor, por tanto, los productos de investigación y desarrollo adelantados tendrá en obligatoriedad como autor visible a la Escuela de Inteligencia y Contrainteligencia BG. Ricardo Charry Solano (ESICI). 22. El contratista cargue en secop el informe de gestión, la cuenta de cobro o factura (esta última si aplica) y la planilla 23. El contratista debe custodiar y a la terminación del presente contrato devolver los insumos, suministros, herramientas, dotación, implementación, inventarios y/o materiales que sean puestos a su disposición para la prestación del servicio objeto de este contrato. 24. Entregar al final de la prestación del servicio, back up de la información producto de la ejecución de este contrato. 25. Las demás obligaciones establecidas en el estudio previo, documento que el contratista declara conocer y que hace parte del presente contrato. 26. Las demás obligaciones que se deriven del objeto del contrato.
10. DOCUMENTOS QUE SOPORTAN EL CUMPLIMIENTO DE LAS OBLIGACIONES CONTRACTUALES	- Registro de trabajo estudiantes en Semillero de Estudios en Inteligencia y Seguridad Estatal, Semillero de Escenarios Multidimensionales para la Seguridad y Defensa y Semillero Ciberseguridad Avance de articulo de investigación. **UNESI y sus conceptos doctrinales** **Introducción:** La "Unión de Esfuerzos de Inteligencia (UNESI)" es un concepto doctrinal fundamental en la función de conducción de la guerra inteligencia dentro del Ejército Nacional de Colombia. Este concepto enfatiza la necesidad de un enfoque integrado y coordinado en las actividades de inteligencia, donde todos los elementos de la comunidad de inteligencia deben trabajar de manera cohesionada para cumplir los objetivos operacionales. La UNESI se presenta como una organización cohesionada cuya estructura, sistemas de gestión y cultura están alineados para apoyar un objetivo común, el cual es facilitar la comprensión del ambiente operacional y proporcionar al comandante la inteligencia necesaria para la toma de decisiones informadas y oportunas. El propósito principal de la UNESI en el Ejército Nacional es canalizar y sincronizar los esfuerzos de todas las unidades de inteligencia y contrainteligencia, asegurando que la recolección de información, el análisis y la producción de inteligencia se realicen de manera eficiente y efectiva. Esto incluye la integración de las unidades de inteligencia, contrainteligencia, las secciones de inteligencia en los diferentes escalones, y los especialistas en inteligencia, quienes poseen la formación adecuada para interpretar la información recolectada y generar productos de inteligencia precisos. De esta manera, la UNESI garantiza que el poder de toda la comunidad de inteligencia sea aprovechado al máximo para apoyar las operaciones militares y la seguridad nacional. Diversos autores y doctrinas militares han abordado la importancia de la integración y coordinación en las actividades de inteligencia, similar al concepto de UNESI. Por ejemplo, en la doctrina de inteligencia de los Estados Unidos, el concepto de "Joint Intelligence Operations" es fundamental para asegurar que todas las ramas de las fuerzas armadas y agencias de inteligencia trabajen en conjunto para proporcionar inteligencia precisa y oportuna a los comandantes operacionales. Este enfoque de inteligencia conjunta, al igual que la UNESI, se basa en la premisa de que la colaboración y la cohesión entre diversas unidades y agencias son esenciales para las actividades de inteligencia para lograr una ventaja operativa decisiva en el campo de batalla. **Desarrollo:** El concepto "Medición y Firma de Inteligencia (MASINT)" es un componente clave dentro del ámbito de la inteligencia militar que se enfoca en la recolección y análisis de datos derivados de señales técnicas y científicas. Este tipo de inteligencia se diferencia de otros métodos tradicionales, como la inteligencia de señales (SIGINT) o la inteligencia de imágenes (IMINT), debido a su capacidad para identificar, rastrear y describir las características distintivas de las fuentes o los eventos, utilizando técnicas avanzadas de procesamiento de datos. En Colombia, el tema de MASINT ha sido escasamente abordado en la literatura y la doctrina militar. De hecho, el documento en cuestión se destaca como el único texto colombiano que profundiza en la conceptualización y aplicación de MASINT dentro del contexto militar del país. Este hecho resalta la novedad y la especialización del tema en el contexto nacional, donde la inteligencia MASINT aún se encuentra en una fase emergente de desarrollo y aplicación. Este tipo de inteligencia ofrece ventajas estratégicas significativas, permitiendo a las fuerzas armadas colombianas acceder a un nivel más profundo de análisis de amenazas y eventos, mejorando la capacidad de respuesta ante desafíos complejos. Las tecnologías utilizadas en la disciplina de Medidas y Huellas Distintivas (MASINT) son diversas y se enfocan en la recolección de datos a través de diferentes métodos avanzados. A continuación, te explico algunas de las tecnologías mencionadas en el documento: 1. "Inteligencia de Radar (RADINT)" : Esta tecnología se basa en el uso de radares para detectar, rastrear y analizar objetos, tales como misiles o aeronaves. Los radares pueden captar señales de radiofrecuencia reflejadas por los objetos, lo que permite determinar su posición, velocidad y características físicas. 2. Inteligencia Óptica (OPTINT): Implica el uso de dispositivos ópticos, como cámaras y telescopios, para la observación y análisis de objetos y eventos a Boletín final publicable:



ISSN: 2981-3506

BOLETÍN Nº 11

BOGOTÁ JULIO-SEPTIEMBRE 2024

ESICI BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

MEDIDAS DE PROTECCIÓN ESTRATÉGICA CONTRA RANSOMWARE EN INFRAESTRUCTURAS CRITICAS EN EL EJERCITO NACIONAL DE COLOMBIA

Escrito por: ST. Vargas Soto Carlos Manuel
Orientado por: Julián Camilo Guevara Cardona

Resumen: En la era digital actual, las infraestructuras críticas del Ejército Nacional de Colombia enfrentan crecientes amenazas cibernéticas, siendo el ransomware una de las más peligrosas. Estos ataques no solo pueden paralizar operaciones militares esenciales, sino también comprometer la seguridad nacional. Este boletín explora estrategias efectivas, basadas en investigaciones académicas para fortalecer la defensa contra el ransomware en el contexto militar colombiano.

Antecedentes en Colombia sobre el Rasomware:

A

El primer antecedente se presenta en el año 2018 a la empresa Carvajal Tecnología y Servicios, una empresa colombiana de soluciones de tecnología, que fue víctima de un ataque de Ransomware y a la vez comprometió su infraestructura tecnológica. Este incidente impactó a diversas entidades que dependían de sus servicios tecnológicos. *(Fuente: VENTASDESEGURIDAD.COM-VER HOSTING WEB, 2018)*

B

El ataque más reciente se presentó en septiembre de 2023, la empresa de servicios de telecomunicaciones IFX Networks sufrió un ataque de Ransomware que afectó a numerosas entidades en Colombia y otros países de América Latina. La suspensión de los servicios de IFX tuvo un impacto considerable, especialmente en empresas y organismos gubernamentales que dependían de sus servicios de internet y conectividad. *(Fuente: EL TIEMPO.COM-VER HOSTING WEB, 2023)*

RANSOMWARE

El Ransomware se mantiene como uno de los ataques preferidos por los cibercriminales. Esta modalidad criminal, con la que se secuestra información de una compañía, obligando o usuario para cobrar un rescate, tiene en alerta al continente americano, ante una ola de ataques que ha puesto a prueba sus relativamente inmaduros sistemas de ciberseguridad gubernamentales que dependían de sus servicios de internet y conectividad.

(Fuente: FORBES, 2023)

TÉCNICAS DE CIBERDELINCUENTES

En el ciberespacio hay diferentes técnicas utilizadas por los ciberdelincuentes, entre las más importantes se conocen las siguientes cuatro:

1. **PHISHING**
El phishing es una técnica en la que los atacantes envían correos electrónicos o mensajes que parecen provenir de fuentes confiables para engañar a las víctimas y hacer que revelen información confidencial, como contraseñas o datos bancarios.
(Fuente: VERIZON, 2023)

2. **VULNERABILIDAD CSRF**
La vulnerabilidad CSRF (Cross-Site Request Forgery), también conocida como "falsificación de solicitud en sitios cruzados", es una técnica de ataque que aprovecha la confianza que un usuario autenticado para que realice acciones no deseadas en una aplicación web en la que está autenticado.
(Fuente: OWASP FOUNDATION, n.d)

3. **MOVILIDAD LATERAL**
La movilidad lateral es una técnica utilizada por los ciberdelincuentes para explorar dentro de una red comprometida después de haber obtenido acceso inicial. Su objetivo es expandir su presencia en el control y buscar datos sensibles o sistemas críticos.
(Fuente: ZIMBA & WANG,Z, 2019)

4. **FUERZA BRUTA**
CrowdStrike 2023 Global Threat Report menciona que los ataques de fuerza bruta siguen siendo una técnica común entre los ciberdelincuentes, especialmente contra sistemas mal asegurados.
(Fuente: CROWDSTRIKE, 2023)



BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

TAXONOMÍA DE RANSOMWARE

- Plataformas PCS/ estaciones de trabajo dispositivos moviles IOT.
- Victimas y usuarios finales y organizaciones.
- Correos phishing.
- Aplicaciones Maliciosas.
- Descarga Automática.
- Vulnerabilidades.

OBJETIVOS | MÉTODOS DE INFECCIÓN | COMUNICACIÓN DE C&C | ACCIÓN MALICIOSA

- Cifrado IP.
- Basado en DGA.
- Cifrado.
- Bloqueo.
- Exfiltración de datos.

(Fuente: Flórez Rojas, N. F., & León Rubio, Y. L. (2024).

COMPRENSIÓN DE LA AMENAZA

Para desarrollar una defensa efectiva, es fundamental entender las tácticas, técnicas y procedimientos (TTP) utilizados por los actores de ransomware. Según Martínez et al. (2022) en Revista Colombiana de Seguridad Informática, el 75% de los ataques de ransomware contra entidades gubernamentales comienzan con campañas de phishing dirigidas y explotación de vulnerabilidades no parchadas.

(Fuente: Martínez, L., Gómez, A., & Rodríguez, P. (2022).

EVALUACIÓN DE RIESGOS Y VULNERABILIDAS

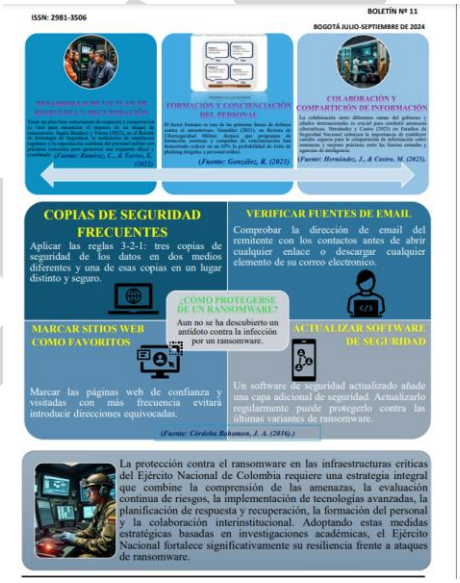
La identificación y evaluación continua de riesgos son esenciales para proteger las infraestructuras críticas. Pérez y López(2023), en el Journal de Defensa Nacional, destacan como una empresa de energía eléctrica debe someterse a revisiones constantes para prevenir ataques a los sistemas de seguridad de la empresa por parte del desarrollador del ingeniero de sistemas, aplicando una matriz de chequeo en el administrador de tareas.

(Fuente: Pérez, M., & López, S. (2023).

IMPLEMENTACIÓN DE TECNOLOGÍAS DE DEFENSA

Adoptar tecnologías avanzadas es clave para detectar y responder rápidamente a incidentes de ransomware. García et al. (2023) en Tecnología y Seguridad Militar, enfatizan el uso de soluciones de detección y respuesta extendida (XDR) y la inteligencia artificial para la identificación temprana de amenazas, reduciendo significativamente el tiempo de respuesta ante un ataque.

(Fuente: García, F., Ramírez, T., & Sánchez, J. (2023).



ISSN: 2981-3506

BOLETÍN Nº 11

BOGOTÁ JULIO-SEPTIEMBRE 2024

COPIAS DE SEGURIDAD FRECUENTES

Aplicar las reglas 3-2-1: tres copias de seguridad de los datos en dos medios diferentes y una de esas copias en un lugar distinto y seguro.

VERIFICAR FUENTES DE EMAIL

Comprobar la dirección de email del remitente con los contactos antes de abrir cualquier enlace o descargar cualquier elemento de su correo electrónico.

¿COMO PROTEGERSE DE UN RANSOMWARE?

Aun no se ha descubierto un antídoto contra la infección por un ransomware.

MARCAR SITIOS WEB COMO FAVORITOS

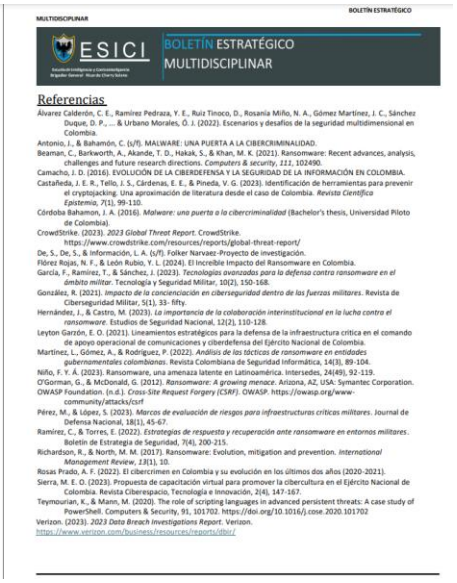
Marcar las páginas web de confianza y visitadas con más frecuencia evitará introducir direcciones equivocadas.

ACTUALIZAR SOFTWARE DE SEGURIDAD

Un software de seguridad actualizado añade una capa adicional de seguridad. Actualizarlo regularmente puede protegerlo contra las últimas variantes de ransomware.

(Fuente: Córdoba Bahamon, J. A. (2016).)

La protección contra el ransomware en las infraestructuras críticas del Ejército Nacional de Colombia requiere una estrategia integral que combine la comprensión de las amenazas, la evaluación continua de riesgos, la implementación de tecnologías avanzadas, la planificación de respuesta y recuperación, la formación del personal y la colaboración interinstitucional. Adoptando estas medidas estratégicas basadas en investigaciones académicas, el Ejército Nacional fortalece significativamente su resiliencia frente a ataques de ransomware.



BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

ESICI BOLETÍN ESTRATÉGICO MULTIDISCIPLINAR

Referencias

Álvarez Calderón, C. E., Ramírez Pedraza, Y. E., Ruiz Tinoco, D., Rosanía Miño, N. A., Gómez Martínez, J. C., Sánchez Duque, D. P., ... & Urbano Morales, Ó. J. (2022). Escenarios y desafíos de la seguridad multidimensional en Colombia.

Antonio, I., & Bahamón, C. (s/f). MALWARE: UNA PUERTA A LA CIBERCRIMINALIDAD.

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490.

Camacho, J. D. (2016). EVOLUCIÓN DE LA CIBERDEFENSA Y LA SEGURIDAD DE LA INFORMACIÓN EN COLOMBIA.

Castañeda, J. E. R., Tello, J. S., Cárdenas, E. E., & Pineda, V. G. (2023). Identificación de herramientas para prevenir el cryptojacking. Una aproximación de literatura desde el caso de Colombia. *Revista Científica Epistemia*, *7*(1), 99-110.

Córdoba Bahamon, J. A. (2016). *Malware: una puerta a lo cibercriminalidad* (Bachelor's thesis, Universidad Piloto de Colombia).

CrowdStrike. (2023). *2023 Global Threat Report*. CrowdStrike. https://www.crowdstrike.com/resources/reports/global-threat-report/

De, S., De, S., & Información, L. A. (s/f). Folker Narvaez-Proyecto de investigación.

Flórez Rojas, N. F., & León Rubio, Y. L. (2024). El increíble Impacto del Ransomware en Colombia.

García, F., Ramírez, T., & Sánchez, J. (2023). *Tecnologías avanzadas para la defensa contra ransomware en el ámbito militar*. Tecnología y Seguridad Militar, 10(2), 150-168.

González, R. (2021). *Impacto de la concienciación en ciberseguridad dentro de las fuerzas militares*. Revista de Ciberseguridad Militar, 5(1), 33- fifty.

Hernández, J., & Castro, M. (2023). *La importancia de la colaboración interinstitucional en la lucha contra el ransomware*. Estudios de Seguridad Nacional, 12(2), 110-128.

Leyton Garzón, E. D. (2021). Lineamientos estratégicos para la defensa de la infraestructura crítica en el comando de apoyo operacional de comunicaciones y ciberdefensa del Ejército Nacional de Colombia.

Martínez, L., Gómez, A., & Rodríguez, P. (2022). *Análisis de las tácticas de ransomware en entidades gubernamentales colombianas*. Revista Colombiana de Seguridad Informática, 14(3), 89-104.

Niño, F. Y. Á. (2023). Ransomware, una amenaza latente en Latinoamérica. Intersedes, 24(49), 92-119.

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Arizona, AZ, USA: Symantec Corporation.

OWASP Foundation. (n.d.). *Cross-Site Request Forgery (CSRF)*. OWASP. https://owasp.org/www-community/attacks/csrf

Pérez, M., & López, S. (2023). *Marcos de evaluación de riesgos para infraestructuras críticas militares*. Journal de Defensa Nacional, 18(1), 45-67.

Ramírez, C., & Torres, E. (2022). *Estrategias de respuesta y recuperación ante ransomware en entornos militares*. Boletín de Estrategia de Seguridad, 7(4), 200-215.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

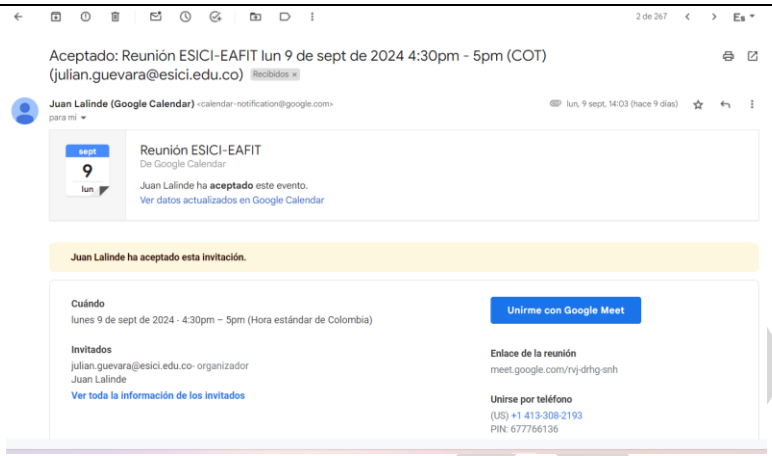
Rosas Prado, A. F. (2022). El cibercrimen en Colombia y su evolución en los últimos dos años (2020-2021).

Sierra, M. E. O. (2023). Propuesta de capacitación virtual para promover la cibercultura en el Ejército Nacional de Colombia. Revista Ciberespacio, Tecnología e Innovación, 2(4), 147-167.

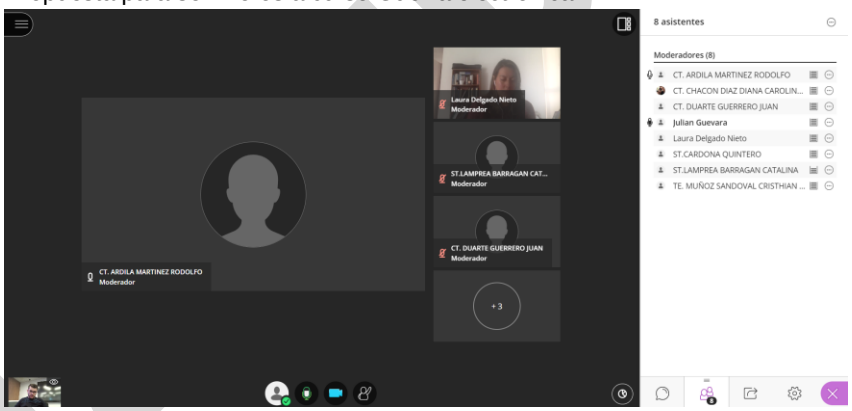
Teymourian, K., & Mann, M. (2020). The role of scripting languages in advanced persistent threats: A case study of PowerShell. Computers & Security, 91, 101702. https://doi.org/10.1016/j.cose.2020.101702

Verizon. (2023). *2023 Data Breach Investigations Report*. Verizon. https://www.verizon.com/business/resources/reports/dbir/

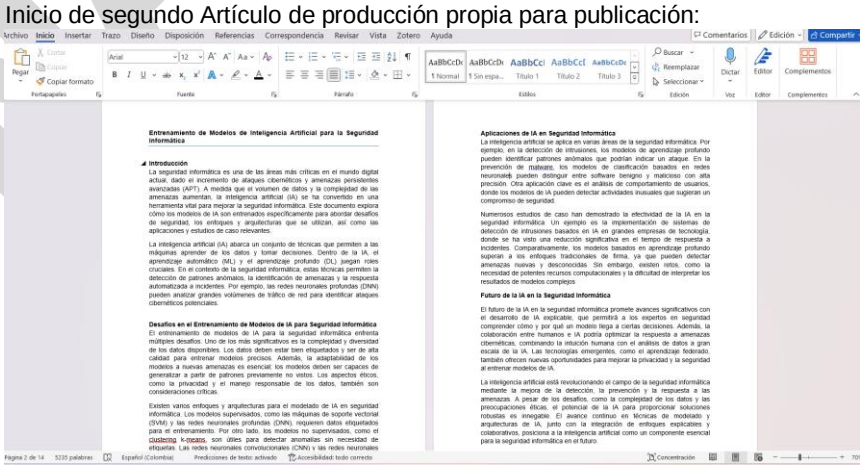
Reunión redes de investigación:



- Propuesta para semilleros a curso Guerra electrónica



- Inicio de segundo Artículo de producción propia para publicación:



- Gestión de invitación a docente a semillero de investigación

	Invitación a V Congreso internacional de Inteligencia Estratégica julian camilo guevara cardona <julian.guevara@esici.edu.co> 10:48 (hace 4 horas) para rafat.ghotme Estimado Profesor Rafat, Espero que se encuentre muy bien. A través de este mensaje, quisiera extenderle una cordial invitación a participar como ponente en el V Congreso Internacional de Inteligencia Estratégica, organizado por la Escuela de Inteligencia y Contrainteligencia BG Ricardo Charry Solano. Este es el evento académico más importante de la escuela, creado para conmemorar el Día de la Inteligencia y ofrecer un espacio de divulgación académica con un enfoque internacional. Considero que su perfil es idóneo para participar en este destacado encuentro. El evento se llevará a cabo en el auditorio de la Escuela Superior de Guerra, Batalla de Ayacucho. Quedo atento a su respuesta. Si está interesado, con mucho gusto le proporcionaré más detalles sobre el evento.  Cordialmente, Julián Camilo Guevara Cardona Profesional en Relaciones Internacionales y Estudios Políticos
11. CONSTANCIAS	Dejo constancia que, durante el plazo de ejecución del contrato, no se han configurado los presupuestos legales del contrato laboral y que he gozado de plena autonomía para ejecutar las obligaciones contractuales relacionadas en el contrato. Así mismo, tanto el/la suscrito/a y el Ministerio de Defensa – Ejército Nacional – Unidad Ejecutora ha dado cumplimiento a las obligaciones legales y contractuales registradas en el contrato.

Para constancia se firma en Bogotá **Septiembre** de 2024



JULIAN CAMILO GUEVRA CARDONA
Cc.1002397365

CENACED