LA CIBERINTELIGENCIA UN ESLABÓN CLAVE PARA LA SEGURIDAD INFORMÁTICA EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR PUBLICA DE COLOMBIA

CESAR AUGUSTO SANABRIA CASANOVA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
AÑO 2022

LA CIBERINTELIGENCIA UN ESLABÓN CLAVE PARA LA SEGURIDAD INFORMÁTICA EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DE COLOMBIA

CESAR AUGUSTO SANABRIA CASANOVA

Proyecto de Grado – Monografía presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

HERNANDO JOSE PEÑA HIDALGO
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA D.C
AÑO 2022

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, DC., Fecha sustentación

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

LISTA DE TABLAS

LISTA DE ANEXOS

Pág.

GLOSARIO

CIBERESPACIO: Mundo Virtual compuesto por medios tecnológicos físico y no físico perteneciente a la infraestructura de sistemas de información, industrial y de telecomunicaciones que interactúan a través del espectro electromagnético.

CIBERINTELIGENCIA: Proceso de inteligencia en el ciberespacio que permite generar prospectiva de las acciones de las amenazas y/o adversarios, logrando fortalecer la ciberseguridad.

CIBERSEGURIDAD: Actividades y procesos que permiten proteger y minimizar los riesgos en el ciberespacio.

CIBERCRIMEN: Conjunto de Actividades que se desarrollan a través del uso de medios tecnológicos compuestos por equipos de cómputo y sistemas de información que se encuentran en el ciberespacio como herramientas para cometer acciones delictivas.

CIBERAMENZAS: Acción de ataque que permite generar un riesgo a los sistemas de información y de telecomunicaciones de una organización u empresa.

MALWARE: Software o programa malicioso que comprometen y vulneran la seguridad de los sistemas de información, logrando comprometer los principios de la seguridad de la información “Disponibilidad, Confidencialidad e Integridad”.

INTELIGENCIA: Es el producto del proceso de información disponible que permite anticipar suceso y toma de decisiones a nivel gerencial, ejecutivo y técnico.

INTELIGENCIA DE FUENTES ABIERTAS, OSINT: Es el resultado del proceso de inteligencia en el ciberespacio de la información pública disponible encontradas en

medios de comunicación, datos públicos, literatura gris, informes de investigación, imágenes entre otros.

SISTEMAS DE INFORMACIÓN: Conjunto de medios tecnológicos interconectados conformado por hardware, software, bases de datos, y procesos automatizados que permiten recolectar, procesar, analizar y difundir información.

RESUMEN

La metodología para realizar la presente monografía se encuentra basada en el análisis del proceso de Ciberinteligencia para establecer como puede ser una estrategia para la toma de decisiones en la seguridad informática en las instituciones de educación Superior IES de Colombia, debido que estás son objetivos permanentes de los cibercriminales, los cuales se encuentra desarrollando ataques informáticos de forma permanente con el fin de comprometer los sistemas informáticos que se encuentra interconectados en el Internet.

El objetivo de esta monografía fue analizar el proceso de ciberninteligencia como estrategia para mitigar los riesgos informáticos, apoyando al gobierno corporativo y gobernanza de las Tecnología de la información logrando establecer políticas de seguridad informáticas en las IES, se plantea una revisión bibliográfica exploratoria mediante la lógica inductiva, el desarrollo de la perspectiva teórica está basado en revisión documental y de modelo mediante la implementación de escenarios simulados que permitirá establecer la unión entre la teoría y lo real.

De acuerdo con el análisis se busca establecer como el proceso de ciberinteligencia sea una estrategia para la toma de decisiones para la seguridad informática, mediante el análisis y evaluación de la información que se logre recolectar, logrando así que los niveles técnicos y tácticos posean la información necesaria para la implementación de la ciberseguridad y el nivel estratégico puedan elaborar políticas de seguridad en la IES de Colombia.

Palabras Claves: Amenazas, Cibierinteligencia, Inteligencia, OSINT, Riesgos, Seguridad Informática.

ABSTRACT

This research is based on the analysis of the cyber intelligence process to establish how a strategy for decision-making in computer security can be in higher education institutions (HEI) in Colombia, because these institutions are permanent targets of cybercriminals, who is permanently developing computer attacks to compromise the computer systems that are interconnected on the Internet.

The objective of this monograph was to analyze the cyberintelligence process as a strategy to mitigate computer risks, supporting corporate governance and governance of Information Technology, managing to establish computer security policies in higher education institutions (HEI), an exploratory bibliographic review is proposed through logic inductive, the development of the theoretical perspective is based on documentary and model review through the implementation of simulated scenarios that will allow to establish the union between theory and reality

According to the analysis, it is sought to establish how the cyber intelligence process is a strategy for making decisions for computer security, through the analysis and evaluation of the information that is collected, thus achieving that the technical and tactical levels have the necessary information for the implementation of cybersecurity and the strategic level can develop security policies in the higher education institutions (HEI) of Colombia

Keywords: Cyberintelligence, Computer Security, Intelligence, OSINT, Risks, Threats.

INTRODUCCIÓN

La inteligencia se viene desarrollando desde los inicios de los tiempos cuando Josué tomo 12 personas para realizar inteligencia a la tierra que su Dios le había dado por heredad, como lo indica la (Reina-Valera 1960) “Enviemos varones delante de nosotros que nos reconozcan la tierra, y a su regreso nos traigan razón del camino por donde hemos de subir, y de las ciudades adonde hemos de llegar”[1], los cuales pudieron saber contra quien se iban a enfrentar y poder crear una estrategia para derrotarlos, Desde entonces la inteligencia ha sido la punta de lanza para los estados, organizaciones, entidades entre otras, permitiendo desarrollar análisis de las amenazas y proyectar los diferentes eventos que pueden acontecer.

En nuestra actualidad existe el ambiente artificial llamado ciberespacio y con ello las diferentes amenazas que pueden generar riesgos en la seguridad de la información, por ello, las organizaciones viene implementado el proceso de inteligencia en el ciberespacio “Ciberinteligencia” como lo viene desarrollando las diferentes empresas como ESET[2] cuando realiza el proceso de la ciberseguridad desde el enfoque de la predicción mediante la ciberinteligencia permitiendo la anticipación de las amenazas del ciberespacio, como hipótesis central que a través de la ciberitneligencia permitirá predecir los vectores de ataques de las diferentes amenazas, permitiendo que las Instituciones de educación superior puedan generar estrategias a nivel táctico y a nivel estratégico con el fin de minimizar los riesgo de los sistemas de información de las IES, para ello nuestro objetivo central es analizar la ciberinteligencia como estrategia para mitigar los riesgos informáticos y apoyo a

[1]Biblegateway, Misión de los doce espías, [Sitio Web], Reina-Valera. (1960). [Consulta el 2 de diciembre de 2020], Disponible en https://www.biblegateway.com/passage/?search=Deuteronomio+1%3A19-33&version=RVR1960

[2] JAI XVIII JORNADA NACIONALES DE ADMINISTRACION E INFORMATICA (18: 10, NOVIEMBRE 2020, YouTube), La ruta de la ciberseguridad. ¿Qué camino puedo seguir?, UNER Facultad de Ciencia de Administración. Consulta 2 de diciembre de 2020, Disponible en https://www.youtube.com/watch?v=q1D1X3jNrC0&list=LL&index=7&t=2158s&ab_channel=UNERFcad

la toma de decisiones en políticas de seguridad para las instituciones de nivel superior pública.

Para ello se plantearon cuatro capítulos, primer capítulo trata de describir las principales amenazas existentes en el ciberespacio que afectan la seguridad informática en las instituciones de educación superior pública, donde se efectúa un estudio teórico de las diferentes amenazas existentes; el segundo capítulo se examina los pasos del proceso de ciberinteligencia para apoyar la seguridad informática en las instituciones de educación superior pública, donde se realiza una inspección minuciosa de las fases del planeamiento, recolección de información, procesamiento y análisis de datos, difusión y explotación de la inteligencia, y la retroalimentación; el tercer capítulo trata cuales son las herramientas de recolección de información, donde se trata de analizar herramientas tecnológicas que permitan la recolección de información de las principales amenazas a través de escenarios simulados para evaluar los impactos en las instituciones de educación superior pública y el cuarto capítulo análisis de amenazas donde se identifica como las amenazas pueden afectar la seguridad de la información y como puede afectar la seguridad informática en las Instituciones de educación superior pública.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

A través del tiempo los incidentes informáticos son cada vez son mayores, teniendo en cuenta que al incrementar el uso de los medios tecnológicos y del ciberespacio por parte de las personas, empresas, instituciones y organización son más propensos a recibir ciberataques aumentando los riesgos en los sistemas de información. En el año 2017 se desato una ola ataque de forma global por parte del software malicioso llamado WannaCry quien logra infectar un aproximado de diez mil equipos por hora y alcanzo infectar doscientos treinta mil equipos en un solo día, este ataque afecto diferentes organización entre ellas se encuentra FedEx, Honda, telefónica, Renault, también fueron víctimas las universidades como la Universidad de Guilin de Tecnología Electrónica, Universidad de Tecnología Aeroespacial de Guilin, Universidad Marítima Dalian, Cambrian College, Universidad Aristóteles de Tesalónica, Universidad de Montreal, así mismo las agencia gubernamentales como las Policía de Andhra Pradesh, Ministerio de Seguridad Pública de China, Instituto Nacional de Salud (Colombia), Servicio Sanitario Nacional (Reino Unido), NHS de Escocia, tribunales de São Paulo, varias administraciones en India (Gujarat, Kerala, Maharashtra, Bengala occidental) estas organizaciones tuvieron realizar grandes pagos en bitcoin dentro del rango de 300 a 600 dolares con una estimación de 130.634 USD por pagos de rescate de información, así mismo la organización Cyence estima el consto de limpieza del ciberataque fue de cuatro mil millones de Dolares (4000 millones de USD) como lo indico (Latto, 2020)[3].

1.2 FORMULACIÓN DEL PROBLEMA

Durante el 2019 las universidades de Europeas recibieron gran cantidad de ataques cibernéticos, dentro de estos ataques han sido mediante el uso del Ransomware y

[3] Latto, N. Avast, ¿Qué es WannaCry?,[Sitio Web] 27 de febrero de 2020. Consultado el 9 de octubre de 2020, Disponible en: https://www.avast.com/es-es/c-wannacry

phishing, logrando así acceder a información como datos personales, pasaportes, dirección de correo electrónico de los integrantes de las universidades vulneradas como lo referencia (Iurcu, 2020)[4], donde se puede observar que las universidades son aperitivos para los ciberdelincuente, teniendo en cuentas que en estas instituciones no cuentan con infraestructura tecnológica adecuada y falta de personal con conocimientos en seguridad informática, sirviendo en bandeja de plata las bases de datos que poseen, así como los productos de investigación avanzada que desarrollan dichas instituciones de educación superior.

En el 2020 al llegar la pandemia del COVID 19, el auge del uso del ciberespacio aumento, permitiendo que los ciberdelincuentes incrementen sus acciones delictivas a través de ataques informáticos a las diferentes empresas y organizaciones aumentando el riesgo de los sistemas de información según (INTERPOL, 2020) cuando define que "Los ciberdelincuentes están creando nuevos ataques e intensificando su ejecución a un ritmo alarmante, aprovechándose del miedo y la incertidumbre provocados por la inestabilidad de la situación socioeconómica generada por la COVID-19"[5], generando como reporte la identificación de 907 mil correos basuras, 737 incidentes con malware, y 48 mil URL maliciosos, de los cuales los cibercriminales han implementado la estafa por internet y phishing, malware de tipo Ransomware y DDoS, Malware de obtención de datos, Dominios Malicioso, y la desinformación.

Ante estas eventuales amenazas que han resultado a través del tiempo, se requiere generar una estrategia y una táctica que permita minimizar, contrarrestar, y conocer

[4] Iurcu, V. Avira, Ciberataques en la universidad: ¿qué universidades son objetivo de los piratas, ¿cómo y por qué?,[Sitio Web] 8 de septiembre de 2020. [consultado 9 de octubre de 2020], Disponible en: https://www.avira.com/es/blog/ciberataques-en-la-universidad-que-universidades-son-objetivo-de-los-piratas-como-y-por-que

[5]INTERPOL Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19, [Sitio Web], Secretaría General de INTERPOL, [Consulta el 9 de octubre de 2020], Disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

todas estas amenazas que ponen en riesgos a múltiples organizaciones, en nuestro caso las instituciones de educación superior, por ello (Candau, 2017) indica que la ciberinteligencia es una estrategia que permite la toma de decisiones en una organización y se puede hacer usos como una táctica para el mejoramiento de la seguridad mediante la detención y respuesta de los posibles ataques que pueden originar los cibercriminales[6], para ellos se requiere que la ciberinteligencia de respuesta quienes son los posibles cibercriminales como lo indica (Ruiz, 2018) cuando hace alusión "La ciberinteligencia Cyber Threat Intellignece (CTI), nació para dar respuesta a estas carencia, se concibió para conocer a los "malos" recabando toda información posible de todas la fuentes hábiles"[7]

Por lo anterior se requiere generar una estrategia que permita mitigar y prevenir todos estos riesgos que pueden generar los ciberdelincuentes al momento de realizar ataques informáticos, es por ello debemos analizar como la ciberinteligencia puede mitigar los riesgos generados por los ciberdelincuentes en las instituciones de educación superior, es por ello que esta es un eslabón clave para la seguridad de la información en las Instituciones de educación superior.

¿Cómo la ciberinteligencia puede ser una estrategia para mitigar los riesgos informáticos y poder apoyar a la toma de decisiones en políticas de seguridad para las instituciones de nivel superior en Colombia?

[6] Candau, Javier. Ciberinteligencia, complemento perfecto para la Ciberseguridad. Revista Redseguridad*, 2017*, nro. 079, pp 52-54 . [consulta 13 octubre de 2020], Disponible en: https://www.redseguridad.com/revistas/red/079/52/

[7] Ruiz, J. J. Ciberinteligencia 2.0: predicción, Revista Redseguridad, nro. 083, pp 56-57, [consulta 13 octubre de 2020], Disponible en: https://www.redseguridad.com/revistas/red/083/56/index.html

2 JUSTIFICACIÓN

Mediante el incremento del uso del ciberespacio por parte de las organizaciones, instituciones y personas, del mismo modo se ha incremento los ataques cibernéticos por parte de los cibercriminales generando grandes pérdidas económicas, estos ataques no se encuentra excluida las Instituciones de educación superior, ya que estas manejan gran cantidad de información de interés para los cibercriminales como información personal de los estudiantes, docentes y directivos, así como investigaciones o proyectos investigativos e información financiera, donde pueden ser víctimas de robo de información, secuestros, acceso no autorizados a las TI, captación de datos en la red, denegaciones de servicios, entre otros, en diferentes países a nivel mundial se conocen que diferentes ciberataques han logrado comprometer los sistemas informáticos como su información, generando pérdida de credibilidad antes la comunidad.

Por lo anterior se requiere que los responsables de la seguridad informática, junto con el gobierno corporativo establezcan estrategias para mitigar y responder antes los diferentes riesgos que se presentan en el ciberespacio, para ello se recomienda realizar un análisis de la estrategia de ciberinteligencia, examinando sus fases y acciones del proceso de inteligencia en el ciberespacio, examinado las herramientas de recolección de información, analizar y evaluar la información recolectada, permitiendo la generación de reportes o informes de ciberinteligencia, para que los responsables de la ciberseguridad y el gobierno corporativo pueden tomar las decisión correspondientes a la mitigación de los riesgos y la continuidad de los servicios en las Instituciones de educación Superior.

Esta monografía permitirá la adopción de la ciberinteligencia como opción fundamental como estrategia para la continuidad de los servicios en las instituciones de educación superior Colombia, mediante la predicción de los ciberataques, mitigación y respuesta de los riesgos apoyando la ciberseguridad a nivel técnico,

táctico y estratégico, brindando confianza ante los clientes que son sus estudiantes, docentes y directivos, y manteniendo el Good Will de la IES, así como el cumplimento los principios rectores de la Ley de protección de datos 1581 de 2012.

Dado que el termino y el proceso de ciberinteligencia es poco conocido y aplicado a la ciberseguridad en las Instituciones de educación superior y/o en organizaciones como estrategia para el fortalecimiento de la ciberseguridad, donde no se ha podido obtener mayor información de interés, la presente monografía contribuirá a futuros estudios abordar la temática de la ciberinteligencia en las organizaciones o en los diferentes contextos que se pueda implementar para la toma de decisiones en el gobierno corporativo y en la gobernanza de la Tecnología de la Información.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el proceso de ciberinteligencia como estrategia para la mitigación de riesgos informáticos en las instituciones de educación superior de Colombia y facilitar su adopción y mejora en los niveles de seguridad.

3.2 OBJETIVOS ESPECÍFICOS

- Inspeccionar las amenazas que pueden afectar los activos de información en el ciberespacio, mediante la revisión de informes y estadísticas oficiales, que permita identificar los principales riesgos a los que se enfrentan las IES de Colombia.

- Examinar las metodologías del proceso de inteligencia en el ciberespacio como estrategia de ciberseguridad, para la adopción por parte de las IES de Colombia.

- Evaluar las herramientas orientadas a la recolección de información de las principales amenazas, mediante la validación de escenarios simulados que permitan evaluar los impactos en las IES de Colombia.

- Demostrar como la estrategia de ciberinteligencia facilita la identificación de riesgos informáticos, mediante informes de inteligencia del ciberespacio sobre amenazas que afectar la ciberseguridad en las IES de Colombia.

4 MARCO REFERENCIAL

4.1 MARCO TEORICO

El ciberespacio es un entorno virtual creado por los humanos en donde existen múltiples amenazas y vulnerabilidades, generando riesgos a los sistemas de información, estas amenazas y vulnerabilidades son dinámicas de acuerdo a los cambios que pueden existir en los cambios de las tecnologías, comportamiento sociales y culturales, dando cavidad a la teoría del caos propuesta por su precursor Edwar Lorenz en 1963 mencionado por (Carlos Martínez, 2018) al definir "… la teoría del caos estudia la sensibilidad a las condiciones iniciales de algunos sistemas, es decir, de aquellos sistemas en los que un pequeño cambio, puede generar grandes consecuencias"[8], por lo anterior el ciberespacio posee un ambiente volátil, incierto, complejo y ambiguo (VICA) exponiendo los sistemas de información a gran cantidad de riesgos, formando un sistema dinámico.

Así mismo los sistemas de información se encuentran conformados por personas, hardware, software, información y procesos, los cuales se encuentra conectados a través de las redes creando el ciberespacio, cada uno de estos componentes conforman vectores de ataques que pueden ser aprovechados por las amenazas. Estas amenazas pueden generar desde pequeños cambios en los sistemas de información como ejemplo la degradación de la información a largo plazos hasta afectar completamente los sistemas de información, así como el aprovechamiento de vulnerabilidades "Zero Day" que permite aprovechar las vulnerabilidades no identificadas por los fabricantes generando riesgos informáticos y con ello afectar a las organizaciones que cuentan con los sistemas información.

[8] Martínez Moncaleano, Carlos Javier. TEORÍA DEL CAOS Y ESTRATEGIA EMPRESARIAL. *Tender.* [en línea]. 2018, vol.19, n.1 [citado el 27-03-2022], pp.204-14. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-69320180001002 04&lng=en&nrm=iso]. ISSN 0124-8693. https://doi.org/10.22267/rtend.181901.94

Desde la creación del ciberespacio se ha generado múltiples amenazas que pueden afectar las organizaciones públicas, estatales y privadas los cuales es de importancia la implementación y uso de la inteligencia en este escenario virtual, creando la ciberinteligencia, unos de los propósitos de la ciberinteligencia es predecir los riesgos en el ciberespacio, minimizando el impacto y la probabilidad de ocurrencia de los riesgos, es por eso que (Oscar Sanchez, 2021) habla de los objetivos de la ciberinteligencia puntualizando lo siguiente "la ciberinteligencia es adelantarse mediante estimaciones a la existencia de riesgo y amenaza"[9].

Como estrategia a implementar para contrarrestar las amenazas es el uso de la inteligencia en el ciberespacio. La inteligencia es el producto de la recolección y procesamiento de datos para la generación del conocimiento, donde (Juan Carlos Estarellas, 2018) define la inteligencia como el conjunto de instrumentos empleados para la generación de información y creación del conocimiento que permitan contrarrestar las amenazas[10], la Escuela de Postgrado de Ciencia del Derecho ratifica el concepto y función de la ciberinteligencia al indicar "Se encarga de conseguir información, procesarla y convertirla en conocimiento valioso para investigar, encontrar y predecir ataques o amenazas cibernéticos, y finalmente proponer planes de acción", descrito dicha información podemos enfatizar que la ciberitneligencia o la inteligencia en el ciberespacio permite establecer una estrategia para la ciberseguridad en las instituciones de educación superior en Colombia, permitiendo que los Directivos a nivel estratégicos y los técnicos a nivel táctico pueden realizar e implementar medidas de seguridad para proteger los sistemas de información.

De igual forma (Camila Gomez, 2017) en su artículo, La nueva era de la información como poder y el campo de la ciberinteligencia cita a Sun Tzun menciona que

[9] Ibit, p 122
[10] Estarellas, J. C. Objetivo de inteligencia: infiltrar Al Qaeda. [En Linea] Madrid: Bubok Publishing S.L. eLibro 2018 [Citado el 08 abril 2022] Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51385?page=20

conocimiento previo es una estrategia para obtener la victoria haciendo alusión a la inteligencia.

> "…what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. That is, knowledge of the enemy's dispositions, and what he means to do. This foreknowledge cannot be elicited from spirits, and cannot be obtained inductively from experience, nor by any deductive calculation. Knowlegde of the enemy's dispositions can only be obtained from other men…"[11]

Frente a la necesidad de salvaguardar la información y los activos informáticos de las amenazas es necesario la generación de conocimiento, para ello se debe implementar métodos y/o procedimientos para el procesamiento de información, para ello se puede contar con el método científico, (Jose Lenin, 2015) cita a (Munch y Angeles, 2007) quienes lo definen como "El método científico es la explicación, descripcion y predicción de fenómenos, su esencia es obtener con mayor facilidad el conocimiento cientifico", de igual forma (Jose Lenin, 2015) define el método científico como "…conjunto de pasos que se siguen en la generación de conocimiento objetivo, avalado por una serie de reglas rigurosas que no den lugar a dudas que ese conocimiento se pueda justificar, teórica y empíricamente, es decir, que el conocimiento es verdadero"[12], Dentro del método científico existe técnicas que permite desarrollar las etapas de investigación permitiendo realizar la recolección de información, clasificación de los datos, correlación y análisis permitiendo así la generación de conocimiento.

---

[11] Camila Gomes de Assis. La Nueva Era De La Información Como Poder Y El Campo De La Ciberinteligencia/ The New Era of Information As Power and the Field of Cyber Intelligence [en línea] URVIO, Revista Latinoamericana de estudios de Seguridad, No 20 junio del 2017 [Consulta 27 de marzo de 2022], Disponible https://revistas.flacsoandes.edu.ec/urvio/article/view/2577/1609

[12] José César Lenin Navarro Chávez. Epistemología y metodología. [En Línea] México D.F: Grupo Editorial Patria, 2015. eLibro. [Citado el 08 de abril 2022] Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/39400?page=202

De igual forma se cuenta con el proceso de la inteligencia que contiene los diferentes fases o pasos como (Misión, Planeación, Recolección de información, Procesamiento, Análisis de información, Diseminación de información) permite poseer un conocimiento previo o prospectiva permitiendo anticiparse de los posibles sucesos que pueden realizar las amenazas, así como lo cita (Oscar Sanchez, 2021) al mencionar "…inteligencia establece estimaciones para una eficaz toma de decisión, inteligencia apoya a las operaciones de una organización, es decir a la seguridad que atiende a proteger al objeto referente, Estado, territorio, individuos etc."[13]

Para la protección de las organización frente a las amenazas existentes en el ciberespacio se debe realizar una constante búsqueda de datos en el Internet, Dark Web y Deep Web que permita realizar el procesamiento y análisis de la información (Proceso de inteligencia) para determinar las tendencias de las ciberamenazas, incidentes informáticos y tipos de vectores de ataque que pueden estar expuestas las organizaciones, la (Universidad de la Rioja 2021) determina este proceso como la ciberinteligencia.

> "Los servicios de ciberinteligencia, también conocidos como inteligencia de ciberamenazas o vigilancia digital, consisten en proporcionar conocimiento basado en evidencias sobre las amenazas contra activos de las organizaciones. Dicho conocimiento incluye información de contexto, descripción de los mecanismos, indicadores de riesgo y recomendaciones de actuación en relación con las amenazas existentes. Además de esto, se enfocan en conocer las últimas ciberamenazas o riesgos relevantes de seguridad a nivel nacional, global y por sector de actividad.[14]"

[13] Oscar Sanchez Belmont, Ciberinteligencia y cibercontrainteligencia: aplicación e impacto en la seguridad nacional (2021) eLibro, (Ciudad de México Instituto Mexicano de Contadores) Recuperado el 20 de marzo de 2022, disponible: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/174910?page=115.

[14] Universidad Internacional de La Rioja UNIR, ¿En qué consiste la ciberinteligencia? Aplicaciones y ejemplos. [Sitio Web] https://www.unir.net [Consulta 20 de marzo de 2022], Disponible en: https://www.unir.net/ingenieria/revista/ciberinteligencia/

La inteligencia en el ciberespacio permitirá identificar la superficie de ataque que pueden aprovechar las amenazas, facilitando identificar las vulnerabilidades existente en la organización, como lo dice Oscar Sanches Belmont al mencionar la importancia de la inteligencia, “Inteligencia permite saber los posibles ataques cibernéticos a posibles activos vulnerables de información, no solo para sustraerla, sino para manipularla a su favor, poniendo en riesgo a la seguridad nacional o al ámbito corporativo”[15], con la ciberinteligencia se identifica las vulnerabilidades y amenazas, facilitando el entendimiento en los niveles de riesgos que se encuentra la organización.

Oscar Belmont rescata que la estrategia para la seguridad de la información es el adecuado análisis de datos que permite la construcción de la información construyendo estrategias con bases a la ciberinteligencia permitiendo minimizar, neutralizar y mitigar las amenazas.

Se observa dentro del proceso de análisis y administración del riesgo el desarrollo del proceso de inteligencia en el ciberespacio en el cual realiza el tratamiento de la información disponible de acuerdo a los datos y activos informáticos que pueden estar expuestos a las ciberamenazas facilitando identificar las posibles vulnerabilidades que pueden generar un riesgo en las organizaciones, como lo indica (Oscar Sanchez Belmont, 2021) al mencionar.

> “Por lo tanto, el análisis y administración de riesgos se centra en aquellos elementos que, dado su significado, por lo vínculos de datos que cuenta, para visualizar algunos posibles eventos que pongan en peligro a dichos datos vinculados, donde pueden ser clasificados como activos, tanto para su protección

[15] Oscar Sanchez Belmont, Ciberinteligencia y cibercontrainteligencia: aplicación e impacto en la seguridad nacional (2021) eLibro, (Ciudad de México Instituto Mexicano de Contadores) Recuperado el 20 de marzo de 2022, disponible: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/174910?page=32

(contrainteligencia) como para la búsqueda (inteligencia) de riesgos o amenazas, a fin de ubicar dichas acciones que ataquen posibles vulnerabilidades del sistema de protección de activos".

El proceso de inteligencia en el ciberespacio se posesiona como estrategia de seguridad de la información permitiendo identificar las vulnerabilidades, amenazas mediante la recolección y análisis de los datos, estableciendo los riesgo que pueden materializarse en los sistemas informáticos, con ello facilita establecer procesos, métodos y políticas que permitan mitigar y neutralizar las amenazas.

4.2 MARCO CONCEPTUAL

El concepto del ciberespacio se puede definir de diferente formas, entre ellas mencionaremos el concepto brindado por el (CONPES 3701, 2011) tomado de la resolución CRC 2258 de 2009, donde indica que el ciberespacio "Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuario"[16], también podemos hacer mención lo que indica el centro criptológico nacional de España, cuando brinda su concepto en la guía de seguridad CCN-STIC-40 donde lo define como "Dominio global y dinámico compuesto por infraestructuras de tecnología de la información — incluyendo internet—, redes de telecomunicaciones y sistemas de información"[17], es por ello que el ciberespacio lo podemos definir como el espacio donde se interconectan entre los diferentes sistemas de información y de comunicaciones que permiten la interacción e intercambio de datos entre sí.

Dentro del ciberespacio existen multiplex amenazas que pueden generar riesgos en

[16] MINISTERIOS DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES, Conpes 3701.[Sitio Web], https://mintic.gov.co/ [Consulta 17 octubre de 2020], Disponible en: https://mintic.gov.co/portal/604/articles-3510_documento.pdf

[17] Centro Criptológico Nacional CCN. [Sitio Web], Madrid, España, Guía De Seguridad (CCN-STIC-401) Glosario Y Abreviaturas. [Consulta 17 de Octubre de 2020], Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

las diferentes organizaciones tanto públicas y privadas por ello se requiere contextualizar que es ciberamenazas, donde (Diaz, 2016) define como ciberamenazas, todas aquellas actividades que tiene el fin de obtención, utilización, manipulación y control de la información mediante los delitos informáticos en el ciberespacio[18], también podemos indicar que estas actividades delictivas se pueden denominar como amenazas ciberneticas o amenazas informática, donde (CONPES 3701, 2011) y (CONPES 3854, 2016) lo define como "aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado"[19], estas definición está relacionada mediante un enfoque de defensa nacional, también podemos mencionar que (CONPES 3854, 2016) indica que las actividades ilegales mediante el uso de medios tecnológicos están asociado a los delitos informáticos.

Mediante el usos de las amenazas cibernéticas los cibercriminales pueden generar los ataques cibernéticos o ciberataque, (CCN, 2015) plantea que los ciberataques se encuentra denominados como "Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan"[20] y el (CONPES 3854, 2016) define los ataques cibernéticos "acción organizada o premeditada de una o más agentes para causar daño o problemas a

[18] Diaz, J. R. Instituto Español de Estudios Estratégicos, Ciberamenazas ¿El terrorismo del Futuro? (Boletín Electrónico 86/2016: 19 agosto 20160), Consulta 17 de octubre de 2020, Disponible en http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

[19] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, Documento CONPES 3854, Política nacional de seguridad digital, [Sitio Web] Bogotá: Cámara De Comercio De Bogotá. [Consulta 17 octubre 2020], Disponible en: https://bibliotecadigital.ccb.org.co/handle/11520/14856

[20] Centro Criptológico Nacional CCN. [Sitio Web], Madrid, España, Guía De Seguridad (CCN-STIC-401) Glosario Y Abreviaturas. [Consulta 17 de Octubre de 2020], Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

un sistema a través del Ciberespacio."[21], estos dos conceptos empleados por Consejo Nacional de política económica y social, y por el Concejo criptológico nacional de España los cuales permite establecer que los ciberataque son perpetuados por los cibercriminales que ponen en riesgos los principios de la ciberseguridad de las tecnologías de información y de las comunicaciones.

Para salvaguardar sistemas informáticos que se encuentra conectados entre sí y hacia el internet se requiere implementar la ciberseguridad, el Consejo criptológico Nacional de España define la ciberseguridad como "Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan"[22], de igual manera lo manifiesta (CISCO, 2020) al indicar que la ciberseguridad es el proceso para salvaguardar los equipos de cómputos en red y mantener seguro a las personas y organización que hacen uso del internet[23].

Unos de las mejores y completa definiciones en cuanto a la ciberseguridad que podemos desatacar es la que hace referencia el (CONPES 3854, 2016), así:

> Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio[24].

---

[21] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, Documento CONPES 3854, Política nacional de seguridad digital, [Sitio Web] Bogotá: Cámara De Comercio De Bogotá. [Consulta 17 octubre 2020], Disponible en: https://bibliotecadigital.ccb.org.co/handle/11520/14856

[22] Centro Criptológico Nacional CCN. [Sitio Web], Madrid, España, Guía De Seguridad (CCN-STIC-401) Glosario Y Abreviaturas. [Consulta 17 de Octubre de 2020], Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

[23] CISCO. ¿Qué es la ciberseguridad? [Sitio Web] www.cisco.com. [Consulta 17 octubre de 2020], Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

[24] Centro Criptológico Nacional CCN. [Sitio Web], Madrid, España, Guía De Seguridad (CCN-STIC-401) Glosario Y Abreviaturas. [Consulta 17 de Octubre de 2020], Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

Por lo anterior podemos indicar que esta definición hace énfasis los diferentes elementos que se deben tener en cuenta en la implementación de la ciberseguridad, dando mayor cobertura en el empleo de buenas prácticas para el cumplimento principios de la seguridad informática en las TIC y defensa en profundidad.

No podemos olvidar mencionar la ciberinteligencia donde (Portillo, 2018)[25] la define como el producto de inteligencia en el ciberespacio la cual permite identificar y contrarrestar los cibercriminales, para fortalecer este concepto es necesario apoyarnos con la definición descrita por (Centro Criptológico Nacional 2015)[26] el cual resalta que la ciberinteligencia son actividades de inteligencia que apoya la seguridad Informática donde realiza el análisis de los cibercriminales con el fin de identificar, localización, y atribuir los ataques cibernéticos, es así que podemos tomar que la ciberinteligencia es el desarrollo del proceso de inteligencia en el ciberespacio que permite fortalecer la ciberseguridad, analizando y evaluando los ataques informáticos que desarrollan los cibercriminales y mitigar los riesgos por parte de las organizaciones.

4.3 MARCO CONTEXTUAL

El ciberespacio dio inicio mediante un proyecto militar del departamento de Defensa de los Estados Unidos de América en el año 1964, mediante el proyecto Arpanet, en este proyecto participaron diferentes instituciones entre ellas se encuentra la Universidad de California, Instituto de Investigación de Stanford, Universidad Santa Barbara de California, y la Universidad de Utah, el proyecto Arpanet tenía como

[25] Portillo, I. La inteligencia de amenazas o Cyber Threat Intelligence, [Sitio Web]. GINSEG. [Consulta 18 octubre de 2020], Disponible en:https://ginseg.com/2018/956/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/

[26]Centro Criptológico Nacional CCN. Guía de Seguridad (CCN-STIC-425) Ciclo De Inteligencia y Análisis de Intrusiones. [Sitio Web] España: Ministerio de la Presidencia. [Consulta 17 de octubre de 2020], Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html

prioridad la transmisión de datos de forma descentralizada y fragmentada , por lo cual se dio la necesidad la implementación de protocolos que permitieran cumplir dicha necesidad durante la historia se fueron creando diferentes protocolos entre ellos se encuentra el protocolo NCP (Nertwork Control Protocol) que fue implantando en el año 1972, también se desarrolló el protocolo TCP - IP (Transmissop -Control Protocol/ Internet Protocol) e inicio su implementación en el año 1983, generando la interconexión de red[27].

Dentro el proceso del desarrollo de la Web y el ciberespacio se crearon varios servicios de transferencia de información digital los cuales podemos encontrar protocolos de correo electrónico entre ellos se encuentra Simple Mail Transfer Protocol (SMTP), Post Office Protocol V3 (POP3), Internet Mesager Acces Protocol (IMAP), Multipurpose Internet Mail Extensión (MIME), dentro de estos servicio también podemos en contra programas de correo electrónico entre transferencia podemos mencionar el protocolo de transferencia de archivos (FTP) el cual permite el uso compartido de archivos y transferir los datos de forma fiable y eficiente, también podemos hablar del aplicativo Telnet el cual tiene una capacidad de realizar conexiones remotas, y como parte fundamental dentro del ciberespacio se encuentra World Wide Web el cual usa un protocolo HTTP, permitiendo la transferencia de información mediante el uso del lenguaje de etiquetas HTML y el sistema de conexión cliente / servidor[28].

Mediante la construcción de la WEB o la red mundial en 1996 (Barlow, 1996) hace la primera cita de la existencia del ciberespacio cuando hace alusión la siguiente frase “Gobiernos del Mundo Industrial, gigantes cansados de carne y acero, vengo del Ciberespacio, el nuevo hogar de la mente.”[29], dando este significado que la WEB

[27] Chávez, C. F. (2018). eLibro. (E. CidEditor, Ed.) Recuperado el 9 de octubre de 2020, de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/36728
[28] Fresno Chávez, C. (2018). ¿Cómo funciona Internet? Editorial Ciudad Educativa. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/36728?page=32
[29] Chávez, C. F. (2018). eLibro. (E. CidEditor, Ed.) Recuperado el 9 de octubre de 2020, de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/36728

es el ciberespacio, un mundo de intangible y virtual creado por los hombre, si damos una mirada nuevamente hacia el pasado cuando se describía la línea de tiempo del ciberespacio, durante su construcción fueron apareciendo software maliciosos que fueron afectando el ciberespacio, unos de los primeros software que se desplazaba por la red sin restricciones fue Creeper, aunque era software no malicioso, fue dominado como el primer virus en el año 1971 creado por Robert Thomas, también podemos hacer alusión la creación de un código que permitía acceder a los sistemas informáticos desarrollado por Fred Cohen en 1984, de acuerdo a (Yanes, 2017) Fred Cohen da una definición a estos códigos maliciosos como "un programa que puede infectar otros programas modificándolos para incluir una versión de sí mismo, posiblemente evolucionada"[30].

De acuerdo a la gran evolución que se viene presentando en el ciberespacio, fue tomando una gran importancia en la sociedad en el mundo actual, hasta el punto de que las Organización del Tratado del Atlántico Norte "OTAN" manifiestan que el ciberespacio es un nuevo dominio de la guerra donde en él se pueden recibir ataques digitales para desestabilizar un país o nación[31], también lo ve de esta manera la (Unidad Análisis de Inteligencia S21SEC, 2017) cuando hacen alusión que "el futuro de la ciberseguridad pasa por un progreso mucho más centrado en el concepto de "ciberguerra" "[32], donde podemos indicar que en el ciberespacio se viene presentando multiplex ataques hacía las diferentes instituciones y organizaciones como públicas y privadas, estos ataques son perpetuados por cibercriminales denominados Hacker Black Hat, entre otros.

[30] Yanes, J. La historia de los virus informáticos. [Sitio Web] OpenMind BBVA. [Consulta 9 octubre de 2020], Disponible en:https://www.bbvaopenmind.com/tecnologia/mundo-digital/la-historia-de-los-virus-informaticos/

[31] Theiler, O. Nuevas amenazas: el ciberespacio [Sitio Web]. Revista de OTAN. [Consulta 9 octubre de 2020], Disponible en: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm

[32] UNIDAD DE ANALSIS DE INTELIGENCIA DE S21SEC. Ciberinteligencia: el Futuro de la Ciberseguridad, Revista Redseguridad,2017, nro. 067, pp 64-65 [Consulta: 14 Octubre de 2020]. Disponible en: https://www.redseguridad.com/revistas/red/079/64/.

Los diferentes cibercriminales realizan diferentes tipos de ataques aprovechando las vulnerabilidades que poseen las organización como entidades gubernamentales, entidades financieras, infraestructura críticas, hospitales y nuestro caso de estudio las instituciones de educación superior, donde estos tipos de ataques usan diferentes técnicas para acceder de forma no autorizada, robar credenciales e información importante y denegación de servicios, dentro de los ataques informático se puede clasificar en ataques pasivos y activos[33], dentro de estos clase de ataques como lo menciona (Ramiro, 2018)[34] cuando define los 25 tipos de ataque más conocidos entre ellos se encuentra los Ataque DoS, Ping Flood, Ping de la Muerte, Escaneo de puertos, ARP Spoofing, ACK Flood, Ataque FTP Boune, TCP Session Hijacking, Ataque Man – in- the- Middle, Ataque de Ingeneria Social, OS Finger Printing, Key Logger, ICMP Tunneling, Ataque LOKI, Ataqeu de secuencia TCP, CAM Table Overflow, Ataques a Aplicación WEB, Malware, (CONVERSIA, 2017)[35] también hace mención de los diferentes tipos de ciberataques de los cuales hace mención del Ransomware, Malware, Phishing, Spyware, DDOS, Troyanos, los cuales son los ataques más comunes en la actualidad[36], adicionalmente (Surmay, 2020) informa que el centro de recursos para robo de identidad (ITRC) manifiesta que de 1115 casos de vulneración de datos durante el año 2019 el 76% de los ataque los más comunes son el uso de Malware, ingeniería Social, Phishing, ataques intermediarios donde hace alusión del Ataque Man – in- the- Middle, Ataque de denegación de servicio e Inyección SQL.

[33] Michael D. Bauer. Seguridad en servidores Linux, Ataques pasivos vs ataques activos. [Sitio Web] España: ITCA-FEPADE, [Consulta 13 octubre de 2020], Disponible en: https://virtual.itca.edu.sv/Mediadores/cms/u46_ataques_pasivos_vs_ataques_activos.html

[34] Ramiro, R. (20 de enero de 2018). ciberseguridad.blog. Recuperado el 20 de octubre de 2020, de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/
Ruiz, J. J. (13 de diciembre de 2018). Red de Seguridad. Recuperado el 13 de octubre de 2020, de https://www.redseguridad.com/revistas/red/083/56/index.html

[35] Surmay, L. (10 de agosto de 2020). www.gb-advisors.com. Recuperado el 13 de octubre de 2020, de https://www.gb-advisors.com/es/estos-son-los-5-tipos-de-ciberataques-mas-comunes/

[36] CONVERSIA. Tipos de ciberataques: más allá del ransomware. [Sitio Web] España: www.consultoria-conversia.es. [consulta 13 octubre de 2020], Disponible en: http://www.consultoria-conversia.es/internet/tipos-ciberataques-infografia-ransomware/

La Asociación Colombiana de Ingenieros de Sistemas (ACIS, 2020) hace mención de los reportes y análisis de la empresa especialista en ciberseguridad Check Point Software Technologies Ltd, quien alerta sobre aumento del 178% de los ataques por parte de los cibercriminales a las organizaciones gubernamentales, infraestructuras críticas, instituciones de salud, proveedores de servicios y usuarios finales a comparación de las organizaciones a nivel mundial y estos son perpetuados a través de correos electrónicos[37]

Por lo anterior se requiere que las organizaciones implementen diferentes estrategias para fortalecer la seguridad informatica, es por ello que una de la forma para fortalecer la ciberseguridad es la ciber inteligencia teniendo que dentro de sus proceso se realiza actividades de recolección de información del ciberespacio y el análisis de la misma permitiendo conocer las amenazas para anticipar los riesgos en una organización es por ello (LISA Institute, 2020) cita el término que brinda el Centro Tecnologías Emergentes de la Universidad Carnegie Mellon, donde define la ciberinteligencia como “La adquisición y el análisis de información para identificar, rastrear y predecir las capacidades, intenciones y actividades cibernéticas que apoye la toma de decisiones”[38], para el desarrollo de la ciberinteligencia se debe implementar el ciclo de inteligencia pero con el enfoque hacia el ciberespacio como lo sugiere(Candau, 2017)[39] al momento que el ciclo de ciberinteligencia debe satisfacer los objetivos de identificar las fortalezas y vulnerabilidades del cliente, así como lograr identificar las fortalezas técnicas, conocimientos e infraestructura tecnológica usada por el cibercriminal, permitiendo así conocer los cibercriminales, quien es su enemigo, al momento de conocer sus enemigo puede establecer una

[37] OJALVO, Check Point Software Technologies Ltd. Check Point Software alerta sobre “La nueva normalidad” para la próxima crisis global: la ciber pandemia [Sitio Web). Colombia, Asociación Colombiana de ingenieros de Sistemas ACIS [Consultado 22 Octubre de 2022], Disponible en: https://acis.org.co/portal/content/check-point-software-alerta-sobre-%E2%80%9Cla-nueva-normalidad%E2%80%9D-para-la-pr%C3%B3xima-crisis-global-la

[38] LISA Institute. ¿Qué es y para qué sirve la Ciberinteligencia? [Sitio Web]España: Ministerio de Interior y lisainstitute. [Consulta 9 octubre de 2020], Disponible en:https://www.lisainstitute.com/blogs/blog/ciberinteligencia-que-es-y-para-que-sirve

[39] Candau, J. (2017). redseguridad. Recuperado el 13 de octubre de 2020, de https://www.redseguridad.com/revistas/red/079/52/

estrategia para minimizar los riesgo como lo indica (TZU, 2003)[40] en su libro el arte de la guerra al mencionar Si conoces a los demás y te conoces a ti mismo, ni en cien batallas correrás peligro.

Para lograr estos objetivos que establecer (Candau, 2017) mediante el ciclo de inteligencia se debe realizar los siguientes actividades como lo señala (Centro Criptológico Nacional, 2015) en su guía de seguridad CNN-STIC-425, al mencionar las fases que son la Dirección y planificación, Recolección, Transformación, Análisis y producción, Difusión y Evaluación[41], también el (Ejercito Nacional Colombia 2017)[42], implementa el proceso de inteligencia donde desarrolla cuatro pasos, que consiste en, Planeamiento y Dirección, Recolección de información, Procesamiento, Difusión y Retroalimentación, para ello también tiene dos actividades continuas dentro del mismo proceso que consiste en analizar y evaluar, el cual les permite en el ejercito a los comandante la toma de decisiones que permitan cumplir con sus misión constitucional con el proceso de inteligencia en el ciberespacio, se lograra emitir informes de nivel técnico, operacional, táctica y estratégica, de acuerdo cada nivel[43], generando un engrane para que se permita la toma de decisiones por parte de los directivos, ejecutivos y responsables de la seguridad en las empresas según sea el caso.

[40] TZU, S. El Arte de la Guerra [Sitio Web] Argentina: Biblioteca Virtual Universal [Consulta 18 octubre de 2020], Disponible en: https://biblioteca.org.ar/libros/656228.pdf

[41] Centro Criptológico Nacional CCN. Guía de Seguridad (CCN-STIC-425) Ciclo De Inteligencia y Análisis de Intrusiones. [Sitio Web] España: Ministerio de la Presidencia. [Consulta 17 de Octubre de 2020], Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html

[42] Ejército Nacional. Manual Fundamental de Referencia de Inteligencia, Proceso de inteligencia. [Sitio Web]. Bogotá: CEDOE. [Consulta Octubre de 2020], Disponible en: https://www.dicoe.mil.co/recurso_user/doc_contenido_pagina_web/800130633_4/458748/mfre_2_0_inteligencia.pdf

[43] Portillo, I., & Gonazalez, G.Monta la NSA en tu casa, Inteligencia aplicada al mundo Ciber[Sitio Web]. HonyCon 4 edición, [Consulta 18 Octubre de 2020], Disponible en: https://doplayer.es/140691341-Monta-la-nsa-en-tu-casa-inteligencia-aplicada-al-mundo-ciber.html

5 LAS PRINCIPALES CIBERAMENAZAS EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

Para describir las amenazas existentes en el ciberespacio que pueden afectar la seguridad informática en las instituciones de educación superior se debe identificar cuáles son las amenaza cibernética o ciberamenazas existentes en el ciberespacio, para ello toma como referencia el (Gobierno de España 2019)[44] en la estrategia nacional de ciberseguridad del año 2019, cuando menciona que el ciber espionaje es una amenaza que permiten realizar diferentes y múltiples ataques sobre un objetivo específico mediante el usos de APT “Amenazas Persistentes Avanzadas” logrando mantener de forma continua las acciones que requiere los principales actores contra el adversario, también hacen mención a los las diferentes organizaciones como las corporaciones u organismos del estados, según (CISDE 2016)[45] usan este tipo de modalidad con el fin de anticiparse frente a sus adversarios o competidores, para ello requieren usar las técnicas como el hackeo, crakeo y malware, para la obtención de información de acuerdo a cada caso de estudio, (Torre 2016) hace mención de los posibles efectos del ciber espionaje al realizar la siguiente afirmación “Los gobiernos, las agencias de seguridad y otras entidades públicas y privadas suelen hacer uso de estos métodos, vulnerando los derechos sobre la identidad digital y la privacidad de los ciudadanos[46]”, dando lugar al ciber espionaje como un delito estipulado en la ley 1273 de 2009 de delitos

[44] Gobierno de España. Estrategia Nacional de Ciberseguridad[Sitio Web]. España CCN-CERT.[Consulta 08 Noviembre de 2020],Disponible en: https://www.ccn-cert.cni.es/pdf/documentos-publicos/3809-estrategia-nacional-de-ciberseguridad-2019/file.html

[45]CISDE. La amenaza cibernética: ciberguerra y ciberdefensa [Sitio Web] España: CISDE Observatorio.[Consulta 8 Noviembre de 2020], Disponible en: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/

[46] Torre, M. S. Ciberespionaje: una nueva forma de ataque y de defensa cibernética [Sitio Web].Barcelona: Universitat Pompeu Fabra Barcelona. [Consulta 22 Noviembre de 2020],Disponible en:https://www.upf.edu/web/antenas/el-neologismo-del-mes/-/asset_publisher/GhGirAynV0fp/content/ciberespionaje-una-nueva-forma-de-ataque-y-de-defensa-cibernetica?__cf_chl_captcha_tk__=pmd_qG85Y3yV3y88y0XtaK85QE9AUGQPcGMBTzHlyr.DD2g-1634611870-0-gqNtZGzNA5CjcnBszQil#.YW4yvhrMJEY

informáticos en Colombia, (Ramos y AUSAPE 2019)[47] hace alusión que las empresas, organizaciones e instituciones logran obtener ventaja competitiva frente a sus rivales mediante la amenaza del ciber espionaje.

Como ejemplo del ciber espionaje en instituciones de educación superior podemos mencionar el ocurrido en el mes de septiembre del 2022 en la Universidad Politécnica del Noroeste en Xi'an, quien recibió mil ataques informáticos a través de 40 herramientas de software maliciosos y diferentes vectores de ataque como correo electrónico con phishing y donde al parecer se filtro 140 gigabyte de información, esta universidad es de gran importancia ya que realizar investigación aeronáutica y espacial[48].

También podemos encontrarnos las amenazas Hibridas, de acuerdo a (LISA Institute 2019)[49] son aquellas que aprovechan las vulnerabilidades del ciberespacio y permiten realizar acciones militares, ciberataques, operaciones de manipulación de la información y presión económica, según (Albors y Arroyo 2019)[50] las amenazas hibridas hacen uso de varios fenómenos que permiten generar amenazas complejas y multidimensional en los diferentes sectores como los políticos, sociales y económicos, estas amenazas hibridas se viene implementando mediante el uso de fusión de técnicas y herramientas tecnológicas maliciosas logrando fortalecer los vectores de ataque, permitiendo ser más eficaces y exactos al momento de realizar algún tipo de ataque hacia las organizaciones e instituciones,

[47] SECCON MAGISTRA CIBERSEGURIDAD AUSAPE, Ramos, A., & AUSAPE. Ciberespionaje en organizaciones [Sitio Web]. España: AUSAPE Youtube. [Consulta 22 Noviembre de 2020], Disponible en: https://www.youtube.com/watch?v=0gl2FQHzgOQ&ab_channel=AUSAPEVideos

[48] XINHUA ESPAÑOL, China condena enérgicamente ciberataques de EEUU contra Universidad Politécnica del Noroeste de China. [Sitio Web] China: spanish.news.cn [Consulta 30 Octubre de 2022] Disponible en: https://spanish.news.cn/20220906/9484b9da5a674ed8b2f2445b368555af/c.html

[49] LISA Institute, Qué es la Guerra Híbrida y cómo nos afectan las Amenazas Híbridas. [Sitio Web].España: LISA Institute. [Consulta 8 Noviembre de 2020], Disponible en: https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas.

[50] Albors, J., & Arroyo, R. Cada Vez funcionan mejor las amenazas hibridas [Sitio Web]. España: Youtuber ESET. [Consulta 22 noviembre de 2020], Disponible en: https://www.youtube.com/watch?v=-meAWpbjRko&ab_channel=ITTelevisi%C3%B3n

estas amenazas hibridas no poseen ninguna restricción legal, moral al momento de actuar frente a una organización logrando buscar desestabilizar la institucionalidad de una nación u organización ya que está amenaza permanece de forma anónima, esto lo podemos evidenciar de acuerdo a lo mencionado por (V. P. Navarro 2020)[51] cuando menciona el ataque desarrollado por Rusia a Estonia en el año 2007.

La cibercriminalidad se trata de un enfoque de seguridad ciudadana, donde pueden ser víctimas diferentes instituciones, empresas y ciudadanos, donde hacen el usos del ciberespacio para realizar actividades ilícitas como el fraude, el robo, chantaje, entre otros, los cuales pueden afectar el bien jurídico mediante el uso de herramientas tecnológicas[52], entre las herramientas tecnologías maliciosas que podemos mencionar se encuentra el malware, Botnet's, Cryptojacking, Ransomware, malware, phishing, entre otros[53], aprovechando las nuevas tecnologías como la conexión 5G, Internet de las cosas (IoT) e Inteligencia Artificial, permitiendo generar mayor impacto, velocidad y exactitud en las actividades de los criminales en el ciberespacio.

Dentro de las ciber amenazas se encuentra el ciberterrorismos, los cuales pueden desarrollar o ejercer terror en un ambiente físico o virtual hacia la población civil o a las personas, así como lo indica (CISDE 2016) cuando cita el significado de ciberterrorismo por parte del FBI "el ataque premeditado y políticamente motivado contra información, sistemas computacionales, programas de computadoras y datos que puedan resultar en violencia contra objetivos no combatientes por parte de

[51] Navarro, V. P. Amenazas Hibridas: Las nuevas tecnologías como instrumentos de Guerra.[Sitio Web] España, Barcelon: UNITEDEXPLNATIONS. [Consulta 23 Noviembre de 2020], Disponible en: https://www.unitedexplanations.org/2020/01/13/amenazas-hibridas/

[52]CISDE. La amenaza cibernética: ciberguerra y ciberdefensa [Sitio Web] España: CISDE Observatorio.[Consulta 8 Noviembre de 2020], Disponible en: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/

[53] INTERPOL, Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. [Sitio Web].España; INTERPOL. [Consulta 23 Noviembre de 2020], Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

grupos subnacionales o agentes clandestinos"[54], como cuando ocurrió el ataque masivo de Ransomware en el año 2017, los cuales afecto a los sistemas informáticos, secuestrando la información, comprometiendo los sistemas informáticos y generando caos a nivel mundial, la amenaza de ciberterrorismo está ligado desde actividades no penales hasta actividades criminales como lo indica (Lux 2018) cuando hace referencia del terrorismo "Just like a "terrorist", a "cyberterrorist" can also engage in a wide range of activities online, ranging from non-criminal, to criminal but not terrorist, through to terrorist in nature"[55].

Las acciones del ciberterrorismo según (Lux 2018)[56], se encuentran enfocadas desde una perspectiva tradicional de la planificación, la conspiración, comprometiendo las Redes SCADAS mediante el uso de las tecnologías, así como desarrollar ataques de denegación de servicios a sistemas de cómputo y dañar o destruir sistemas de infraestructura critica que afecte de forma masiva a grupos de personas. Otra de la forma de desarrollarse las amenazas del ciberterrorismo mediante la modalidad de actividades en secuencias de forma creciente desde el acceso a sistemas informáticos para la captación y destrucción de información hasta la ejecución de ataques a infraestructura críticas, generando daños o afectación al sector físico.

De igual forma se puede mencionar que gran parte de los ataques perpetuadas por los cibercriminales en los Estados Unidos en el año 2010 fueron desarrollados por los denominados Insider, son aquellas personas que hacen parte de la organización

[54]CISDE. La amenaza cibernética: ciberguerra y ciberdefensa [Sitio Web] España: CISDE Observatorio.[Consulta 8 Noviembre de 2020], Disponible en: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/

[55] Lux, L. M. Defining cyberterrorism, [en línea]. Scielo, Revista chilena de derecho y tecnología, vol.7 nro.2 Santiago Diciembre. 2018. [Consultado 08 noviembre de 2020] ISSN 0719-2584 doi:10.5354/0719-2584.2018.51028, disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005&lng=en&nrm=iso&tlng=es

[56] [56]CISDE. La amenaza cibernética: ciberguerra y ciberdefensa [Sitio Web] España: CISDE Observatorio.[Consulta 8 Noviembre de 2020], Disponible en: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/

en la que trabajan, los cuales aprovechan el acceso a los sistemas de información, facilitando destruir o robo de la información, no necesariamente son hacker los Insider, solo son personas que tiene un interés o atienden un interés para un tercero aprovechando su estatus o posición en la organización, a diferencia del hacking, que son personas que acceden a los sistemas informáticos a través de las redes de comunicación evadiendo los sistemas de protección, violando la reserva de la información[57].

No se debe olvidar el hacktivismo, según (Rochina 2016)[58] los hacktivista pueden realizar ciberataques mediante uso de herramientas disponibles en el internet por motivos ideológicos para generar impactos sociales o desarrollar presión política, las técnicas más comunes es el Doxing, esta técnica permite encontrar, compartir y publicar información de personas en sitios web, otras de la técnica es la Denegación de servicio (DoS) y/o denegación de servicios distribuido (DDoS) las cuales permiten desarrollar ataques para inhabilitar servicios web de organización públicas o privada que se encuentren en desacuerdo, o no tiene finalidad con la misionalidad u objetividad de la comunidad activista, así como la destrucción o secuestro de páginas web mediante el acceso no autorizado de las redes sociales de los objetivos o contraparte de la organización, al momento de acceder a estas cuentas de redes sociales logran realizar alteración de la información, incrustar fake new o noticias falsa, así como hacer publicación de información con clasificación reservada, De igual forma esta amenaza desarrolla actividad de violación de información, logrando la suplantación o clonación de perfiles en el ciberespacio para desarrollar delitos informáticos.

---

[57] Miró Llinares, F. *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio.*[En línea] Elibro Marcial Pons Ediciones Jurídicas y Sociales [Consultado 22 de abril de 2022], Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/58741?page=57

[58] Rochina, P. Hacktivismo: ¿Qué hay detrás de este movimiento activista? [en línea]. España Revista digital INEMSE. [Consultado 23 de Noviembre de 2020], Disponible en: https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

Durante la descripción de las principales amenazas del ciberespacio que afectan la seguridad informática y de la información en los institutos de educación se logra caracterizar las ciberamenazas mediante el cuadro 1, permite la relación entre las acciones que desarrollan las amenazas en el ciberespacio, sus técnicas, herramientas, vectores de ataque, y su relación con los delitos informáticos.

Cuadro 1 Ciberamenazas, Acciones y técnicas de ataques

CIBERAMENAZAS	ACCIONES EN EL CIBERESPACIO	DELITOS EN EL CIBERESPACIO	TECNICAS - HERRAMIENTAS – VECTOR DE ATAQUES
Ciberespionaje	Amenazas Avanzadas Persistentes	Robo de información	Hackeo Adware Sqlinjection
		Acceso no Autorizado Sistemas de información	Malware
		violación Propiedad Intelectual	
		Clonación de tecnología	Phishing
Amenazas Hibridas	Acciones Militares	Secuestro Digital	Ransomware
	Ciberataques	Acceso no Autorizado Sistemas de información	Phishing
	Manipulación Información	Desinformación	Fake new - deep fakes
	Sabotaje	extorsión	Malware
Cibercrimen	Ciberterrorismo	Financiación al terrorismo	Criptomonedas
		Ataques cibernéticos	Ransomware
			DDOS - DOS
		Ataques infraestructura critica	Malware - Troyanos
			Botnes
	Ciberdelitos	extorsión	Ransomware
		Secuestro Digital	
		Lavado de Activos	Cryptojacking
			Botnes
		Falsificación Medios Pagos Electrónico	Phishing - Malware - clonación
		Pornografía Infantil	Cyberbulling
		Piratería informática	Cracking
		Prestación de servicios ilícitos	Deep WEB - Dark Web
Hacktivismo	Ciberataques	Denegación de Servicios	DDoS - DoS
	Manipulación Información	Desinformación	Fake new - deep fakes
	Difusión de información datos personales	Violación de Datos	Doxing
	Acosos cibernéticos	Robo de identidad – Suplantación	Cyberbulling

Fuente: elaboración propia 23 de noviembre de 2020

Estas ciberamenazas pueden ser ejecutadas por los hacker, teniendo en cuenta que aquellas personas que tienen conocimiento avanzado en tecnología y hacen del uso de las herramientas tecnológicas para acceder sin autorización de forma remota a los sistemas de información y de comunicaciones como el uso backdoor, las Amenazas Avanzadas Persistentes para la violación de datos, el malware para el secuestro de la información, alteración, extorción o eliminación de la información, generando sabotaje cibernético en las organizaciones de Instituciones de educación superior.

Durante la descripción de las amenazas del ciberespacio logramos identificar los diferentes tipo de vectores de ataque o herramientas tecnológicas maliciosas, que pueden usar los cibercriminales para la realización de ataques a las instituciones de educación superior publica, como lo indica (Deloitte 2018)[59] cuando hace referencia que la fuga de información se desarrolla mediante los vectores de ataque de ingeniería social, Phishing, robo de credenciales, DDoS, generando riesgos de perdida de integridad, inaccesibilidad de la información y fraude, lo cual podemos hacer referencia que estos ataques cibernéticos son producidos al parecer por amenazas del cibercrimen, ya que en ellos son los más interesados para obtener información digital y ser ofrecida en el ciberespacio al mejor postor.

De acuerdo a los reportes realizados por (Check Point, 2022), los cibercriminales hacen uso de las familias de códigos malicioso en America son el Trickbot, Remcos, Formbook y Phorpiex, así mismo las amenazas cibernéticas hacen uso de los protocolos de distribución de código malicioso a través de páginas web y correos electrónicos a través de archivos maliciosos con formatos de archivo (.exe, .xls, .pdf, .doc), identificando unos de los métodos y técnicas para realizar ataques

[59] Deloitte. Estudio de Ciberseguridad, Principales Universidades de España.[Sitio Web].España Deloitte Advisory. [Consultado 23 Noviembre de 2020], Disponible en: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Ciberseguridad-Universidades.pdf

cibernéticos[60], generando un aumento del 29% de ciberataques al sector educativo e investigación en el año 2021, así mismo en comparación del año 2021 y año 2022 a nivel global el sector de educación e investigación es el sector con mayor ataque con mil seiscientos cinco ataques por organización por cada semana con un aumento del 75% frente al año anterior, teniendo en cuenta que los vectores de ataques más utilizados Archivos maliciosos en páginas web y correos electrónicos[61].

En Colombia podemos mencionar algunas ataques cibernéticos generados por cibercriminales, entre los incidentes informáticos ocurridos se encuentra la Universidad del Tolima en el año 2018 donde fue afectado el principio de la Integridad de la información mediante la modificación de las notas del segundo semestre del 2017, así lo anuncio la FM en su página de internet[62], la Universidad de los Andes también fue comprometida por un ataque cibernético en el año 2016 y el año 2021, así lo menciono el periódico Al Derecho donde indican que el último incidente informático ocurrido en el 2021 fue a través del software malicioso de tipo Ransomware y distribuido través de la extensión de Nukak[63]; la revista Forbes Colombia menciona también que la universidad del Bosque fue hackeada en el mes de junio del 2021, al parecer fue comprometidas las plataformas académicas y financieras, logrando afectar aproximadamente 48 horas sus labores en las

[60] Check Point Research, Cyber Security Report, 2022, "Informe Sobre Seguridad 2022, Capitulo 5 Estadísticas Globales." [Sitio Web] Israel, https://www.checkpoint.com/ [Consultado 22 Octubre de 2022], Disponible en: https://www.checkpoint.com/downloads/resources/cyber-security-report-2022-ES.pdf?mkt_tok=NzUwLURRSC01MjgAAAGHoQ6BgFtqenMmlAbU7Un1emeotHIblvJBNzmJ0wMhmgjtNFNmZTH07tzEdYuWWbMg_db1PXVJj3oWuYorv98I9f8cgUowQNIXeW7FyAvA8mdWvah7

[61] Check Point Research, Cyber Security Report, 2022, "Informe Seguridad Cibernética 2022, Capitulo 5 Estadísticas Globales." [Sitio Web] Israel, https://www.checkpoint.com/ [Consultado 22 Octubre de 2022], Disponible en: https://go.checkpoint.com/security-report/page-global-malware-statistics.php

[62]La Fm, Hackearon sistema de Universidad del Tolima y modificaron notas de estudiantes [en Linea] Colombia, La FM radio, [Consultado 24 de Octubre de 2022] Disponible en: https://www.lafm.com.co/colombia/hackearon-sistema-de-universidad-del-tolima-y-modificaron-notas-de-estudiantes

[63] Universidad, Periódico Al Derecho, 2021 "Ataque Informatico a la Universidad de los Andes ¿Qué hacer para protegerse?"[Sitio Web] https://alderecho.org, Colombia, [Consultado 29 octubre 2022], Disponible en: https://alderecho.org/2021/04/14/ataque-informatico-a-la-universidad-de-los-andes-que-hacer-para-protegerse/

plataformas tecnológicas[64], así mismo la universidad Pontificia Universidad Javeriana recibió un ataque cibernético en las sedes ubicadas en las ciudades de Bogotá y Cali, estos hechos fueron comunicados a través de la circular No 19 de fecha 22 de Noviembre de 2021[65], estos ataques cibernéticos se encuentra en procesos de investigación bajo el marco de la Ley 1273 de 2009.

De acuerdo con las consultas realizadas en las diferentes fuentes de información abiertas, como bases de datos de bibliotecas virtuales, repositorios de universidades, revistas tecnológicas, Centros Cibernéticos, entre otros, se logra evidenciar solo cuatro reportes de incidentes informáticos de Instituciones de educación Superior en Colombia entre ellas la Universidad del Tolima, Universidad de los Andes, Universidad el Bosque y la Universidad Javeriana, pero al realizar la comparación frente a los ataques cibernéticos a nivel global, el sector educación recibe un promedio de mil seiscientos cinco ataques por organización cada semana, adicionalmente el mapa de índice de amenaza global del reporte de Checkpoint indica que Colombia cuenta con un 52.6% de Riesgo y que se encuentra en la clasificación No 21[66].

De igual forma el Profesor asociado Jeimy Cano de la Universidad del Rosario, indica que el presupuesto destinado a la seguridad digital es de menos de 1% de las ventas de acuerdo al informe de Impacto de los Incidentes de Seguridad Digital del 2017, realizado por la OEA, El banco interamericano de Desarrollo y el Ministerio

[64]Forbes Staff, Universidad El Bosque dice logró recuperar todas sus plataformas digitales, tras hackeo general [en Linea] Colombia. Forbes Colombia, [Consultado 24 de Octubre de 2022] Disponible en: https://forbes.co/2021/07/01/actualidad/universidad-el-bosque-que-dice-logro-recuperar-todas-sus-plataformas-digitales-tras-hackeo-general/

[65] Adriana Diaz, Pontificia Universidad Javeriana, Información de Prensa, [En linea] Bogotá, https://javeriana.edu.co [Consultado 30 Octubre de 2022] Disponible en: https://www.javeriana.edu.co/recursosdb/20125/724951/22-11-2021+Comunicado+de+prensa+-+Seguridad+informa%CC%81tica+Javeriana.pdf/a37fa6b9-3140-9d3f-58bb-df991857a9b2?t=1637602154780

[66] Check Point Research, Cyber Security Report, 2022, “Informe Seguridad Cibernética 2022, Capitulo 5 Estadísticas Globales.” [Sitio Web] Israel, https://www.checkpoint.com/ [Consultado 22 Octubre de 2022], Disponible en: https://go.checkpoint.com/security-report/page-global-malware-statistics.php

de Tecnológica de información y Comunicaciones[67], logrando identificar que gran parte de las organizaciones incluida el sector Educación no cuenta con un adecuado sistemas de seguridad informática e información, personal idóneo y especializado en seguridad informática e infraestructura que permita identificar, minimizar y mitigar los incidentes de seguridad de información los cuales afectan los sistemas y recursos informáticos de la IES.

[67]Jeimy Cano, Colombia no está preparada ante un ciberataque, [Sitio Web] Colombia: Universidad del Rosario, https://www.urosario.edu.co/ [Consultado 28 septiembre 2022], Disponible en: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

6 PROCESO DE INTELIGENCIA EN EL CIBERESPACIO COMO ESTRATEGIA PARA LA SEGURIDAD DE INFORMACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

Para el desarrollo del análisis de las diferentes amenazas, prevenir, gestionar, minimizar y mitigar las acciones de las diferentes amenazas del ciberespacio, se debe implementar el proceso de inteligencia con el fin que las instituciones de educación superior logren conocer el comportamiento de las amenazas y con ello realizar una adecuada toma de decisiones que permitan contrarrestar los riesgos del ciberespacio.

Dentro de las fases del ciclo de inteligencia en el ciberespacio se debe realizar la dirección y planificación, recolección de información, transformación, análisis y producción, difusión y evaluación, estas fases del ciclo de inteligencia se debe desarrollar de forma ordenada, cíclica, dinámica y permanente, la fase de evaluación se debe realizar en cada una de las fases, es decir se debe realizar evaluación en la fase de dirección y planificación, así como la evaluación en la recolección de información, así sucesivamente en cada una de las cinco fase del ciclo de inteligencia[68].

Para el desarrollo de la fase de Dirección y planificación del ciclo de inteligencia en el ciberespacio se debe conocer y entender la misión de la institución, así como el problemática del entorno digital, para ello se debe determinar cuáles son los requisitos u objetivos a trabajar, así mismo se debe establecer como se va desarrollar las actividades que permitan cumplir los objetivos para la recolección de información que permitan el análisis de los datos y generar inteligencia del ciberespacio [69].

[68]Centro Criptológico Nacional CCN. Guía de Seguridad (CCN-STIC-425) Ciclo De Inteligencia y Análisis de Intrusiones. [Sitio Web] España: Ministerio de la Presidencia. [Consulta 17 de Octubre de 2020], Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html

[69] Ibid., p.7.

Para ellos vamos a establecer los requisitos que se debe cumplir para analizar los ciberdelincuentes, donde debe contestar los interrogantes, quien, que, porque, cuando, donde, como, por ello debemos tener los sientes requisitos, así:

- Identificar los objetivos que pueden tener como intereses los cibercriminales en las instituciones de educación superior pública.
- Cuáles son los métodos de ataque más usados y efectivos desarrollados por los cibercriminales en las instituciones de educación superior pública.
- Cuáles son las características y estructura que poseen las herramientas y ataques que poseen los cibercriminales.
- Cuáles pueden ser los posibles daños que puede ocasionar los atacantes.

Como segundo paso del proceso de inteligencia en el ciberespacio, es la recopilación de datos e información, para la recolección de información podemos contar con varios fuente de recolección de información, El (Gobierno de España 2019) a través de la guía de seguridad (CCN-STIC-425) hace mención la inteligencia geoespacial, inteligencia humana, Inteligencia de fuente abiertas, inteligencia de señales, entre otras, permitiendo tener un contexto amplio de las características de las amenazas existente en el ciberespacio, así como su evolución a través del tiempo y avances tecnológicos.

Es de destacar la inteligencia de fuentes abiertas (OSINT), permite obtener información de medios de comunicaciones, datos públicos, literatura gris, de igual forma podemos contar con la inteligencia de señales las cuales están integrada por inteligencia de comunicaciones, Inteligencia electrónica, Inteligencia de señales, brindando gran cantidad de datos e información que transitan en el espectro electromagnético [70].

[70] Ibid., p.8.

Por lo anterior, la información recolectada durante el proceso de inteligencia es desarrollar un adecuado tratamiento y/o procesamiento de la información, el tratamiento de los datos tiene como finalidad de convertir los datos en información de valor que permita el análisis de la información y generar inteligencia predictiva para la toma de decisiones en los niveles técnicos, operativos y estratégicos. Para ello se debe contar con medios humanos y tecnológicos que logren realizar la transformación de los datos, es de resaltar que los medios humanos deben tener habilidades, destrezas y capacidades que permitan transformar la información, así mismo los especialistas dependen de herramientas tecnológicas que faciliten desarrollar tareas de forma más ágil y precisa, unos de los ejemplo que indica (Gobierno de España 2019) en la guía de seguridad, cuando menciona tareas para tratamiento de datos, hace referencia a traducir textos de diferentes idiomas, descifrar información como contraseñas, conversión de datos telemétricos[71]; dentro de las técnicas de tratamientos de los datos podemos encontrar como lo menciona (Gobierno de España; Ministerio de Industria, Energia y Turismo 2017) en su guía uso de herramientas Básicas de tratamientos de datos cuando hace mención del DATA CLEASING (limpieza de datos), DATA WRANGLING (transformación de datos) y del RECORD LINKAGE (enlace de datos), logrando que los datos existentes se encuentra de forma adecuada, utilizable y con formatos de estructura HTML, CVS, XLS.

Para la implementación del tratamiento de los datos es de gran importancia el uso de herramientas que faciliten desarrollar las técnicas de data Cleasign, data wrangling y record, por ello (Ministerio de Hacienda y Administracion Publica de España 2014) en su decálogo denominado “Reutilizado de datos del sector público” menciona Open Refine o Data Wrangler como herramientas de tratamientos de

[71] Ibid., p. 9.

datos[72], permitiendo generar información útil para el siguiente paso del proceso de inteligencia en el ciberespacio “análisis de la información”.

El análisis y producción de la información es unos del paso más importante del proceso de inteligencia del ciberespacio ya que mediante un adecuado procesamiento, análisis, evaluación e integración de información permite generar el producto final que es la inteligencia, la producción de inteligencia es de gran importancia para la seguridad de informática en las instituciones de educación superior, permitiendo predecir las posibles amenazas, vulnerabilidades y riesgos que se encuentra sometida la organización educativa, permitiendo satisfacer las necesidades de reducir los riesgos actuales y del futuro.

Según (Centro Criptológico Nacional 2015, 10) en la guía de seguridad CCN-STIC-425 del Ciclo de Inteligencia y Análisis de Intrusiones hace una pequeña descripción del esquema que implementan los analista de ciberintelgencia con los datos recopilados al mencionar los siguiente pasos, “ Los analistas reciben información de entrada, evalúan tal información –poniéndola, incluso, frente a otra información previa o a su propia experiencia personal-, elaboran un “estado de situación” de la actividad bajo análisis y, en último lugar, realizan un pronóstico respecto de lo que es presumible esperar y de la tendencia futura”[73], dentro del análisis y procesos de la información desarrollados cabe aclarara que la inteligencia producida por los analistas del ciberespacio no es totalmente absolutas, los entornos tecnológicos poseen un escenario VICA (Volátil, incertidumbre, complejo y ambiguo) como lo denomino (J. M. Navarro 2018) director de Ciberinteligencia Estratégica en

[72] Ministerio de Hacienda y Administración Publica de España. Decálogo Reutilización de Datos del Sector Publico. [Sitio Web] España: Ministerio de Hacienda y Administración Publica. [Consulta 18 septiembre de 2021]. Disponible en: https://datos.gob.es/sites/default/files/guia-decalogo-reutilizador-opendata.pdf

[73] Centro Criptológico Nacional CCN. Guía de Seguridad (CCN-STIC-425) Ciclo De Inteligencia y Análisis de Intrusiones. [Sitio Web] España: Ministerio de la Presidencia. [Consulta 17 de Octubre de 2020], Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html.

PROSEGUR Ciberseguridad[74], teniendo en cuenta con múltiples variables al momento de inferir en la predicción de los riesgos de la seguridad informática y de la información.

hay que tener en cuenta que existen diferentes tipos productos de inteligencia denominadas como la inteligencia actual, análisis de tendencia, evaluación de largo plazo, inteligencia estimativa, inteligencia de aviso, inteligencia de investigación, inteligencia científica y técnica, estos producto obtenidos por el análisis y procesamiento de la información hace referencia a los avances y madures según la capacidad de recolección y procesamiento de la información, cuando se iniciar a realizar ciberinteligencia los primeros productos que van obteniendo es el la inteligencia actual, ya que cuenta con información del día a día, a través del tiempo se logra obtener análisis de tendencia, ya que cuenta con mayor información procesada con antecedentes de los diferentes eventos que se han presentado en la organización, así como en otras entidades de educación superior, permitiendo realizar comparaciones con las diferentes información disponibles "OSINT, COMINT, SIGINT, HUMINT", entre otras que se encuentra en el espectro electromagnético, logrando obtener una evaluación de largo plazo que logra una base de conocimientos que permite identificar las tendencias de las amenazas de forma detallada, con ello llevar a generar la inteligencia estimativa y de aviso como recurso preventivos frente a los riesgos que pueden afectar la seguridad de las instituciones de educación superior de Colombia[75].

[74] Navarro, Jose Maria Blanco. Ciberinteligencia, La Via para la Ciberseguridad. [En Línea] España: Cuaderno de la Guardia Civil, nro. 57, 2018, ISSN 2341-3263 [Consulta: 18 septiembre de 2021].Disponible en: https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/img/local_repository/koha_upload/6a7214531a3239c800669262ea3d0b36_1%20CIBERINTELIGENCIA,%20LA%20V%C3%8DA%20PARA%20LA%20CIBERSEGURIDAD.pdf.

[75] Centro Criptológico Nacional CCN. Guía de Seguridad (CCN-STIC-425) Ciclo De Inteligencia y Análisis de Intrusiones. [Sitio Web] España: Ministerio de la Presidencia. [Consulta 17 de Octubre de 2020], Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html.

Dentro de los productos de inteligencia se encuentra la inteligencia investigativa e Inteligencia científica y técnica, con estas dos inteligencias permite desarrollar actividades que logran identificar el modus operandi de la amenaza, evaluando sus capacidades, características, técnicas y capacidad tecnológica, logrando apoyar procesos de investigación, desarrollo e innovación (I+D+I) en seguridad para los sistemas de información de las organizaciones académicas de nivel superior.

Dentro del análisis de la información se debe hacer uso de las técnicas cualitativas, cuantitativas y estructuradas o prospectiva como lo indica (J. M. Navarro 2018, 24), de igual forma indica el apoyo que puede brindar los análisis de riesgos, destacando la norma ISO 31000, NIST, The Kill Chain, modelo Diamante, así como las nuevas tecnologías convergentes como el Big Data, Machine Learning, Inteligencia artificial, redes neuronales, Deep learning, entre otras, con ello permitir generar acciones predilectas al tomador de decisión a nivel estratégico, operacional y técnico.

El paso de difusión y evaluación del proceso de ciberinteligencia, para el desarrollo de la difusión como primera medida se deben establecer los canales de comunicación adecuados que permitan la difusión de los informes de inteligencia a las partes interesadas y grupos de interés que permitan generar las tomas de decisiones a nivel estratégico, operacional y técnico que permita minimizar y mitigar los riesgos que se pueden presentar en los sistemas de información.

Para establecer los canales de comunicación nos debemos basarnos a los diferentes niveles de tomas de decisión que se encuentra establecidos como son los estratégicos, operacional y técnico, cada uno de estos niveles debe poseer su canal de comunicación teniendo en cuenta que cada una de ellas tienen características diferenciales que permiten la implementación de las medidas de seguridad a nivel políticas de seguridad e implementación a nivel técnico de sistemas perimetral de seguridad.

Los canales de comunicaciones disponibles que pueden implementar las instituciones de educación superior son los escritos, orales y tecnológicos, para ello se pueden hacer el uso de correos electrónicos instituciones, canales y mesas de ayuda intranet, redes sociales corporativas, video conferencia, reuniones, manuales, boletines, los cuales permitirán direccionar la información de acuerdo con la necesidades, requerimientos, solicitudes, repuestas e informes de inteligencia.

Dentro de los protocolos de los canales de comunicación con la alta gerencia se puede desarrollar a través de informes ejecutivos que permitan brindar la inteligencia obtenida frente a las amenazas y riesgos de la infraestructura de sistemas de información, así mismo se puede implementar el canal oral en el momento que se implemente reuniones y/o web conferencia facilitando las tomas de decisiones a nivel de políticas para la gestión de seguridad informática y asignación de roles.

Frente a los canales de comunicación hacia el nivel operacional que permita facilitar la difusión de las tomas de decisiones de la alta gerencia por motivos de la inteligencia generada, se puede implementar el uso de medios tecnológicos correo electrónico o medios audiovisuales, escritos a través de boletines y verbales mediante reuniones o capacitación, permitiendo una difusión y concientización los miembros de la organización.

A nivel técnico el canal de comunicación se debe garantizar que se implemente de forma bidireccional, permitiendo una continua retroalimentación entre las partes, permitiendo generar una constante evaluación del desarrollo de las políticas e implementación de las configuraciones técnicas que se implementan en los sistemas perimetrales, el informe que se brinda a los técnicos debe ser especifico donde indique las necesidades, requerimiento que se debe implementar en los dispositivos tecnológicos según la necesidad requerida para el fortalecimiento de los sistemas de información, estos informes se debe ser enviados a través de los

medios oficiales establecidos por el instituto de educación superior de forma escrita y autorizada por los altos directivos, y la validado por el director de seguridad de la información.

El desarrollo de los pasos de análisis, evaluación y difusión de la información de inteligencia es de carácter permanente, teniendo en cuenta que son pasos que se deben implementar en todo el proceso de inteligencia del ciberespacio de forma continua permitiendo mantener una visión más amplia de los datos, indicios, información e inteligencia.

7 ANÁLISIS DE HERRAMIENTAS DE RECOLECCIÓN DE DATOS PARA LA SEGURIDAD DE LA INFORMACIÓN

En el desarrollo del análisis de herramientas tecnológicas que permiten la recolección de información de las principales amenazas y métodos de ataques para explotar las vulnerabilidades de los sistemas de información de las instituciones de educación superior publica y que hace parte del paso o fase de búsqueda de información del proceso de inteligencia en el ciberespacio, la inteligencia de fuentes abiertas (OSINT) es unos de los métodos más importante de recolección de información para la seguridad de la información, OSINT se puede implementar las diferentes técnicas de recolección que se encuentra categorizadas como pasivas, semi - pasivas y activas, como ejemplo dentro de las técnicas de recolección de información en la categoría pasiva podemos hacer énfasis al mencionar cuando implementamos herramientas como Google D-ork o Google Hacking, frente a la categoría semi - pasivas hace referencia cuando se realizar búsquedas en Linkedin, esto significa que cuando una persona o amenaza se encuentra realizando esta búsqueda por likendin, linkendin genera un reporte al usuario final que alguien se encuentra realizando una consulta sobre el perfil de la plataforma y finalmente en la categoría de monitoreo activa podemos indicar que es cuando existe una interacción de forma directa con los servicios, dentro de las herramientas que podemos mencionar que genera esta interacción son las herramientas Osmedeus, Nmap, Nexus, OpenVas, para el desarrollo de recolección de información tanto activa como pasiva podemos se puede contar con la información disponible en el cuadro 2, que hace alusión a los tipo y herramientas de recolección de información OSINT para la ciberinteligencia.

Cuadro 2 Tipos y herramientas de Recolección de información OSINT.

N°	Tipo de recolección de información	Herramientas
1	Passive Foorprinting	Google Dork/Google Hacking
		TrueCaller
		Shodan
		Whois
		Robtex
		The Harvester
		Iplogger
		Google Search
		Anubis
		pwned?
2	Active Footprinting	Whatweb
		Maltego
		Wireshark
		Nmap
		Aircrak
		informática Forense
		Autopsy
		Wireshark
		Network Miner
		ExifTool
		Browser History
		OpenVas
		Nexxus
		Tinfoleaks "Twienter"
		Spiderfoot
		Metagoofil " Extacion Documentos"
		WayBackMachine
		Osintux
		FOCA

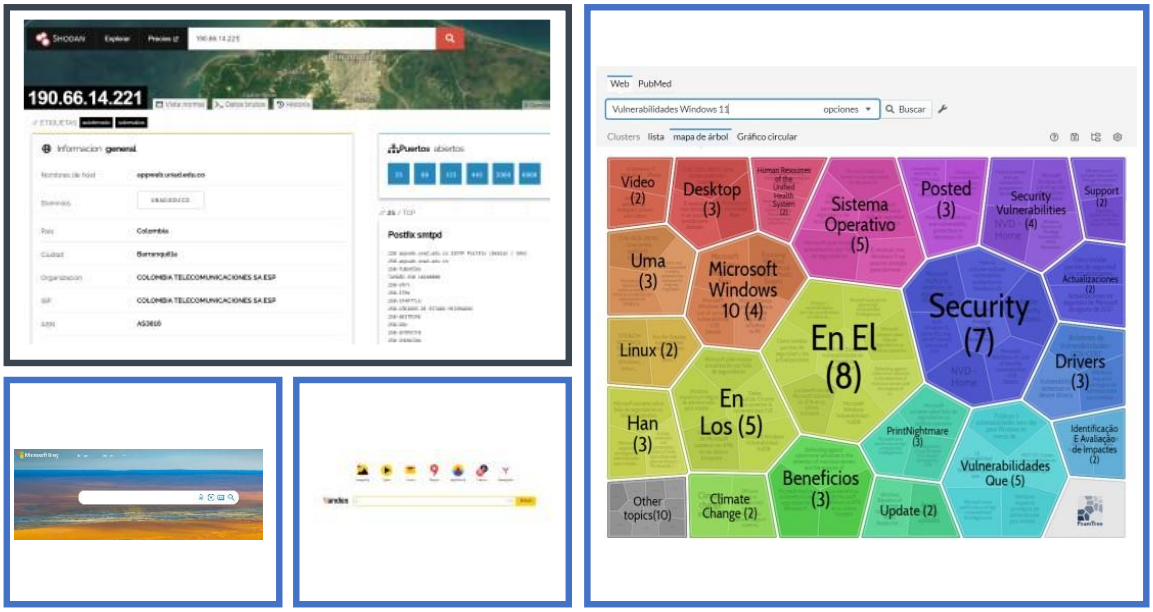
Fuente: Elaboración propia, 28 de septiembre de 2021.

Mediante el uso de técnicas de recolección de información en el ciberespacio a mediante las diferentes herramientas, permite identificar cuáles son los datos y documentos expuestos en la web que poseen las instituciones de educación superior en Colombia, para identificar las vulnerabilidades existentes en las IES se clasifican los tipos de activos tecnológicos que posee la organización educativa entre ellas se encuentra la organización que comprende los procesos y procedimientos, rutina de gestión, personal, ambiente físico, también se debe tener presente el ambiente físico y virtual los cuales se puede mencionar el hardware,

software, quipos de comunicaciones, Datos, Claves encriptadas, instalaciones, como lo menciona la norma técnica Colombiana ISO 27005.

El desarrollo de la inteligencia de fuentes abiertas en la categoría pasiva podemos hacer uso de los diferentes navegadores de internet como Google, Yandez, Bing, Shodan, carrot2, Baidu, como se puede apreciar en la figura 1, hace alusión a los diferentes Buscadores para la implementación de la inteligencia de fuente abiertas OSINT, logrando realizar de forma gráfica la visualización, obtención y filtrado de información disponible en la red insegura (Internet).

Figura 1 Buscadores para OSINT.

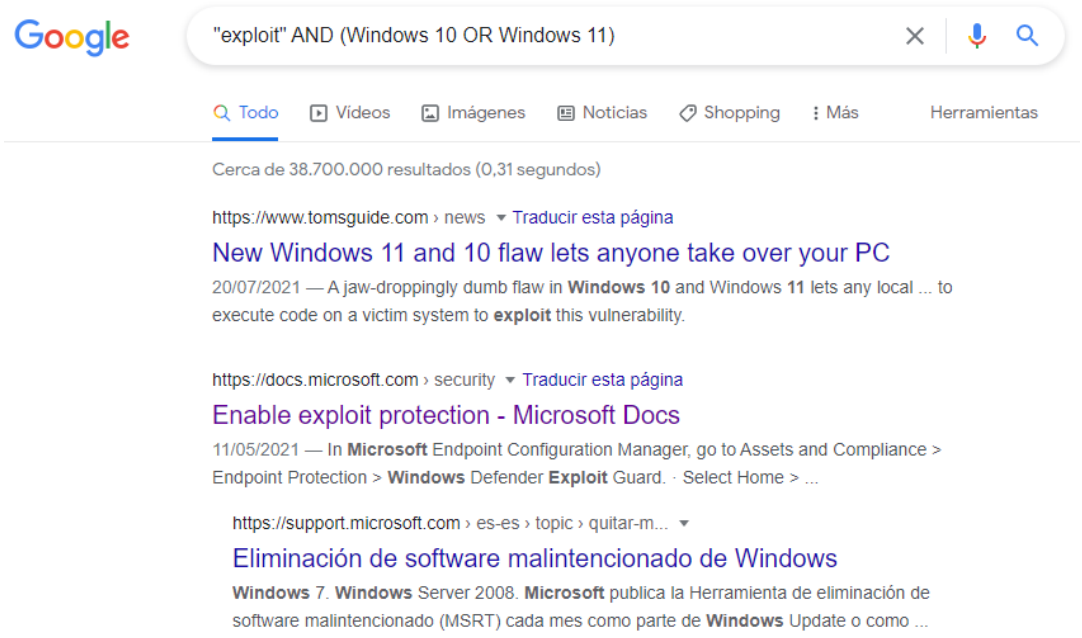


Fuente: Elaboración propia, 23 de septiembre de 2021

dentro de los navegadores se pueden realizar métodos de consultas que permitan obtener información de interés, muchas de los cibercriminales hacen usos de estas consultas avanzadas con el objetivo de identificar vulnerabilidades de los sistemas de información, unas de las consultas a implementar es el uso de las comilla, las comillas permiten hacer un énfasis especifica en la búsqueda teniendo en cuenta que tiene un límite de 10 términos, dentro de las búsquedas básicas se encuentra

el uso de paréntesis para la agrupación de palabras que requiera unir en una búsqueda, así como la implementación de operadores booleanos como AND, OR, NO[76], unos de los ejemplos que podemos implementar como búsqueda básica en la siguiente consulta, **"exploit" AND (Windows 10 OR Windows 11**), logrando obtener 38.700.000 resultados en 0.31 segundos, como se observa en la figura 2, se evidencia la implementación de la técnica de Google hacking implementada para OSINT, resultado de obtener información de interés en el ciberespacio, permitiendo identificar los tipo vulnerabilidades existentes, dicha información recolectada también puede ser utilizada por parte de las diferentes amenazas en contra de las instituciones de educación superior, dejando en evidencia la información disponible en la web, permitiendo anticipar y prevenir la ingeniería social o ciberataques por parte de las amenazas.

Figura 2 Búsqueda Básica de Google Hacking.



Fuente: Elaboración propia, 20 de septiembre del 2021

[76] LISA Institute. Navegadores y servicio Online de búsqueda Avanzadas, 2020/02, En Curso Experto en OSINT, de LISA Institure, 1-24. [Consulta 20 de septiembre de 2021]. p 3-9.

Las forma para desarrollar búsquedas de fuentes abiertas mediante el uso de operadores avanzados de Google, según (González 2012)[77] son aquellas búsquedas que permiten descubrir ficheros y usuarios de diferentes plataformas tecnológicas, de igual forma facilitan también encontrar errores o vulnerabilidades en los ficheros de usuarios y contraseñas de páginas web, detención de servicios web vulnerables, hardware disponibles en la web con vulnerabilidades, entre otras. El Google hacking o dorks permite tanto identificar los diferentes tipos de ataques existentes, vulnerabilidades de los sistemas de información y sus principales impactos en las instituciones de educación superior.

A través de los operadores de búsquedas avanzadas de Google o Google hacking, nos permitirá hallar e identificar los diferentes datos expuestos en la WEB, haciendo parte de la fase de búsqueda de información en el ciberespacio, estos operadores nos permitirá hacer búsqueda de identidades del personal integrantes del instituto de educación superior, estos datos nos permitirá saber las preferencias asociadas entre los datos personales y la información de las IES, donde las amenazas pueden hacer uso de esta información para poder planear e implementar el vector de ataque a usar, así mismo lo pueden implementar los analistas de ciberinteligencia pero con el objetivo minimizar los ataques y técnicas a emplear las amenazas como el phishing, ingeniería social, evitando el robo de credenciales y acceder a los sistemas de información de las personas y de las IES, en la cuadro 3, podemos identificar los operadores avanzados, el propósito del operador y ejemplo de uso de dichos operadores, las cuales facilitan la obtención de información de forma más específica y puntual.

[77] Gonzáles. A Google Hacking & Dorks (46 ejemplos): cómo consigue un hacker contraseñas usando sólo Google. Google puede ser tu peor enemigo. [En Línea]. España: antoniogonzalezm.es. [Fecha de Consulta 20 octubre de 2021]. Disponible en:

Cuadro 3 Operadores Google hacking o Dorks.

Operador	Ejemplo de Búsqueda	Propósito Búsqueda	Se puede combinar
Site	site:unad.edu.co	Buscar resultados dentro de un sitio específico	si
Related	related: unad.edu.co	Buscar sitios relacionados	si
Cache	cache: unad.edu.co	Buscar la versión del sitio en caché	si
Intitle	intitle: unad.edu.co	Buscar en el título de la página	si
Inurl	inurl: unad.edu.co	Buscar una palabra contenida en una URL	si
filetype:env	filetype:pdf	Buscar por tipos de archivo específicos	si
Intext	ntext:unad	Buscar en el texto del sitio web solamente	si
" "	"UNAD"	Buscar palabra por coincidencia exacta	si
+	Cesar+augusto+sanabria	Buscar más de una palabra clave	si
-	dulces - artificial	Excluir palabras de la búsqueda	si
OR	jaguar OR car	Combinar dos palabras	Si
*	how to * Wikipedia	Operador de comodín	si
@	@wikipedia	Buscar en redes sociales	si
#	#unad	Buscar hashtags	si
$	camera $400	Buscar un precio	Si
..	camera $50..$100	Buscar dentro un rango de precios	si

Fuente: Elaboración propia tomado de Raggis Nicolas, 20 septiembre de 2021, tomado de Raggi, Nicolas. 2021. Weliveecurity By eset. 21 de Julio. Último acceso: 20 de Septiembe de 2021. https://www.welivesecurity.com/la-es/2021/07/29/google-hacking-averigua-que-informacion-sobre-ti-o-empresa-aparece-resultados/.

De igual forma a través del OSINT se puede identificar información de la organización, de los clientes "Estudiantes", docentes, directivos, entre otros, que hagan parte del instituto de educación superior que se encuentre expuesta en la web o red insegura, donde las amenazas pueden hacer uso de esta información facilitando implementar diferentes técnicas de ataques para obtener información de interés para los cibercriminales, adicionalmente OSINT también puede ser útil para realizar estudio del personal que ingresa a trabajar al instituto de educación superior con el fin de evitar los Insider en la organización educativa.

A través del uso de los navegadores también se puede realizar búsqueda de foros, conferencia, charlas videos entre otros que nos facilitara identificar como los cibercriminales desarrollan las diferentes técnicas de OISNT, phishing, ingeniería social, entre otros, permitiendo obtener información o crear perfiles falso para desarrollar los diferentes vectores de ataque, unos de los ejemplos que nos indica (Seisdedos 2020) en la conferencia dada en ekoparty security 2020 es la creación de perfiles falso para desarrollar los diferentes tipos de investigación e inteligencia en el ciberespacio para minimizar los rastros de huella digital para la obtención de información, es de rescatar que estos procedimientos lo pueden implementar los cibercriminales para acceder a las diferentes redes sociales, network, de forma pasiva o activa en búsqueda de información, suplantación y/o robo de información de los usuarios, con ello lograr acceder a los sistemas de información de las instituciones de educación superior y lograr su cometido a través de la ingeniería social.

Dentro de las búsqueda de información de fuente abiertas podemos destacar, el uso de información presentada en los diferentes foros de seguridad, que permite identificar los diferentes tipos de vulnerabilidades, técnicas y procedimientos que vienen implementando las diferentes amenazas en el ciberespacio, para resaltar la policía de Colombia dentro de su página WEB CSIRT PONAL, publica el boletín N 022/11:00 Horas del 17 de septiembre del 2021, donde mencionan que cibercriminales vienen implementando el método de phishing por correo electrónico mediante mensaje y suplantación de página web de Bancolombia, logrando engañar a las personas para obtener el usuario y la contraseña de las tarjetas débito o crédito[78]. a través de estos boletines, foros, noticias entre otros identificar los métodos que se encuentra utilizando las diferentes amenazas y a través de ello se

[78] Boletín Informativo No 22 - Alerta Phising circulando en la red. [En línea]. Colombia: cc-csirt.policia.gov.co - CSIRT PONAL. [Fecha de Consulta 21 Septiembre de 2021]. Disponible en: https://cc-csirt.policia.gov.co/alertas-tips/2021/tercer-trimestre/boletin-informativo-no-022-alerta-phishing-circula.

logra anticipar estos ataques mediante la concientización a los integrantes de las instituciones de educación superior.

En el cuadro 4, foros de vulnerabilidades encontrada mediante OSINT, permite evidenciar una lista de páginas web con información de interés acerca de las diferentes vulnerabilidades en los activos de información que posiblemente poseen las IES, con ello facilita generar conocimiento e inteligencia para la prevención de riesgos.

Cuadro 4 Páginas web, foros de vulnerabilidades encontrada mediante OSINT.

N°	Organismo	Página Web
1	Policía Nacional	https://caivirtual.policia.gov.co/
2	Centro Criptológico Nacional	https://www.ccn-cert.cni.es/
3	Instituto Nacional de Ciberseguridad de España	https://www.incibe.es/
4	CVE	https://cve.mitre.org/
5	NIST - Base de datos Nacional de Vulnerabilidades	https://nvd.nist.gov/
6	Grupo de Respuesta a emergencia ciberneticas de Colombia	https://www.colcert.gov.co/
7	Welivesecurity by ESET	https://www.welivesecurity.com/la-es/
8	Centro de respuesta de seguridad de Microsoft	https://msrc.microsoft.com/update-guide/
9	CVE	https://www.cvedetails.com/index.php
10	McAfee	https://www.mcafee.com/enterprise/es-es/threat-center/mcafee-labs/reports.html

Fuente: Elaboración propia 29 de septiembre 2021.

Dentro del proceso académico podemos hacer un ejemplo frente al rector de nuestra gran y reconocida universidad UNAD, donde con solo hacer uso de operadores avanzados podemos lograr obtener información sensible que puede afectar la información personal del rector, así como la información que pueda construir e implementar ataques de ingeniería social por parte de los diferentes actores de las amenazas del ciberespacio.

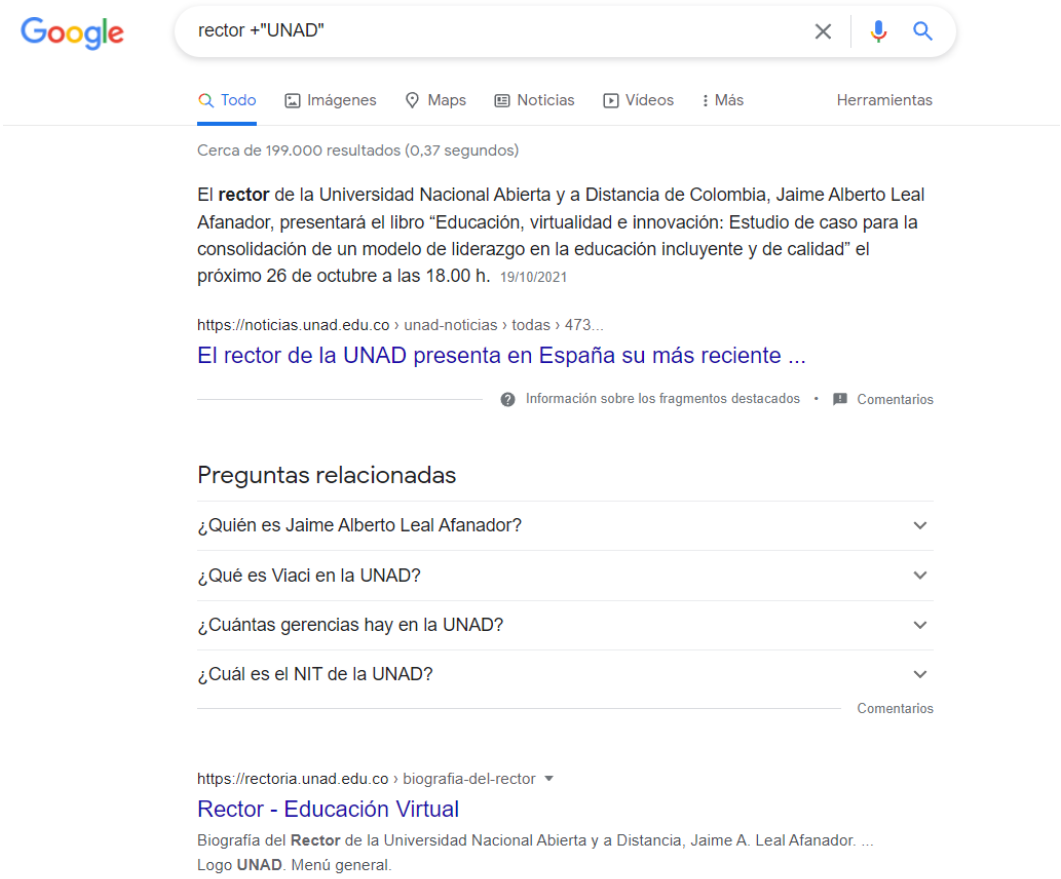
Ejemplo de Operador Google Hacking o Dork

Primer Paso

Rector + “UNAD”

En la figura 3, se evidencia en Google 199 mil resultados, logrando como medida identificación los nombres completos, correo electrónico institucional, profesión, estudios, familiares, número de teléfono, extensión, página web de la institución, entre otros datos, con ello permitirá continuar la búsqueda avanzada, facilitando obtener información específica y detallada del objetivo.

Figura 3 Primer paso de Búsqueda de datos Rector UNAD



Fuente: Elaboración propia 29 de septiembre 2021

Segundo Paso

Jaime+Alberto+Leal+Afanador "cedula"

Con la búsqueda avanzada “Jaime+Alberto+Leal+Afanador "cedula" ” aumenta la obtención de información del rector de la universidad, como se evidencia en la figura

4, se realiza el segundo paso de búsqueda avanzada y se identificando la exposición de información personal, lo cual hará objeto de ataque por parte de las ciber amenazas a través de la obtención de gran cantidad de información personal, exponiendo la seguridad la información de la universidad si no se hace un adecuado tratamiento de las vulnerabilidad y exposición de los datos.

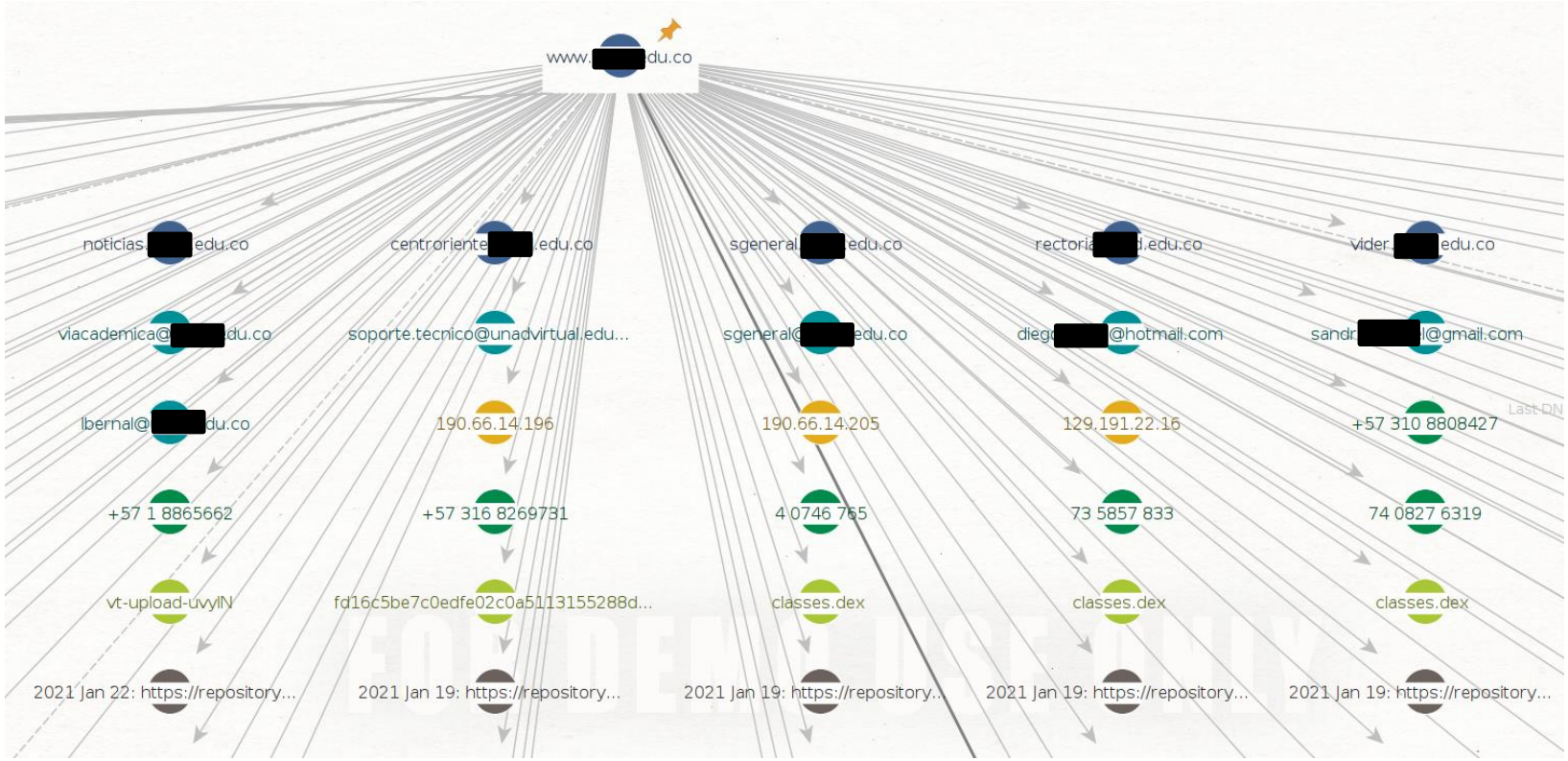
Figura 4 Segundo Paso de Búsqueda Avanzada de Google Hacking.

Fuente: Elaboración propia 29 de septiembre 2021

Las herramientas como Maltego que nos permite realizar búsqueda de información abierta, facilitando identificar los activos de información disponible y expuesta de las instituciones de educación superior, como ámbito académico realizaremos el estudio del dominio unda.edu.co, desplegando los servicios de Shodan, social link CE, a través de Maltego nos permite identificar los diferentes activos de información que posee la organización en este caso un instituto de educación superior.

Al desarrollar el despliegue de la herramienta Maltego hacia el dominio que posee un instituto de educación superior podemos observar la ilustración 5, se logra evidenciar obtener información de sitios web, numero de teléfonos, servicios DNS, blogs, correos electrónicos, nombre de personas o usuarios, ubicaciones geográficas, direcciones IP, entre otros datos de gran importancia que permite quedar al descubierto la información que puede obtener un cibercriminal.

Figura 5 Despliegue de Maltego en el Dominio .EDU.CO,



Fuente: Elaboración propia, 07 de junio de 2022

De igual forma podemos contar con la herramienta whatweb, la cual permite obtener información del sitio web, logrando identificar diferentes factores con que cuenta esta página web como el tipo de servidor, dirección IP, ubicación geográfica “Country”, correo electrónico, framework, lenguaje de programación, entre otros.

Si, se observa la figura 6, dicha herramienta logro obtener la dirección IP “190.66.1x.xxx” del dominio www.xxx.edu.co, mostrando que se encuentra ubicada geográficamente en Colombia y que el servicio se encuentra alojado en un servidor Apache, la universidad hace uso de Google Analytics, de igual forma se identifica que la página web se encuentra desarrollada a través de Frame Bootstrap, HTML 5, CSS, JS, así -mismo implementa cabeceras de protección X-XSS-Protection.

Figura 6 Despliegue de herramienta Whatweb para análisis de sitio web.

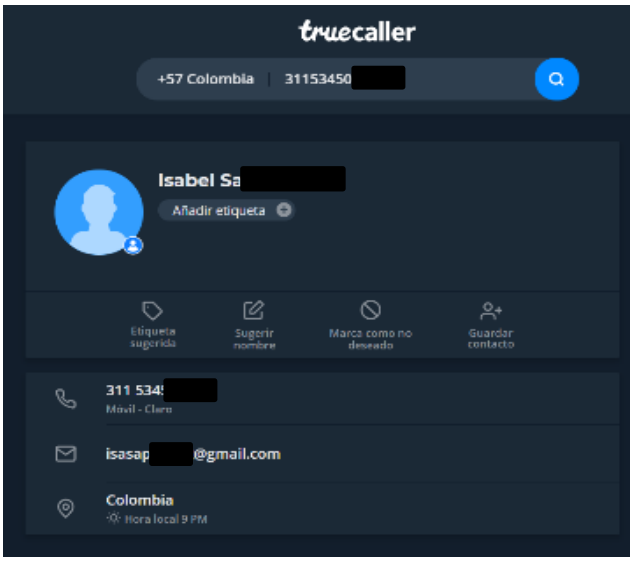
Fuente: Elaboración propia del autor, 07 de junio de 2022.

De igual forma podemos inferir el uso del OSINT permite realizar análisis de información para identificar a los integrantes de los instituto de educación superior vienen haciendo uso adecuado de los medios tecnológicos disponibles destacando la segmentación de los datos personales y/o familiares versus datos laborales, facilitando el entendimiento el comportamiento de los datos de la capa ocho “usuarios – factor humano”, con la finalidad de la implementación de políticas y directivas de seguridad de la información.

Unas de las herramientas que podemos hacer uso e identificar los datos expuestos de integrantes de la institutos de educación superior IES, es la herramienta truecaller, el cual posee una base de datos abierta que permite identificar el nombre de las personas correspondiente al número de celular, de igual forma permite obtener correo electrónico de dicho usuario como se puede observar en la ilustración 5, esta información permite validar que información se encuentra expuesta por parte de los integrante de la IES, así mismo facilitar al analista de ciberinteligencia proyecta un posible vector de ataque a utilizar las amenazas, de igual forma esta herramienta logra suministra información vital de los posibles actores que se encuentren desarrollando la actividad ilícita y si logramos percibir todas las herramientas OSINT se pueden implementar según los objetivos previsto por el usuario.

En la figura 7, recopila información de sus bases de datos e identifica del posible tenedor del número de celular, en este caso de estudio se seleccionó un numero de celular aleatorio el cual se identificó con el nombre de Isabela.

Figura 7 Información obtenida a través Truecaller.



Fuente: Elaboración propia 30 septiembre de 2021

Búsqueda de información en el ciberespacio, son los datos que nos permita identificar si hemos sido víctima de ciberataque. Realizar búsqueda de información de nuestra organización y de nuestros proveedores, teniendo en cuenta que si nuestro proveedor ha sido victimas por parte de las amenazas, nosotros también podemos haber sido afectados, para ello podemos hacer uso de la herramienta “ pwned? ”, con ello podemos identificar si existe algún tipo de exposición de datos e información de nuestro correos electrónicos, al momento de ser positivos podemos realizar cambios de nuestras contraseñas, para minimizar los riesgos.

En la figura 8, se puede evidenciar la consulta de dos correos electrónicos con resultados diferentes, en la primera imagen de color verde, indica que la cuenta o correo electrónico que se encuentra registrada en las diferentes plataformas tecnológicas no presenta ningún reporte de ataque o hackeo, a diferencia de la imagen de color rojo si aparece el mensaje “Oh no maldito”, hace referencia que las cuenta de usuario o correo electrónico que se encuentra registradas en plataformas digitales, si ha recibido ha recibido algún tipo de ataque o filtración de información.

Figura 8 Búsqueda de información de víctimas de ciberataques.

Fuente: Elaboración propia 28 de septiembre 2021

Con la ciberinteligencia nos permite identificar los vectores de ataques que pueden desarrollar las diferentes amenazas en contra del instituto de educación superior, logrando reciclar las técnicas más conocidas y eficaz que pueden implementar y así mismo nos permite la implementación de las medidas y políticas de seguridad, del mismo modo conocer y determinar a través de los analista de ciberinteligencia cuales son los objetivos que tienen estos cibercriminales a través de la determinación de casos de estudios presentados en otra organizaciones pares.

Otras de las herramientas que podemos implementar es conocer de forma detallada la infraestructura tecnológica, personas, políticas, procedimientos que se desarrolla en los sistemas de información de los institutos de educación superior, con ello permitirá implementar las herramientas, procedimientos y políticas para construir un sistema maduro en seguridad de la información que permita minimizar los riesgos existentes.

Frente a la protección de los perfiles falsos podemos hacer uso de las herramientas **Search by Image** la cual es una extensión de Google que permite desarrollar búsquedas inversas de imágenes que permiten identificar qué tipo de relación tiene dicha imagen con otras facilitando identificar las imágenes de perfil de los diferentes usuarios e identificar posibles perfiles falso o reales, evitando a través de inteligencia ser engañados mediante técnicas de ingeniería social.

Todas esta herramientas que hacen búsqueda de información de los activos de información a nivel pasiva y activa, logran brindar gran cantidad de información al analista de ciberinteligencia que permita generar conocimiento e inteligencia con el propósito de generar informes de inteligencia para el equipo azul y los directivos de seguridad para la implementación de políticas, directrices y medidas técnicas de seguridad, logrando que la institución de educación superior se encuentre en la vanguardia en seguridad de la información frente a los diferentes amenazas que se encuentran al asecho de las IES.

8 CIBERINTELIGENCIA ESTRATEGIA DE SEGURIDAD INFORMATICA MEDIANTE EL ANALISIS DE LA INFORMACION.

La ciberinteligencia comprende el ciclo de inteligencia en el ciberespacio, donde se debe tener el entendimiento de la misión en el cual se debe comprender el objetivo a cumplir en la institución de educación superior frente a la seguridad de la información, posteriormente realizar el planeamiento de búsqueda de información que permite direccionar los procesos para la búsqueda de información en el ciberespacio y entorno físico, así mismo en el ciclo de inteligencia se contempla la fase de búsqueda de información, esta fase es de gran importancia porque permite establecer los posibles vectores de ataque que puede utilizar un cibercriminal aprovechando las vulnerabilidades expuestas por los sistemas de información de la IES como lo indica (Caballero y Serrano 2018) al mencionar "el éxito de los ataques e intrusiones que sufren las empresas y organizaciones se debe en gran parte a la cantidad de información que directa o indirectamente un atacante puede obtener sobre sus sistemas o empleados."[79], por esta razón los especialistas y analista de informacion deben pensar como los cibercriminales, maliciosamente y poseer gran imaginación, permitiendo así obtener la mayor cantidad de información disponible mediante uso de diferentes tipos de herramientas, técnicas y procedimiento (externa footprinting – internal footprinting) para la recopilación de informacion.

El proceso de inteligencia en el ciberespacio se encuentra la fase de análisis de información y difusión de los productos de inteligencia, esta fase es de gran importancia ya que nos permite determinar qué información es de relevancia para la seguridad de información, por tal razón se debe realizar un adecuado tratamiento de información por ello se tomó como referencia la estructura del informe que implementa (Proyecto Aurora 2020)[80] y (Kaspersky 2021)[81] que permite desarrollar

[79] CABALLERO, Maria Angeles y SERRANO, Diego Cilleros. Protección de la información digital, En: El Libro del Hacker 2018 ed. Madrid: Juan Ignacio Luca, 2018. p. 175 194.
[80] Oscar Orellana. Taller Gratuito Ciberinteligencia con herramientas Open Source Enfoque OSINT [En linea]. Youtube Proyecto Aurora Org. [Consulta 1 de Octubre de 2021], Disponible en: https://www.youtube.com/watch?v=dO4v1v6aEJg&t=2s.
[81] Kaspersky. Informe de vulnerabilidades,[Sitio Web] Kaspers Online Help, .[Consultado 05 Octubre de 2021]. Disponible en: https://support.kaspersky.com/Cloud/1.0/es-ES/166189.htm

y estructurar un informe de inteligencia y ser difundido a nivel ejecutivo y técnico, haciendo énfasis en los siguientes puntos, así.

Gestión de documentos

- Elaboro
    - Nombre y Apellido del funcionario
    - Cargo
    - Firma
    - Fecha
- Revisor
    - Nombre y Apellido del funcionario
    - Cargo
    - Firma
    - Fecha
- Aprobó
    - Nombre y Apellido del funcionario
    - Cargo
    - Firma
    - Fecha

Tabla de Contenido

Historial de Cambio (Trazabilidad e integridad del documento)

- Fecha
- Versión
- Descripción
- Autor

Dentro del documento se debe implementar la nomenclatura de la empresa,

Cuadro 5. Nomenclatura

Código	IT PA VC	Gestión de Documentos	Imagen de la Empresa
Versión	2.0		
Vigencia	Borrador		
Pagina	4 de 10		

Fuente: Elaboración Propia tomado de Oscar Orellana. Taller Gratuito Ciberinteligencia con herramientas Open Source Enfoque OSINT [En linea]. Youtube Proyecto Aurora Org. [Consulta 1 de Octubre de 2021], Disponible en: https://www.youtube.com/watch?v=dO4v1v6aEJg&t=2s.

Definir el Alcance del informe.

Se debe describir el requerimiento solicitado por el usuario y que tipo de contrato se realiza, autorización y alcance que puede tener el proceso de inteligencia del ciberespacio.

Referencia

Se debe realizar una descripción detallada del contrato, responsables del proceso de ciberinteligencia, numero de contrato, tipos de técnicas y herramientas a implementa para la búsqueda de información en el ciberespacio.

Responsabilidades

Se describe el equipo de trabajo, nombres y apellidos, identificación, profesión, funciones, tareas.

Definiciones

Se debe describir todas las palabras técnicas que se emplea en el informe ejecutivo que permita al lector comprender sobre los temas desarrollados en el proceso de ciberinteligencia.

Cuerpo del Informe.

- Búsqueda de información

  Se describe las fuentes de información, información encontrada, técnicas de obtención de la información, cuales herramienta de búsqueda de información

fue implementada, de igual forma en el desarrollo de búsqueda de información se debe realizar la verificación de información obtenida, permitiendo contrastar con diferentes fuentes de información o escenarios facilitando generar un análisis de la información.

Es de rescatar durante la fase de búsqueda de información se debe tener en cuenta los datos de los sistemas cognitivos e informáticos de acuerdo a los grupos de datos por su naturaleza sistémica como lo señala (Oscar Sanchez Belmont, 2021) en su libro de ciberinteligencia y contrainteligencia aplicación e impacto en la seguridad Nacional[82], De igual forma se debe describir los datos obtenidos de las vulnerabilidades identificadas de los sistemas, teniendo en cuenta el siguiente ítem, como lo plantea (Kaspersky 2021)[83].

- Nombre de los Dispositivos
- Descripción del Dispositivos
- Ubicación Geográfica de los Dispositivos Tecnológicos.
- Oficina o Dependencia
- Nivel de Clasificación de la Información
- Información Disponible del Dispositivo Tecnológico
- Sistema Operativos
- Nivel de gravedad
- Proveedor de Servicios
- Aplicaciones/Software disponibles
- Versión de la Aplicación
- Nombre de la Vulnerabilidad
    - Fecha y Hora de la Detención
    - Versión de la vulnerabilidad

[82] Oscar Sanchez Belmont, Ciberinteligencia y cibercontrainteligencia: aplicación e impacto en la seguridad nacional (2021) eLibro, (Ciudad de Mexico Instituto Mexicano de Contadores) Recuperado el 22 de marzo de 2022, de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/174910?page=135

[83] Kaspersky Endpoint Security Cloud. Informe de Vulnerabilidades.[En Linea]. España: support.kaspersky [Fecha de Consulta: 15 Octubre de 2021]. Disponible en: https://support.kaspersky.com/Cloud/1.0/es-ES/152344.htm

- Amenazas que pueden aprovechar la Vulnerabilidad
- Parches de Seguridad disponibles
- Posibles Medidas de Correctivas de vulnerabilidades
- Dirección Web
- Puerto
- Reglas
- Estado de cifrado o Encriptación
- Vector de ataque y/o técnicas que pueden realizar las amenazas para explotar la Vulnerabilidades
- Dirección IP
    - Publica
    - Privada
- Dirección MAC
- Umbral de Riesgo
    - Nivel de Importancia del Riesgo
    - Severidad de Perdida.
- Ubicación Geográfica de los Dispositivos
    - País
    - Departamento
    - Municipio
    - Vereda
    - Barrio
    - Dirección
- Documentación disponible del usuario o empresa.
    - Tipo de Archivo
    - Clasificación de la información
    - Formato de Archivo
- Información Disponible del Usuario.
    - Nombre de los usuarios
    - Edad
    - Sexo

- Cargo Laboral
- Nivel de clasificación de Información.
- Ubicación Geográfica del Usuario
    - País
    - Departamento
    - Municipio
    - Vereda
    - Barrio
    - Dirección
- Correo Electrónico
- Número de Identificación.
- Teléfono / Celular
- Dirección Física
- Nivel Académico
- Profesión
- Redes Sociales
- EPS
- Cuenta de Banco
- Estudios Académicos
- Hobbies

- Informatica Forense
    - Recopilación de Evidencia Digital
        - Imagen de disco (Bit a Bit)
        - Obtención de Hash MD5 de la Copia validar autenticidad de los datos.
        - Fecha y Hora de cada paso
        - Número de Serie
        - Componente
        - Sistema Operativo

- Fotografía (Nivel General “Entorno”– Nivel Especifico “Equipo y componentes”)
- Acompañamiento Persona Testigo Recopilación de Datos “Notario o Policía Judicial”
- Registro y Contenidos de la cache
- Registros y logs del sistema
- Ficheros Ocultos
- Contenido de la Memoria RAM
- Estado de la Conexión de red, tablas y rutas
- Enumeración de Puertos
- Dirección IP – Direcciones Física MAC
- Estado de los procesos en ejecución
- Contenido del sistema de archivo y de los disco duros
- Contenido de otros dispositivos de almacenamiento
- Listados de usuarios conectados local
- Usuarios Remotos conectados
- Configuración de seguridad del sistema

- Hallazgo del Ataque
  - Huella digital del atacante
  - Herramientas utilizadas por el atacante
  - Alcance del ataque
  - Origen del ataque
  - Cronología del ataque
- Dentro del proceso de preservación de evidencia ante un ataque informático se debe generar dos copias de la evidencia y hacer uso de la función hash MD5 que permite comprobar y garantizar la integridad de la evidencia obtenida.

Escenario.

- Búsqueda

  Se describe los posibles escenarios que se pueden presentar según los resultados obtenidos de la búsqueda de la información y del análisis de información.

- Análisis

  Se realiza el análisis de los diferentes escenarios establecidos e implementación del análisis DOFA - PESTEL.

  En el análisis DOFA que hace referencia la figura 9, se debe tener presente la información recolectada entre ella las amenazas, fortalezas, debilidades y oportunidades, las cuales permiten analizar las características internas "Debilidades y Fortalezas" y externa "Amenazas y Oportunidades" de la seguridad de la información de las instituciones de educación superior de Colombia que permitan realizar las tomas de decisiones a los directivos de las IES.

Figura 9 Matriz DOFA,

Fuente: Elaboración propia 01 octubre de 2021 tomado de BETANCOURT, Diego. Cómo hacer el análisis FODA (matriz FADO) paso a paso + ejemplo práctico. [En línea]. 19 de abril de 2018. [Fecha de Consulta 24 octubre de 2021]. Disponible en: www.ingenioempresa.com/matriz-foda.

En el análisis DOFA se debe tener en cuenta las diferentes preguntas a realizar por cada uno de los componentes como lo sugiere (Betancurt 2018)[84] cuando menciona los seis pasos de cómo hacer el análisis DAFO.

En el componente amenaza son todos aquellos riesgos externos que no poseemos control para cumplir la seguridad de la seguridad de la información, para ello se debe contemplar las siguientes preguntas

¿Como está cambiando el panorama de las ciber amenazas?

- ¿Qué están haciendo los cibercriminales?
- ¿Cuáles son las técnicas utilizadas para los ciberataques?
- ¿Cuáles son las posibles intensiones de la ciberamenaza?
- ¿Alguna vulnerabilidad puede ser una ciberamenzas para la IES?
- ¿Están cambiando los tipos, métodos y técnicas de ataques de las amenazas?
- ¿Cómo afecta las medidas económicas, gobierno, académicas y social a la seguridad de la información?
- ¿Cuáles son las nuevas tecnologías que hacen uso las amenazas cibernéticas? ´

Frente al componente de Oportunidades son los factores positivos que posee las instituciones de educación superior que se pueden aprovechar, para ello se debe hacer las siguientes preguntas.

- ¿Cuáles son las tendencias de seguridad de información?
- ¿Cuáles son los cambios tecnológicos se pueden implementar para la seguridad y monitoreo de redes?
- ¿Qué herramientas opensource y libre debemos implementar para la seguridad de la información?

[84] BETANCOURT, Diego. *Cómo hacer el análisis FODA (matriz FADO) paso a paso + ejemplo práctico*. [En línea]. 19 de abril de 2018. [Fecha de Consulta 24 octubre de 2021]. Disponible en: www.ingenioempresa.com/matriz-foda.

- ¿Qué eventos, Webinar y/o Talleres de capacitación gratuita se puede implementar al personal administrativo y técnico de la IES?
- ¿Cómo los Directivos de las IES apoyan e implementan las políticas de Seguridad de la Información?
- ¿Cómo se comporta las personas frente a las políticas de seguridad de la información?
- ¿Existen alguna fortaleza que podamos explotar?

En el componente de Fortalezas se puede indicar que son aquellos factores internos positivos de la institución de educación superior frente a la seguridad de la información, para ello se deben tener presente los siguientes parámetros.

- ¿Cuáles son nuestras Políticas de Seguridad de Información?
- ¿Contamos con el equipo de personas capacitado en seguridad de la información?
- ¿Contamos con tecnología que permite implementar las medidas y seguimiento de seguridad de información?
- ¿Cuáles son los procesos de seguridad de información se desarrollan mejor?
- ¿Cuáles son los planes de mejoras?
- ¿Se cuenta con el apoyo financiero y/o económico para la implementación de la seguridad de la información?
- ¿Se cuenta con planes de capacitación en relación en seguridad de la información y/o certificaciones?

Finalmente, el componente de debilidades hace alusión a los factores negativos de la IES, las cuales pueden poner en desventajas frente a las ciber amenazas, por ello se debe tener cuenta los siguiente.

- ¿Cuáles son las actividades que compromete la seguridad de la información?
- ¿Cuáles son las malas prácticas en seguridad de la información identificadas por las diferentes organizaciones?
- ¿Cuáles son las vulnerabilidades existentes en las plataformas tecnológicas disponibles en las IES?

- ¿Cuáles y cuanta información se encuentra disponible en la red insegura?
- ¿Cuál es el nivel de madures de seguridad de la información de la IES?
- ¿Cuáles son los softwares que se encuentra desactualizados?

Conclusiones.

Las conclusiones se deben elaborar de forma objetiva, generando propuestas de mejora de acuerdo con el análisis e información que permita minimizar los riesgos en las IES.

Condiciones de Comunicación.

Dentro de las especificaciones se deben establecer las condiciones de comunicación y términos de confidencialidad de la información.

Revisión

Dentro del proceso de revisión o retroalimentación de la información es fundamental que se establezca cada cuanto se volverá a desarrollar el proceso de ciber inteligencia en los sistemas de información de la organización, con el fin de mantener la mejora continua en la seguridad de la información del instituto de educación superior.

Cuadro 6 Control de Cambio y Revisión

Versión	Fecha	Cambios Realizados	Responsables

Fuente: Oscar Orellana. Taller Gratuito Ciberinteligencia con herramientas Open Source Enfoque OSINT [En linea]. Youtube Proyecto Aurora Org. [Consulta 1 de Octubre de 2021], Disponible en: https://www.youtube.com/watch?v=dO4v1v6aEJg&t=2s.

Visto Bueno y Aprobado

El documento debe poseer las firmas del técnico que desarrollo el documento dando la vista bueno, así mismo debe tener la firma de jefe del proyecto aprobando el documento desarrollado.

Teniendo en cuenta la información recolectada a través de las diferentes diciplinas (HUMINT - OSINT - SIGINT – SOCMINT - ELINT – COMINT – Informatica Forense), permite realizar el proceso de organización, procesamiento, análisis y evaluación de la informacion a través de métodos científicos, Ciberinteligencia y la metodología DOFA, logrando generar informes de inteligencia de calidad, facilitando el entendimiento de las diferentes amenazas y como estas puede aprovechar las vulnerabilidades disponible en nuestro entorno tecnológico, así como detectar los patrones de ataques, el modus operandi, sus técnicas, tácticas y procedimiento esto se le llama conocer al enemigo y establecer la probabilidad de ocurrencia e impacto que puede ocasionar en los sistema de información evitando los incidentes informáticos.

Como estrategia de seguridad Informática para las instituciones de educación superior es la implementación y usos de sistemas trampas (HoneyPost), estos sistemas trampas deben ser similares a los sistemas informáticos de la IES o a los sistemas que se encuentra en producción, que contengan pequeños cambios que permitían realizar recolección y análisis de informacion de los cibercriminales con el objetivo de identificar herramientas, métodos y vectores de ataques que pueden afectar los sistemas de informacion, así como llevar estadísticas de tipos ataques, nivel de afectación, refinar los sistemas detención y previsión de intrusos, permitiendo asegurar adecuadamente los sistemas informáticos[85].

Los informes de inteligencia elaborados por los especialistas permitirán gestionar una adecuada estrategia de seguridad informática desde el nivel Directivo hasta el nivel táctico, por ejemplo la implementación y actualización de políticas de seguridad informática e informacion, metodología de gestión de incidentes de seguridad y contingencia, plan de continuidad del negocio, estrategias de recuperación de informacion, establecer técnicas, tácticas y procedimientos de ciberseguridad, gestionar mediante convenios o contratos la implementación de las capacidades de

[85] ROBLES, Javier leonardo. Informatica Forense un alizado en la estrategia de ciberseguridad implementada en Colombia. [En línea]. 31 de julio de 2022. [Fecha de Consulta 31 julio de 2022]. Disponible en: http://polux.unipiloto.edu.co:8080/00001174.pdf

Informatica forense y seguridad informática a nivel técnico y jurídico dirigido al personal de las TIC, integrante de la comunidad académica y directivos que permita la concientización, ya que son los principales vectores de ataques por parte de las ciberamenazas, así mismo permite desarrollar el planeamiento, implementación y seguimiento de los proceso de seguridad informática e implementar el plan director de seguridad a través del centro de operaciones de seguridad (SOC) mediante la metodología del Purple Team, previniendo y minimizando los riesgos identificados en el ciberespacio, aprovechando las oportunidades existente y mejorar las fortalezas, logrando minimizar y mitigar los riesgos de las instituciones de educación superior.

Finalmente, el proceso de ciberinteligencia debe ser parte de la estrategia de seguridad informática, permitiendo mantener el mejoramiento continuo en la seguridad informática y de la informacion, reduciendo los futuros vectores de ataques de las amenazas en el ciberespacio y los sistemas de información como entornos seguros de las Instituciones de Educación Superior.

9 CONCLUSIONES

Durante el desarrollo de la metodología y estudio académico se logra analizar el proceso de inteligencia en el espacio logrando establecer la ciberinteligencia como una estrategia de seguridad de la información que permite anticipar las amenazas e identificación de las vulnerabilidades a través de la búsqueda de información y mediante la difusión de informes de inteligencia, minimizar los posibles riesgos que pueden enfrentar las instituciones de educación superior en Colombia.

En el ciberespacio se logra identificar múltiples amenazas que pueden afectar los sistemas información y sus activos tecnológicos, entre las principales amenazas se encuentra el ciber espionaje, amenazas hibridas, cibercrimen y hackitivismo, cada una de ellas pueden materializarse a través de técnicas de ciberataque aprovechando y explotando las vulnerabilidades de las organizaciones y empresas, en nuestro caso las IES como se encuentra descripto en el cuadro 1 Amenazas. En Colombia se evidencia como principales modalidades o técnicas de ataques cibernéticos, como el phishing, suplantación de identidad, Malware, ransomware, visishing, smishing, carta nigeriana y ciberbullying, estas técnicas son empleadas por los cibercriminales para realizar estafas, robo de información, acceso abusivo a los sistemas de información, afectando la confidencialidad, integridad y disponibilidad de los sistemas tecnológicos de la información y las comunicaciones de estas llegando al punto de perjudicar el GoodWill de la institución.

Es de aclarar que en Colombia la mayoría de los sectores económicos no documentan, denuncian o reportan los incidentes y eventos informáticos lo cual afectan el GoodWill de la Entidad, teniendo en cuenta que no se cuenta en Colombia con suficiente personal Capacitado y certificado en seguridad informática, no cuenta con Políticas de seguridad, Sistemas de Gestión de seguridad de la Información, procedimiento de gestión de incidentes, así como la baja inversión en el área de ciberseguridad, manteniendo la brechas de seguridad informáticas e información.

Al examinar los cuatro pasos del proceso de inteligencia en el ciberespacio, permite desarrollar una estrategia de seguridad para las instituciones de educación superior de Colombia mediante la anticipación de eventos mediante la comprensión del modus operandi de los cibercriminales y de la institución educativa, es indispensable dentro de cada fase del proceso de ciberinteligencia emplear de forma transversal y continua el análisis y evaluación de la información, ya que permite mejorar los objetivos planteados, proceso, productos, datos e información disponibles, a su vez permite caracterizar de forma adecuada la evolución de las amenazas y vulnerabilidades de las tecnológicas que hacen parte de los activos de información de las IES en Colombia.

En el proceso ciberinteligencia cuenta con multiplex medios, métodos y herramientas de recolección, unos de los métodos más útil para la recolección de información en el ciberespacio es el uso de la inteligencia de fuente abiertas “OSINT” permite identificar las principales amenazas, vulnerabilidades e información disponible en web que puede ser aprovechada por los cibercriminales afectando la seguridad de los activos de información de las instituciones de educación superior Colombia. A través de la inteligencia de fuentes abiertas “OSINT”, permite la obtención de información de forma pasiva y activa en los diferentes sistemas de publica disponible como los medios de comunicación, datos públicos, literatura gris, informes de investigación, imágenes entre otros, facilitando el entendimiento en los procesos, procedimientos, técnicas y tácticas de las diferentes amenazas, así como conocer el comportamiento de las mismas instituciones de educación superior de Colombia en el ciberespacio, la búsqueda de información en los diferentes foros, blogs, centro de investigación, repositorios, conferencias, reportes, hace parte del OSINT, proporcionando información de interés al analista del ciberespacio como las ultimas tendencia, comportamiento y herramienta que vienen usando los cibercriminales y con ello permite caracterizar el modus operandis de las amenazas y facilitando el entendimiento de los cibercriminales, así mismo permite identificar las vulnerabilidades existentes en el

ciberespacios que pueden poseer las IES y como los cibercriminales se aprovechan esta información, es de aclarar que el uso del método OSINT también es utilizado por parte de los cibercriminales facilitando identificar cual es la información disponible que posee las IES en la red insegura “Internet”, dentro de las herramientas usadas para la implementación del OSINT se puede hacer mención algunas de ellas como Google Dork/Google Hacking, Shodan, Google Search, Whois, Maltego, Nmap, Osintux, FOCA, con lo que permite al cibercriminal desarrollar técnicas de ingeniería social, phishing, suplantación de identidad, Vishing, Smishing, estafa por compra y/o venta, malware específicos y avanzados, entre otras afectando de forma transversal a la organización, los activos de información y goodwiil de la IES.

Los informes de inteligencia se encuentra ligada a la fase de evaluación y difusión de la información, esta fase es de gran importancia ya que permite difundir la ciberinteligencia a través de informes de las amenazas, riesgos existentes, métodos y técnicas que implementan los cibercriminales hacia las instituciones de educación superior, permitiendo anticipar las acciones de los cibercriminales y minimizar riesgos que puedan generar estas amenazas mediante la explotación de las vulnerabilidades e información disponibles en el ciberespacio, permitiendo a la alta gerencia, directivos, tomar decisiones adecuadas e implementar políticas de seguridad de la información, establecer niveles de accesos y privilegios, apoyo financiero en capacitación, concientización y cultura de seguridad, y fortalecimiento de la infraestructura tecnológica de la mismas, conformación del centro de operaciones de seguridad “SOC” en la institución de educación superior o apoyo de equipo de respuesta CERT / CSIRT, implementación de apoyos de equipos Red Team, Blue Team o Purple Team .

Así mismo los informes de inteligencia deben ser implementado a nivel técnico, con ello permitirá al área de infraestructura tecnológica y comunicaciones, como a los especialistas de seguridad de la información implementar herramientas tecnológicas y configuraciones más adecuadas que se adapten a las necesidades

de las IES y que permitan implementar políticas como filtrado datos y protocolos, listas de control de acceso “ACL”, sistemas de monitoreo, analizador de protocolos y control de datos, sistemas de prevención de perdida de información “DLP”, segmentación de las redes, implementación de grupo de usuarios y privilegio a través de directorio activo, entre otros.

Por lo anterior la ciberinteligencia se establece como una estrategia de ciberseguridad para las instituciones de educación superior en Colombia, mediante la aplicación del proceso de inteligencia en el ciberespacio, logrando desarrollar informes de ciberinteligencia que permiten alertar, prevenir, denegar, anticipar las diferentes amenazas, vulnerabilidades y riesgos que pueden sufrir las instituciones de educación superior, así mismo caracterizar las fortalezas y oportunidades que influyen en la adecuada toma de decisiones a nivel gerencial, ejecutivo y/o técnico para que implementen medidas preventivas, proactivas y/o correctivas frente a la seguridad informática e información en las instituciones de educación superior de Colombia.

10 RECOMENDACIONES

En base de las conclusión y resultados obtenidos durante el estudio académico de la Ciberinteligencia como de seguridad informática e información se recomienda a la comunidad de ciberseguridad mantener y continuar con los estudios del uso de la ciberinteligencia para la seguridad informática mediante el apoyo de las tecnologías convergentes “Big Data, Ciencia de Datos, Inteligencia Artificial” con el objetivo de fortalecer el desarrollo del proceso de inteligencia en el ciberespacio.

De igual forma se recomienda a las instituciones de educación superior de Colombia, implementar el modelo del proceso de inteligencia en el ciberespacio “Ciberinteligencia”, como estrategia de ciberseguridad que permite la anticipación de las amenazas y minimizar los riesgos de ciberespacio, así como capacitar al personal de ciberseguridad a nivel técnico, analista y director del SOC, con el ánimo de fortalecer las capacidades de respuesta y mitigación de los riesgos en los sistemas de información, con ello permite un producto de inteligencia maduro e información relevante para la toma de decisiones a nivel estratégica y táctica.

Dentro del proceso de estudio de estrategias de seguridad de la información en las instituciones de educación superior, se recomienda realizar investigación documental acerca del uso de la ciberinteligencia en la Deep web y Dark web que permita anticipar las diferentes amenazas en el ciberespacio.

11 BIBLIOGRAFIA

Albors, J., & Arroyo, R. Cada Vez funcionan mejor las amenazas hibridas [Sitio Web]. España: Youtuber ESET. [Consulta 22 noviembre de 2020], Disponible en: https://www.youtube.com/watch?v=-meAWpbjRko&ab_channel=ITTelevisi%C3%B3n

Adriana Diaz, Pontificia Universidad Javeriana, Información de Prensa, [En linea] Bogotá, https://javeriana.edu.co [Consultado 30 Octubre de 2022] Disponible en: https://www.javeriana.edu.co/recursosdb/20125/724951/22-11-2021+Comunicado+de+prensa+-+Seguridad+informa%CC%81tica+Javeriana.pdf/a37fa6b9-3140-9d3f-58bb-df991857a9b2?t=1637602154780

Betancourt, Diego. *Cómo hacer el análisis FODA (matriz FADO) paso a paso + ejemplo práctico*. [En línea]. 19 de abril de 2018. [Fecha de Consulta 24 octubre de 2021]. Disponible en: www.ingenioempresa.com/matriz-foda

Biblegateway, Misión de los doce espías, [Sitio Web], Reina-Valera. (1960). [Consulta el 2 de diciembre de 2020], Disponible en https://www.biblegateway.com/passage/?search=Deuteronomio+1%3A19-33&version=RVR1960

Boletín Informativo No 22 - Alerta Phising circulando en la red. [En línea]. Colombia: cc-csirt.policia.gov.co - CSIRT PONAL. [Fecha de Consulta 21 Septiembre de 2021]. Disponible en: https://cc-csirt.policia.gov.co/alertas-tips/2021/tercer-trimestre/boletin-informativo-no-022-alerta-phishing-circula

Centro Criptológico Nacional CCN. Guía de Seguridad (CCN-STIC-425) Ciclo De Inteligencia y Análisis de Intrusiones. [Sitio Web] España: Ministerio de la Presidencia. [Consulta 17 de Octubre de 2020], Disponible en https://www.ccn-

cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html

CABALLERO, Maria Angeles y SERRANO, Diego Cilleros. Protección de la información digital, En: El Libro del Hacker 2018 ed. Madrid: Juan Ignacio Luca, 2018 [Consultado 15 abril de 2021 Cap. 5 de El libro del Hacker]. p. 181 200.

CABALLERO, Maria Angeles y SERRANO, Diego Cilleros. Protección de la información digital, En: El Libro del Hacker 2018 ed. Madrid: Juan Ignacio Luca, 2018 [Consultado 23 junio de 2022 Cap. 5 de El libro del Hacker]. p. 175 194.

Chávez, C. F. (2018). eLibro. (E. CidEditor, Ed.) Recuperado el 9 de octubre de 2020, de https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/36728

Consejo Nacional De Política Económica y Social, Documento CONPES 3854, Política nacional de seguridad digital, [Sitio Web] Bogotá: Cámara De Comercio De Bogotá. [Consulta 17 octubre 2020], Disponible en: https://bibliotecadigital.ccb.org.co/handle/11520/14856

Centro Criptológico Nacional CCN. [Sitio Web], Madrid, España, Guía De Seguridad (CCN-STIC-401) Glosario Y Abreviaturas.[Consulta 17 de Octubre de 2020], Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

CISCO. ¿Qué es la ciberseguridad? [Sitio Web] www.cisco.com. [Consulta 17 Octubre de 2020], Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

CONVERSIA. Tipos de ciberataques: más allá del ransomware.[Sitio Web] España: www.consultoria-conversia.es. [consulta 13 Octubre de 2020], Disponible en:

http://www.consultoria-conversia.es/internet/tipos-ciberataques-infografia-ransomware/

Candau, Javier. Ciberinteligencia, complemento perfecto para la Ciberseguridad. Revista Redseguridad*, 2017*, nro. 079, pp 52-54 . [consulta 13 octubre de 2020], Disponible en: https://www.redseguridad.com/revistas/red/079/52/

Check Point Research, Cyber Security Report, 2022, "Informe Sobre Seguridad 2022, Capitulo 5 Estadísticas Globales." [Sitio Web] Israel, https://www.checkpoint.com/ [Consultado 22 Octubre de 2022], Disponible en: https://www.checkpoint.com/downloads/resources/cyber-security-report-2022-ES.pdf?mkt_tok=NzUwLURRSC01MjgAAAGHoQ6BgFtqenMmlAbU7Un1emeotHIblvJBNzmJ0wMhmgjtNFNmZTH07tzEdYuWWbMg_db1PXVJj3oWuYorv98I9f8cgUowQNIXeW7FyAvA8mdWvah7

CISDE. La amenaza cibernética: ciberguerra y ciberdefensa [Sitio Web] España: CISDE Observatorio.[Consulta 8 Noviembre de 2020], Disponible en: https://observatorio.cisde.es/archivo/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa/

Diaz, J. R. Instituto Español de Estudios Estratégicos, Ciberamenazas ¿El terrorismo del Futuro?. (Boletín Electrónico 86/2016: 19 agosto 20160), Consulta 17 de Octubre de 2020, Disponible en http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Deloitte. Estudio de Ciberseguridad, Principales Universidades de España.[Sitio Web].España Deloitte Advisory. [Consultado 23 Noviembre de 2020], Disponible en: https://www2.deloitte.com/content/dam/Deloitte/es/Documents/governance-risk-compliance/Deloitte-ES-GRC-Ciberseguridad-Universidades.pdf

Ejército Nacional. Manual Fundamental de Referencia de Inteligencia, Proceso de inteligencia. [Sitio Web]. Bogotá: CEDOE. [Consulta Octubre de 2020], Disponible

en:
https://www.dicoe.mil.co/recurso_user/doc_contenido_pagina_web/800130633_4/458748/mfre_2_0_inteligencia.pdf

Estarellas, J. C. Objetivo de inteligencia: infiltrar Al Qaeda. [En Linea] Madrid: Bubok Publishing S.L. eLibro 2018 [Citado el 08 abril 2022] Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/51385?page=20.

Forbes Staff, Universidad El Bosque dice logró recuperar todas sus plataformas digitales, tras hackeo general [en Linea] Colombia. Forbes Colombia, [Consultado 24 de Octubre de 2022] Disponible en: https://forbes.co/2021/07/01/actualidad/universidad-el-bosque-que-dice-logro-recuperar-todas-sus-plataformas-digitales-tras-hackeo-general/

Fresno Chávez, C. (2018). ¿Cómo funciona Internet?. Editorial Ciudad Educativa. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/36728?page=32

Yanes, J. La historia de los virus informáticos. [Sitio Web] OpenMind BBVA. [Consulta 9 octubre de 2020], Disponible en:https://www.bbvaopenmind.com/tecnologia/mundo-digital/la-historia-de-los-virus-informaticos/

Gonzáles. A Google Hacking & Dorks (46 ejemplos): cómo consigue un hacker contraseñas usando sólo Google. Google puede ser tu peor enemigo. [En Línea]. España: antoniogonzalezm.es. [Fecha de Consulta 20 octubre de 2021]. Disponible en:https://antoniogonzalezm.es/google-hacking-46-ejemplos-hacker-contrasenas-usando-google-enemigo-peor/

Gobierno de España. Estrategia Nacional de Ciberseguridad [Sitio Web]. España CCN-CERT.[Consulta 08 Noviembre de 2020],Disponible en: https://www.ccn-cert.cni.es/pdf/documentos-publicos/3809-estrategia-nacional-de-ciberseguridad-2019/file.html

INTERPOL, Los ataques cibernéticos no conocen fronteras y evolucionan a gran velocidad. [Sitio Web].España; INTERPOL. [Consulta 23 Noviembre de 2020], Disponible en: https://www.interpol.int/es/Delitos/Ciberdelincuencia

INTERPOL Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19, [Sitio Web], Secretaría General de INTERPOL, [Consulta el 9 de octubre de 2020], Disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

JAI XVIII JORNADA NACIONALES DE ADMINISTRACION E INFORMATICA (18: 10, NOVIEMBRE 2020, YouTube), La ruta de la ciberseguridad. ¿Qué camino puedo seguir?, UNER Facultad de Ciencia de Administración. [Consulta 2 de diciembre de 2020], Disponible en https://www.youtube.com/watch?v=q1D1X3jNrC0&list=LL&index=7&t=2158s&ab_channel=UNERFcad

Jeimy Cano, Colombia no está preparada ante un ciberataque, [Sitio Web] Colombia: Universidad del Rosario, https://www.urosario.edu.co/ [Consultado 28 septiembre 2022], Disponible en: https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/

Kaspersky. Informe de vulnerabilidades, [Sitio Web] Kaspers Online Help, .[Consultado 05 Octubre de 2021]. Disponible en: https://support.kaspersky.com/Cloud/1.0/es-ES/166189.htm

La Fm, Hackearon sistema de Universidad del Tolima y modificaron notas de estudiantes [en Línea] Colombia, La FM radio, [Consultado 24 de Octubre de 2022] Disponible en: https://www.lafm.com.co/colombia/hackearon-sistema-de-universidad-del-tolima-y-modificaron-notas-de-estudiantes

Latto, N. Avast, ¿Qué es WannaCry?,[Sitio Web] 27 de febrero de 2020. Consultado el 9 de octubre de 2020, Disponible en: https://www.avast.com/es-es/c-wannacry

Lux, L. M. Defining cyberterrorism, [en línea]. Scielo, Revista chilena de derecho y tecnología, vol.7 nro.2 Santiago Diciembre. 2018. [Consultado 08 noviembre de 2020] ISSN 0719-2584 doi:10.5354/0719-2584.2018.51028, disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005&lng=en&nrm=iso&tlng=es

Iurcu, V. Avira, Ciberataques en la universidad: ¿qué universidades son objetivo de los piratas, ¿cómo y por qué?,[Sitio Web] 8 de septiembre de 2020. [consultado 9 de octubre de 2020], Disponible en: https://www.avira.com/es/blog/ciberataques-en-la-universidad-que-universidades-son-objetivo-de-los-piratas-como-y-por-que

LISA Institute. Navegadores y servicio Online de búsqueda Avanzadas, 2020/02, En Curso Experto en OSINT, de LISA Institure, 1-24. [Consulta 20 de septiembre de 2021]. p 3-9.

LISA Institute. ¿Qué es y para qué sirve la Ciberinteligencia? [Sitio Web]España: Ministerio de Interior y lisainstitute. [Consulta 9 Octubre de 2020], Disponible en:https://www.lisainstitute.com/blogs/blog/ciberinteligencia-que-es-y-para-que-sirve

LISA Institute, Qué es la Guerra Híbrida y cómo nos afectan las Amenazas Híbridas. [Sitio Web].España: LISA Institute. [Consulta 8 Noviembre de 2020], Disponible en: https://www.lisainstitute.com/blogs/blog/guerra-hibrida-amenazas-hibridas.

Ministerios De Tecnologías De La Información y Comunicaciones, CONPES 3701.[Sitio Web], https://mintic.gov.co/ [Consulta 17 Octubre de 2020], Disponible en: https://mintic.gov.co/portal/604/articles-3510_documento.pdf-

Ministerio de Hacienda y Administración Publica de España. Decálogo Reutilización de Datos del Sector Publico. [Sitio Web] España: Ministerio de Hacienda y Administración Pública.
[Consulta 18 septiembre de 2021]. Disponible en: https://datos.gob.es/sites/default/files/guia-decalogo-reutilizador-opendata.pdf

Michael D. Bauer. Seguridad en servidores Linux , Ataques pasivos vs ataques activos. [Sitio Web] España: ITCA-FEPADE, [Consulta 13 octubre de 2020], Disponible en: https://virtual.itca.edu.sv/Mediadores/cms/u46_ataques_pasivos_vs_ataques_activos.html

Navarro, V. P. Amenazas Hibridas: Las nuevas tecnologías como instrumentos de Guerra.[Sitio Web] España, Barcelon: UNITEDEXPLNATIONS. [Consulta 23 Noviembre de 2020], Disponible en: https://www.unitedexplanations.org/2020/01/13/amenazas-hibridas/

Navarro, Jose Maria Blanco. Ciberinteligencia, La Via para la Ciberseguridad. [En Línea] España: Cuaderno de la Guardia Civil, nro. 57, 2018, ISSN 2341-3263 [Consulta: 18 septiembre de 2021].Disponible en: https://intranet.bibliotecasgc.bage.es/intranet-tmpl/prog/img/local_repository/koha_upload/6a7214531a3239c800669262ea3d0b36_1%20CIBERINTELIGENCIA,%20LA%20V%C3%8DA%20PARA%20LA%20CIBERSEGURIDAD.pdf

Oscar Sanchez Belmont, Ciberinteligencia y cibercontrainteligencia: aplicación e impacto en la seguridad nacional (2021) eLibro, (Ciudad de Mexico Instituto Mexicano de Contadores) Recuperado el 20 de marzo de 2022, disponible: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/174910?page=32

Oscar Orellana. Taller Gratuito Ciberinteligencia con herramientas Open Source Enfoque OSINT [En linea]. Youtube Proyecto Aurora Org. [Consulta 1 de Octubre de 2021], Disponible en: https://www.youtube.com/watch?v=dO4v1v6aEJg&t=2s.

OJALVO, Check Point Software Technologies Ltd. Check Point Software alerta sobre “La nueva normalidad” para la próxima crisis global: la ciber pandemia [Sitio Web). Colombia, Asociación Colombiana de ingenieros de Sistemas ACIS [Consultado 22 Octubre de 2022], Disponible en: https://acis.org.co/portal/content/check-point-software-alerta-sobre-%E2%80%9Cla-nueva-normalidad%E2%80%9D-para-la-pr%C3%B3xima-crisis-global-la

Portillo, I., & Gonazalez, G.Monta la NSA en tu casa, Inteligencia aplicada al mundo Ciber[Sitio Web]. HonyCon 4 edición, [Consulta 18 Octubre de 2020], Disponible en: https://docplayer.es/140691341-Monta-la-nsa-en-tu-casa-inteligencia-aplicada-al-mundo-ciber.html

Portillo, I. La inteligencia de amenazas o Cyber Threat Intelligence, [Sitio Web]. GINSEG. [Consulta 18 Octubre de 2020], Disponible en:https://ginseg.com/2018/956/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/

Ruiz, J. J. Ciberinteligencia 2.0: predicción, Revista Redseguridad, nro. 083, pp 56-57, [consulta 13 octubre de 2020], Disponible en: https://www.redseguridad.com/revistas/red/083/56/index.html

Ramiro, R. (20 de enero de 2018). ciberseguridad.blog. Recuperado el 20 de Octubre de 2020, de https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

Ruiz, J. J. (13 de diciembre de 2018). Red de Seguridad. Recuperado el 13 de octubre de 2020, de https://www.redseguridad.com/revistas/red/083/56/index.html

Rochina, P. Hacktivismo: ¿Qué hay detrás de este movimiento activista? [en línea]. España Revista digital INEMSE. [Consultado 23 de Noviembre de 2020], Disponible en: https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

ROBLES, Javier leonardo. Informatica Forense un aliado en la estrategia de ciberseguridad implementada en Colombia. [En línea]. 31 de julio de 2022. [Fecha de Consulta 31 julio de 2022]. Disponible en: http://polux.unipiloto.edu.co:8080/00001174.pdf

Surmay, L. (10 de agosto de 2020). www.gb-advisors.com. Recuperado el 13 de octubre de 2020, de https://www.gb-advisors.com/es/estos-son-los-5-tipos-de-ciberataques-mas-comunes/

Sección Magistra Ciberseguridad AUSAPE, Ramos, A., & AUSAPE. Ciberespionaje en organizaciones [Sitio Web]. España: AUSAPE Youtube. [Consulta 22 Noviembre de 2020], Disponible en: https://www.youtube.com/watch?v=0gl2FQHzgOQ&ab_channel=AUSAPEVideos

Theiler, O. Nuevas amenazas: el ciberespacio [Sitio Web]. Revista de OTAN. [Consulta 9 Octubre de 2020], Disponible en: https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.html

TZU, S. El Arte de la Guerra [Sitio Web] Argentina: Biblioteca Virtual Universal [Consulta 18 Octubre de 2020], Disponible en: https://biblioteca.org.ar/libros/656228.pdf

Torre, M. S. Ciberespionaje: una nueva forma de ataque y de defensa cibernética [Sitio Web].Barcelona: Universitat Pompeu Fabra Barcelona. [Consulta 22 Noviembre de 2020],Disponible en:https://www.upf.edu/web/antenas/el-neologismo-del-mes/-/asset_publisher/GhGirAynV0fp/content/ciberespionaje-una-nueva-forma-de-ataque-y-de-defensa-

cibernetica?__cf_chl_captcha_tk__=pmd_qG85Y3yV3y88y0XtaK85QE9AUGQPcGMBTzHlyr.DD2g-1634611870-0-gqNtZGzNA5CjcnBszQil#.YW4yvhrMJEY

Unidad de Análisis de Inteligencia De S21SEC. Ciberinteligencia: el Futuro de la Ciberseguirdad, Revista Redseguridad,2017, nro. 067, pp 64-65 [Consulta: 14 Octubre de 2020]. Disponible en: https://www.redseguridad.com/revistas/red/079/64/.

Universidad, Periódico Al Derecho, 2021 “Ataque Informatico a la Universidad de los Andes ¿Qué hacer para protegerse?”[Sitio Web] https://alderecho.org, Colombia, [Consultado 29 octubre 2022], Disponible en: https://alderecho.org/2021/04/14/ataque-informatico-a-la-universidad-de-los-andes-que-hacer-para-protegerse/

XINHUA ESPAÑOL, China condena enérgicamente ciberataques de EEUU contra Universidad Politécnica del Noroeste de China. [Sitio Web] China: spanish.news.cn [Consulta 30 Octubre de 2022] Disponible en: https://spanish.news.cn/20220906/9484b9da5a674ed8b2f2445b368555af/c.html

12 ANEXOS

Anexo A RAE

Fecha de Realización:	31/octubre/2022
Programa:	Especialización Seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	La ciberinteligencia un eslabón clave para la seguridad informática en las instituciones de educación superior publica de Colombia
Autor(es):	Sanabria Casanova Cesar Augusto
Palabras Claves:	Ciberinteligencia, Riesgos, Amenazas, ciberseguridad, Instituciones de educación superior.
Descripción:	La metodología del estudio del proceso de inteligencia en el ciberespacio como estrategia de seguridad informática en las instituciones de educación superior en Colombia, en donde se realiza las inspección de las diferentes amenazas que pueden incidir y afectar las IES en Colombia, así mismo analizar y evaluar el proceso de inteligencia y como esta puede ser implementar como estrategia de seguridad para mitigar los riesgos del ciberespacio y permitir la toma de daciones a nivel estratégico y táctico de la IES y anticiparse a la amenazas.

Fuentes bibliográficas destacadas:

INTERPOL Un informe de INTERPOL muestra un aumento alarmante de los ciberataques durante la epidemia de COVID-19, [Sitio Web], Secretaría General de INTERPOL, [Consulta el 9 de octubre de 2020], Disponible en: https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

MINISTERIOS DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES, Conpes 3701.[Sitio Web], https://mintic.gov.co/ [Consulta 17 Octubre de 2020], Disponible en: https://mintic.gov.co/portal/604/articles-3510_documento.pdf

Centro Criptológico Nacional CCN. [Sitio Web], Madrid, España, Guía De Seguridad (CCN-STIC-401) Glosario Y Abreviaturas.[Consulta 17 de Octubre de 2020], Disponible en: https://www.ccn-cert.cni.es/pdf/guias/glosario-de-terminos/22-401-descargar-glosario/file.html

UNIDAD DE ANALSIS DE INTELIGENCIA DE S21SEC. Ciberinteligencia: el Futuro de la Ciberseguirdad, Revista Redseguridad,2017, nro. 067, pp 64-65

<table>
<tr><td colspan="2">[Consulta: 14 Octubre de 2020].Disponible en: https://www.redseguridad.com/revistas/red/079/64/

LISA Institute. ¿Qué es y para qué sirve la Ciberinteligencia? [Sitio Web]España: Ministerio de Interior y lisainstitute. [Consulta 9 Octubre de 2020], Disponible en:https://www.lisainstitute.com/blogs/blog/ciberinteligencia-que-es-y-para-que-sirve

Ejército Nacional. Manual Fundamental de Referencia de Inteligencia, Proceso de inteligencia. [Sitio Web]. Bogotá: CEDOE. [Consulta Octubre de 2020], Disponible en: https://www.dicoe.mil.co/recurso_user/doc_contenido_pagina_web/800130633_4/458748/mfre_2_0_inteligencia.pdf

Centro Criptológico Nacional CCN. Guía de Seguridad (CCN-STIC-425) Ciclo De Inteligencia y Análisis de Intrusiones. [Sitio Web] España: Ministerio de la Presidencia. [Consulta 17 de Octubre de 2020], Disponible en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1093-ccn-stic-425-ciclo-de-inteligencia-y-analisis-de-intrusiones/file.html</td></tr>
<tr><td>Contenido del documento:</td><td>En el desarrolle la metodología académica se estipularon cuatro objetivos específicos que permitirá llevar a cabo el análisis del proceso de inteligencia como estrategia para mitigar los riesgos en las IES de Colombia, en donde se presentan un marco conceptual que define el concepto del ciberespacio, descripción de las amenazas cibernéticas, la importancia de la ciberseguridad, así mismo cuenta con un marco contextual de la historia del ciberespacio, las ciberamenazas y la ciberinteligencia.

Dentro del desarrollo del trabajo académico también se realiza el desarrollo de los objetivos en donde se destaca las principales ciberamenzas que afectan las instituciones de educación superior, se caracteriza y analiza el proceso de inteligencia en el ciberespacio para la seguridad de la información, así mismo se realiza el análisis de las herramientas y técnicas para la recolección de información mediante la inteligencia de fuentes abiertas y la estructuración del informe de inteligencia que permita brindar la información relevante para la tomas de decisiones.</td></tr>
<tr><td>Conceptos adquiridos:</td><td>A través del estudio documental del análisis de la ciber inteligencia como estrategia de seguridad de información de las IES en Colombia, se adquirió</td></tr>
</table>

	grandes conceptos frente que es la inteligencia y su importancia durante la historia y en la actualidad, asi mismo como se desarrolla el proceso de inteligencia en el ciberespacio mediante el uso de la inteligencia de fuente abierta, facilitando el entidimiento de las amenazas y de sí mismo como institución de educación superior, logrando entender que es de vital importancia conocer las IES desde el interior y exterior de la organización educativa y así permitir obtener información relevante para anticipar las amenazas y reducir los riesgos y fortalecer las medidas y políticas de seguridad de la información.
Conclusiones:	Durante el desarrollo de la metodología se logró analizar el proceso de inteligencia en el espacio logrando establecer la ciberinteligencia como una estrategia de ciberseguridad que permite anticipar las amenazas e identificación de las vulnerabilidades mediante la difusión de informes de inteligencia, minimizando los posibles riesgos que pueden enfrentar las instituciones de educación superior en Colombia. En el ciberespacio se logra identificar múltiples amenazas que pueden afectar los sistemas información y sus activos tecnológicos, entre las principales amenazas se encuentra el ciberespionaje, amenazas hibridas, cibercrimen y hackitivismo, cada una de ellas pueden materializarse a través de técnicas de ciberataque aprovechando y explotando las vulnerabilidades de las organizaciones y empresas, las principales modalidades o técnicas de ataques cibernéticos es el phishing, suplantación de identidad, Malware, ransomware, visishing, smishing, carta nigeriana y ciberbullying, estas técnicas son empleadas por los cibercriminales para realizar estafas, robo de información, acceso abusivo a los sistemas de información, afectando la confidencialidad, integridad y disponibilidad de los sistemas tecnológicos de la información y las comunicaciones de estas llegando al punto de perjudicar el Good Will de la institución. Al examinar las fases del proceso de inteligencia en el ciberespacio, se logra desarrollar una estrategia de seguridad para las instituciones de educación superior de Colombia, permitiendo comprender el comportamiento y modus operandi de los

	cibercriminales, a su vez conocerse así mismo la institución permite mejorar los proceso y objetivos planteados, a su vez permite caracterizar la evolución de las amenazas y vulnerabilidades de las tecnológicas que hacen parte de los activos de información de las IES en Colombia. En el proceso de inteligencia del ciberespacio se cuenta con multiplex medios, métodos y herramientas de recolección, unos de los métodos más útil para la recolección de información en el ciberespacio es el uso de la inteligencia de fuente abiertas “OSINT” que permite identificar las principales amenazas, vulnerabilidades e información disponible en web que puede aprovechar los cibercriminales afectando la seguridad de los activos de información de las instituciones de educación superior Colombia. Los informes de inteligencia permite difundir la caracterización de las amenazas, riesgos, métodos y técnicas que implementan los cibercriminales hacia las instituciones de educación superior, permitiendo anticipar riesgos que puedan generar estas amenazas a través de la explotación de las vulnerabilidades e información disponibles en el ciberespacio, permitiendo la toma de decisiones a la alta gerencia y el nivel técnico permitiendo implementar políticas de seguridad de la información y configuración necesarias en los servicios tecnológicos y prevenir las diferentes amenazas, vulnerabilidades, riesgos, así mismo el adecuado uso de las fortalezas y oportunidades que pueden permitir una adecuada toma al implementar las medidas preventivas y/o correctivas en seguridad de la información e informática.

Anexo B Ejercicio de búsqueda de información de una institución de educación superior.

Búsqueda de Información.

Dentro del proceso de búsqueda de información mediante el proceso externo footprinting, a través de la técnica de Inteligencia de Fuente Abierta OSINT, se logra recolecta gran cantidad de información disponible en el ciberespacio, así:

Herramienta Subnet Scanner de la página networkappers ubicada en la url; https://networkappers.com/

Dirección IP publica Disponibles: 190.66.1X.XX

Tabla 7: Dirección IP Publica Disponible Dominio XXXX.edu.co.

190.66.1X.XX
190.66.1X.XX - 190.66.1X.XX
190.66.1X.XX - 190.66.1X.XX

Fuente: Elaboración Propia 20 de mayo de 2022.

- 190.66.1X.XX - www.[redacted]du.co
- 190.66. 1X.XX - acceso[redacted].edu.co
- 190.66. 1X.XX - cloud.[redacted].edu.co
- 190.66. 1X.XX - calidad.[redacted].edu.co
- 190.66. 1X.XX - conferencia.[redacted].edu.co
- 190.66. 1X.XX - appmarm.[redacted].edu.co
- 190.66. 1X.XX - autoevaluacion.[redacted].edu.co
- 190.66. 1X.XX - neon.[redacted].edu.co
- 190.66. 1X.XX - appvdpar.[redacted].edu.co
- 190.66. 1X.XX - appsahag.[redacted].edu.co
- 190.66. 1X.XX - caracterizacion.[redacted].edu.co
- 190.66. 1X.XX - sisnalab.[redacted].edu.co
- 190.66. 1X.XX - app.[redacted].edu.co
- 190.66. 1X.XX - streaming.[redacted].edu.co
- 190.66. 1X.XX - rcaservices.[redacted].edu.co

- 190.66. 1X.XX - univeroas.[redacted].edu.co
- 190.66. 1X.XX - bibliotecavirtual.[redacted].edu.co
- 190.66. 1X.XX - db[redacted].edu.co
- 190.66. 1X.XX - labpedagogico.[redacted].edu.co
- 190.66. 1X.XX - srv-jcm-app.[redacted].edu.co
- 190.66. 1X.XX - symphony.[redacted].edu.co
- 190.66. 1X.XX - appweb.[redacted].edu.co
- 190.66. 1X.XX - appcoroz.[redacted].edu.co

Organización: Instituto de Educación Superior
Página Web Principal: www.[redacted].edu.co
Dirección IP publica: 190.66.1x.xxx
Sistema Operativo: Linux 3.x (86%)
Servidor: Apache
Sitio/Lugar: Cundinamarca
Puerto Servicios:

Tabla 8: Servicios Disponibles Dirección IP 190.66.1x.xxx

Port	Protocolo	Estado	Servicio	Versión
80	TCP	Abierto	HTTP	Apache
8008	TCP	Abierto	HTTP	
8010	TCP	Abierto	SSL/Xmpp	
443	TCP	Abierto	SSL/HTTP	Apache
993	TCP	Cerrado	imaps	
995	TCP	Cerrado	Pop3s	
1- 994….	TCP	Filtrado		

Fuente: Elaboración Propia 20 de mayo de 2022

Página Web: https://190.66.1x.xxx/remote/login?lang=en
Dirección IP publica: 190.66.1x.xxx

Tabla 9 Servicios Disponibles Dirección IP 190.66.1x.xxx

Port	Protocolo	Estado	Servicio	Versión
113	TCP	Cerrado		
179	TCP	Abierto	Tcpwrapped	
443	SSL/HTTP	Abierto	Fortinet Securite DEvice Httpd	
1- 997	TCP	Filtrado		

Fuente: Elaboración Propia 20 de mayo de 2022

Página Web: https://190.66.1x.xxx/nextcloud.com
Dirección IP publica: 190.66.1x.xxx

Tabla 10 Servicios Disponibles Dirección IP 190.66.1x.xxx

Port	Protocolo	Estado	Servicio	Versión
25	TCP	Cerrado	smtp	
80	TCP	Abierto	HTTP	Apache
8008	TCP	Abierto	HTTP	
443	TCP	Abierto	SSL/HTTP	Apache
465	TCP	Cerrado	Smtp	
587	TCP	Cerrado	Submission	
1935	TCP	Cerrado	rtmp	
1- 994….	TCP	Filtrado		

Fuente: Elaboración Propia 20 de mayo de 2022

Página Web: https://appvdpar.[redacted].edu.co/
Dirección IP publica: 190.66.1x.xxx

Tabla 11 Servicios Disponibles Dirección IP 190.66.1x.xxx

Port	Protocolo	Estado	Servicio	Versión
53	TCP	Abierta	domain	ISC Bind 9.16.27 **Debian Linux**
80	TCP	Abierto	HTTP	Apache
113	TCP	Cerrada		
179	TCP	Abierta	TCPwrapped	
443	TCP	Abietta	SSL/HTTP	Apache
1- 991….	TCP	Filtrado		

Fuente: Elaboración Propia 05 de junio de 2022

Página Web: https://appvdpar.[redacted].edu.co/
Dirección IP publica: 190.66.1x.xxx

Tabla 12 Servicios Disponibles Dirección IP 190.66.1x.xxx

Port	Protocolo	Estado	Servicio	Versión
53	TCP	Abierta	domain	ISC Bind 9.16.27 **Debian Linux**
80	TCP	Abierto	HTTP	Apache
113	TCP	Cerrada		
179	TCP	Abierta	TCPwrapped	
443	TCP	Abierta	SSL/HTTP	Apache
1- 991….	TCP	Filtrado		

Fuente: Elaboración Propia 05 de junio de 2022

Página Web: campos0d.[redacted].edu.cp
Dirección IP publica: 129.213.170.169
Puerto: 80
Página Web: campos0d.[redacted].edu.cp
Dirección IP publica: 129.213.1xx.xxx
Puerto: 443
Dirección IP publica: 186.118.1xx.0/24

Tabla 13 Dirección IP Publica Disponible Dominio xxxx.edu.co

Dirección IP - Puertos Abiertos
186.118.1xx.xx
186.118. 1xx.xx
186.118. 1xx.xx
186.118. 1xx.xx - 186.118. 1xx.xx
186.118. 1xx.xx - 186.118. 1xx.xx
186.118. 1xx.xx - 186.118. 1xx.xx

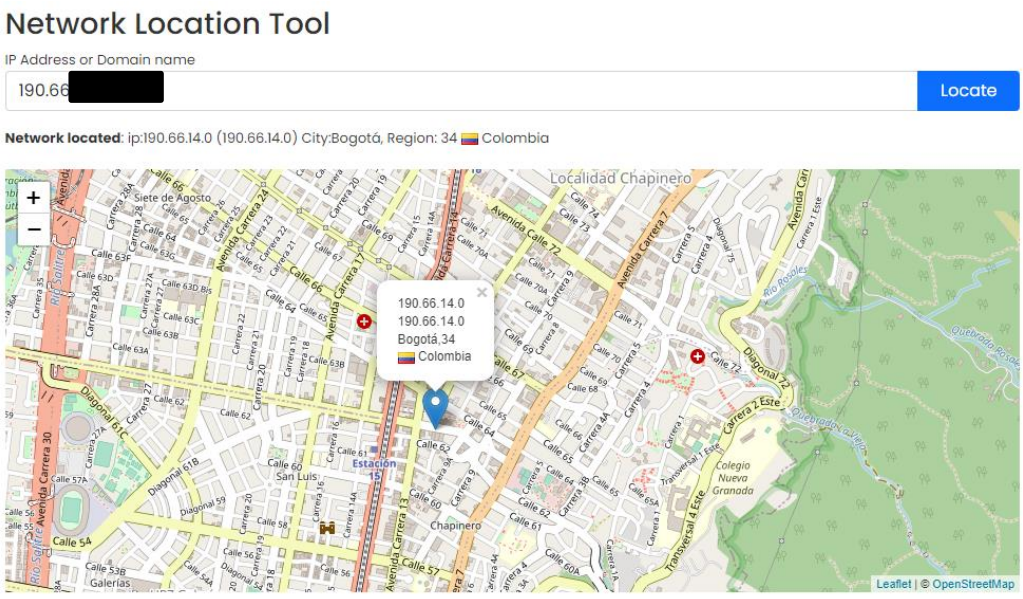
Fuente: Elaboración Propia 05 de junio de 2022

- 186.118.1xx.xx - mail.seabo[redacted]com.co
- 186.118.1xx.xx - appguaji.[redacted].edu.co
- 186.118.1xx.xx - appjag.[redacted].edu.co
- 186.118.1xx.xx - appacaci.u[redacted]edu.co
- 186.118.1xx.xx - appibgue.[redacted].edu.co
- 186.118.1xx.xx - apptunja.[redacted].edu.co
- 186.118.1xx.xx - appbmnga.[redacted].edu.co
- 186.118.1xx.xx - appmllin.[redacted].edu.co
- 186.118.1xx.xx - chatvisae.[redacted].edu.co
- 186.118.1xx.xx - auditoresvisae.[redacted].edu.co
- 186.118.1xx.xx - apppmira.[redacted].edu.co
- 186.118.1xx.xx - appneiva.[redacted].edu.co
- 186.118.1xx.xx - srv-jcm-kweb.[redacted].edu.co
- 186.118.1xx.xx - nubecll53.[redacted].edu.co
- 186.118.1xx.xx - www.ela.[redacted].edu.co
- 186.118.1xx.xx - appsim.[redacted].edu.co
- 186.118.1xx.xx - cronos.[redacted].edu.co
- 186.118.1xx.xx - saturno.[redacted].edu.co
- 186.118.1xx.xx - appjcm.[redacted].edu.co
- 186.118.1xx.xx - appdqueb.[redacted].edu.co
- 186.118.1xx.xx - appstamta.[redacted].edu.co
- 186.118.1xx.xx - appcgena.[redacted].edu.co
- 186.118.1xx.xx - appptocol.[redacted].edu.co

- 186.118.1xx.xx - app0.u[redacted].edu.co
- 186.118.1xx.xxx - mail.[redacted]aludmp.com
- 186.118.1xx.xxx - mail.mailm[redacted].com.co
- 186.118.1xx.xxx - correo.[redacted].com.co

Ubicación Geográfica Dominio InstitucionEducacionSuperior.EDU.CO, ubicado en la Ciudad de Bogotá, DC, Colombia.

Figura 10 Ubicación Geográfica Dominio InstituciónEducacionSuperior.edu.co



Fuente: Tomado de herramienta Network Location Tool de la pagina web https://networkappers.com/. El 5 de julio de 2022

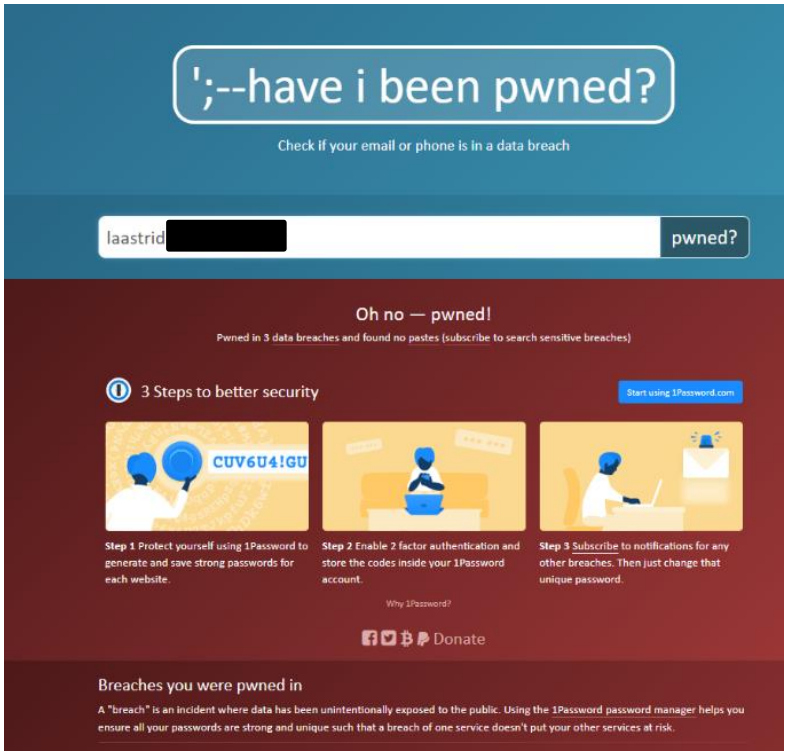
A través de búsquedas avanzadas en los buscadores web Chrome a través de comandos Google Dork Se logra la edificación de información de personal integrante de la Instituto de Educación Superior, dentro de la información disponible en la web se encuentra correos electrónicos institucionales y comerciales, números de teléfono, nombres completos de los funcionarios, los cuales se logra evidenciar que fueron vulnerados o expuestos por cibercriminales de acuerdo a la herramienta haveibeenpwned de la página web https://haveibeenpwned.com/

Link:

- https://www.[redacted]edu.co/images/[redacted]/documentos/atencion-zona-centro-[redacted]-cundinamarca.pdf

- https://www.[redacted].edu.co/images/covid-19/documentos/[redacted]-zona-sur1.pdf
- https://www.[redacted].edu.co/images/covid-19/documentos/atencion-zona-centr[redacted].pdf

Figura 11 Verificación de Usuarios vulnerados o expuestos por cibercriminales**.**



Fuente: Tomado de la herramienta haveibeenpwned de la pagina web https://haveibeenpwned.com/ 15 de junio de 2022

Mediante la herramienta **theHarvester** se logra obtener la siguiente múltiples tipos de información como correos LinkedIn, Dirección IP, Correos Institucionales, Host Disponibles.

Usuarios LinkedIn encontrados: **321 usuarios**.

IP encontradas: **66 host**

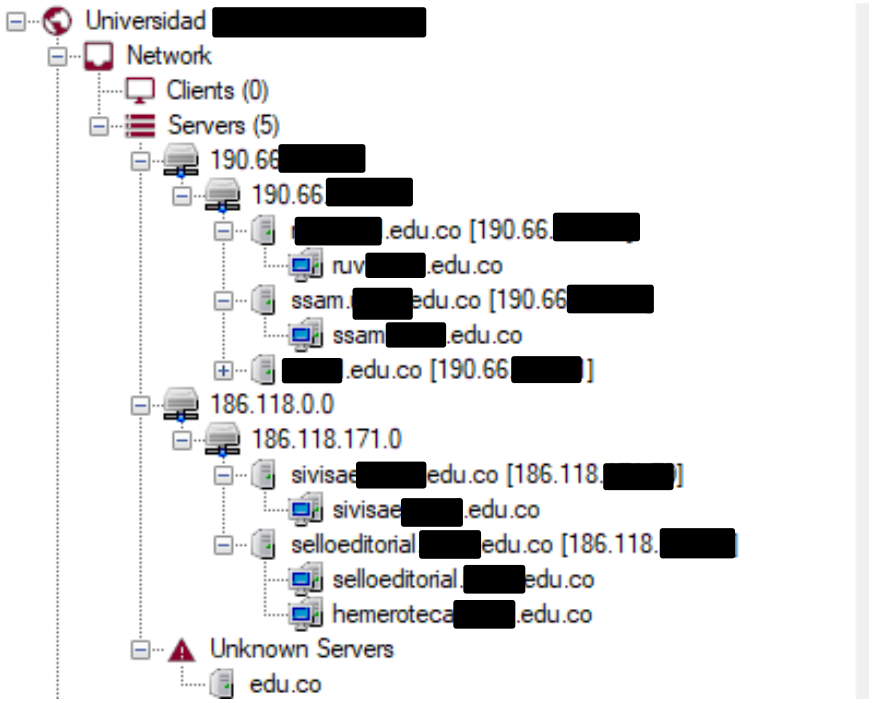
- 45.55.9x.xx
- 66.165.1xx.xxx – 2xx
- 129.150.xx.xxx (Dominion Oracle)
- 129.150.xx.xx (Dominion Oracle)
- 129.150.xx.xx (Dominion Oracle)

- 129.150.xx.xx (Dominion Oracle)
- 129.191.xx.xx – 168 (Dominion Oracle)

Mail institucional @xxxx.edu.co encontrados: **11 @xxx.edu.co**
Equipos disponibles: 766 Host

A través de la herramienta FOCA, se logra la identificación de dos subdominios (190.66.xx.xxx – 186.1xx.xxx) al realizar el volcado de la página instituto de educación superior .edu.co, en el cual se logra la observa los niveles y estructura de red pública disponible.

Figura 12 Subdominios identificados del IES



Fuente: Elaboración Propia mediante la Herramienta FOCA, 27 de junio de 2022

FOCA permite la extracción y análisis de los metadatos, permitiendo identificar los sistemas operativos, software ofimático utilizados en la institución de educación superior, identificación de usuarios que hace parte de la organización de los cuales se obtiene los nombres y apellidos, dirección IP de la red interna, esta información es de gran importancia porque permite a los cibercriminales detectar los diferentes vectores de ataque para acceder a los sistemas de información y afectar la seguridad informática.

Sistemas Operativos disponible en la Red

- CentOs Linux 6.0
- Debian 7.0
- Windows 10
- Windows 7
- Windows XP
- Windows Vista
- Mac OS

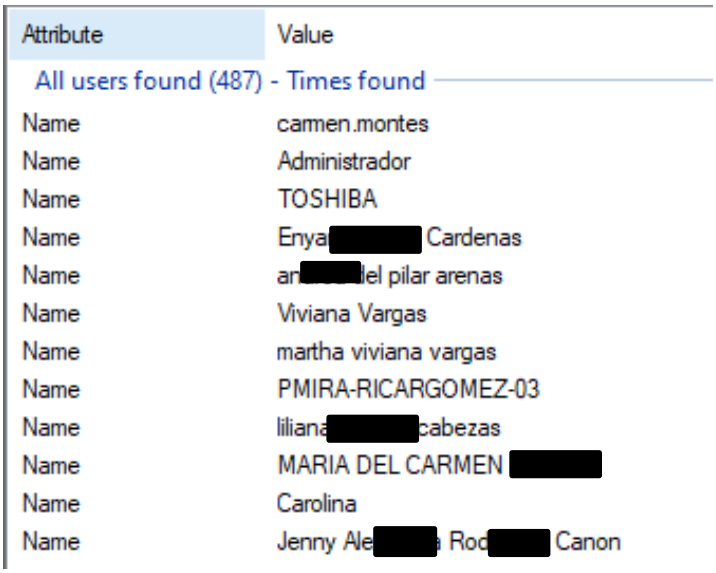
Software:

- Adobe Photoshop CS6 2014
- Adobe Photoshop CS
- OpenOffice
- Microsoft Office 2007
- Microsoft Office 2013
- Microsoft Office 97
- Windows Photo editor 10.0.10011.16384
- Adobe ilustrator CC 2015.3
- Adobe InDesiign CS4 (6.0.6)
- Adobe Acrobat 8.0
- Adobe Indesing 16.4 (Macintosh)
- WPS Office
- Nitro Pro 8 (8.5.5.2) - Nitro Reader 5 (5.5.6.21)
- Ilove PDF.COM
- Core Draw
- Foxit Reader Print 9.3.0
- Kodak Scanner i2000

Usuarios identificados: 480 usuarios.

- Usuarios Administradores:
    - Administrador.edwin.duran@[redacted]

Figura 13 Usuarios Identificados en la red Universidad



Attribute	Value
All users found (487) - Times found	
Name	carmen.montes
Name	Administrador
Name	TOSHIBA
Name	Enya[redacted] Cardenas
Name	an[redacted]del pilar arenas
Name	Viviana Vargas
Name	martha viviana vargas
Name	PMIRA-RICARGOMEZ-03
Name	liliana[redacted]cabezas
Name	MARIA DEL CARMEN [redacted]
Name	Carolina
Name	Jenny Ale[redacted] Rod[redacted] Canon

Fuente: Elaboración Propia mediante la Herramienta FOCA, 27 de junio de 2022

Dirección IP red Interna.

- 172.17.xx.xxx
- 172.17.xx.x
- 10.114.xx.xx
- 192.168.xx.xx
- 192.168.16x.xxx
- 192.168.1xx.xx

Impresoras

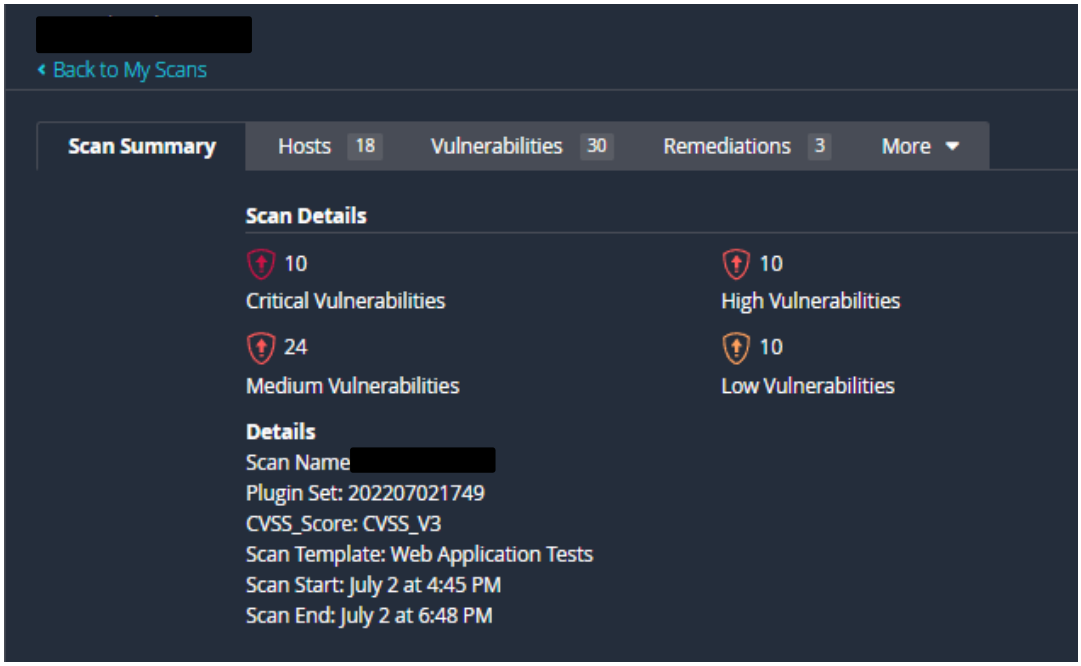
- HP LaserJet 500 MFP M525 PCL
- HP LaserJet M1522 MFP Serie P
- HP LaserJet M4345
- HP LaserJet M3035 Académica
- EPSON L355
- EPSON L200

- HP LaserJet 1200
- HP Deskjet D1 400 Serie
- HP Deskjet 3740 Serie
- Lexmak X646e PS3
- Epson Stylus 600
- Canon MP280

Vulnerabilidades Dominio del Instituto de Educación Superior .EDU.CO.

Mediante la herramienta NESSUS de Tenable se realiza el escaneo y evaluación de vulnerabilidades del dominio unad.edu.co los cuales permite ayudar a identificar los diferentes activos de información, prevenir amenazas y minimizar los riesgos en la seguridad informática, en este caso logro identificar 10 vulnerabilidades Críticos, 24 vulnerabilidades Nicle Media, y 10 vulnerabilidades Bajas.

Figura 14 Resultado Escaneo de Vulnerabilidades Dominio



Fuente: Elaboración Propia mediante la Herramienta NESSUS, 02 de julio de 202

(Nivel Critico)

Host: 190.66.xx.xxx

Detección de protocolo SSL versión 2 y 3, permite explotar estas fallas para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.

Solución

Utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior en su lugar.

Host: 190.66.1x.xxx – 2xx

detección de servidor web no compatible, versión no cuenta con soporte por parte del Servidor

IP: 190.66.1x.2xx

Producto: Apache 2.2.x

Encabezado de respuesta del servidor: Apache/2.2.23 (CentOS)

Versiones compatibles: Servidor Apache HTTP 2.4.x

Vulnerabilidad de denegación de servicio en httpd debido a una falla de des referencia de puntero NULL que se activa cuando un módulo de terceros llama a la función mod_ssl ap_hook_process_connection() durante una solicitud HTTP a un puerto HTTPS.

Vulnerabilidad de denegación de servicio en httpd debido a un error de lectura fuera de los límites en la función ap_find_token() que se activa al manejar una secuencia de encabezado de solicitud especialmente diseñada.

Vulnerabilidad de denegación de servicio en httpd debido a un error al inicializar o restablecer el marcador de posición de valor en [Proxy-]Encabezados de autorización de tipo 'Resumen' antes o entre asignaciones sucesivas de clave=valor por mod_auth_digest

Detección de versión no compatible de PHP, falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Versión instalada: 5.3.29
Fecha de finalización del soporte: 2014/08/14

IP: 190.66.1x.2xx

Producto: Tomcat
Versión instalada: 7.0.90
Soporte finalizado: 2021-03-31
Versiones compatibles: 8.5.x / 9.x / 10.x
Información adicional: http://tomcat.apache.org/tomcat-70-eol.html

Vulnerabilidad de contrabando de solicitudes HTTP en Tomcat debido al mal manejo de los encabezados de codificación de transferencia detrás de un proxy inverso.

vulnerabilidad de lectura de archivos arbitrarios en el protocolo Apache JServ (AJP) de Tomcat debido a un defecto de implementación. Un atacante remoto no autenticado podría explotar esto para acceder a archivos que, en condiciones normales, estarían restringidos. Si la instancia de Tomcat admite la carga de archivos, la vulnerabilidad también podría aprovecharse para lograr la ejecución remota de código. (CVE-2020-1938)

Solución:
Quite el servidor web si ya no es necesario. De lo contrario, actualice a una versión compatible si es posible o cambie a otro servidor, Actualice a Apache versión 2.2.34 o posterior y Actualice a Apache Tomcat versión 7.0.100, 8.5.51, 9.0.31 o posterior; Actualice a una versión de PHP que actualmente sea compatible.

(Nivel Alto)

Host: 190.66.1xx.xxx

Compatible con suites de cifrado de fuerza media SSL (SWEET32), (> 64 bits y < clave de 112 bits, o 3DES)

Solución

Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media.

Host: 190.66.1x.2xx – 2xx:53/UDP

Amplificación de solicitud falsificada de servidor DNS DDoS: El servidor DNS remoto responde a cualquier solicitud. Es posible consultar los servidores de nombres (NS) de la zona raíz ('.') y obtener una respuesta mayor que la solicitud original. Al falsificar la dirección IP de origen, un atacante remoto puede aprovechar esta "amplificación" para lanzar un ataque de denegación de servicio contra un host de terceros utilizando el servidor DNS remoto.

Solución

Restrinja el acceso a su servidor DNS desde la red pública o vuelva a configurarlo para rechazar dichas consultas.

(Nivel Medio)

Host: 190.66.1x.1xx – 1xx

Caducidad del certificado SSL en las fechas

- 3 de enero 23:50:02 2014 GMT
- 11 de septiembre 12:00:00 2020 GMT

El host remoto se ve afectado por una vulnerabilidad de divulgación de información man-in-the-middle (MitM) conocida como POODLE. La vulnerabilidad se debe a la forma en que SSL 3.0 maneja los bytes de relleno al descifrar mensajes cifrados mediante cifrados de bloques en el modo de encadenamiento de bloques de cifrado (CBC).

Certificado SSL firmado con algoritmo hash débil: El servicio remoto utiliza una cadena de certificados SSL que se ha firmado con un algoritmo hash criptográficamente débil (p. ej., MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede explotar esto para generar otro certificado con la misma firma digital, lo que le permite hacerse pasar por el servicio afectado.

Solución:

Compre o genere un nuevo certificado SSL para reemplazar el existente.
Los servicios que deben admitir SSLv3 deben habilitar el mecanismo TLS Fallback SCSV hasta que se pueda deshabilitar SSLv3.

Host: 190.66.1x.2xx

JQuery 1.2 < 3.5.0 Múltiples XSS: la versión de JQuery alojada en el servidor web remoto es mayor o igual a 1.2 y anterior a 3.5.0. Por lo tanto, se ve afectado por múltiples vulnerabilidades de secuencias de comandos entre sitios.

Solución

Actualice a JQuery versión 3.5.0 o posterior

Host: 190.66.1x.2xx

Escáner de modo 6 de protocolo de tiempo de red (NTP). Los dispositivos que responden a estas consultas tienen el potencial de usarse en ataques de amplificación NTP. Un atacante remoto no autenticado podría explotar esto, a través de una consulta de modo 6 especialmente diseñada, para provocar una condición de denegación de servicio reflejada.

Solución

Restrinja las consultas del modo 6 de NTP.

Host: 190.66.1x.2xx – 2xx – 2xx – 2xx

Falta HSTS del servidor HTTPS (RFC 6797): El servidor web remoto no aplica HSTS, según lo define RFC 6797. HSTS es un encabezado de respuesta opcional que se puede configurar en el servidor para indicarle al navegador que solo se comunique a través de HTTPS. La falta de HSTS permite ataques de degradación, ataques de hombre en el medio que eliminan SSL y debilita las protecciones de secuestro de cookies.

Solución

Configure el servidor web remoto para usar HSTS..

(Nivel Bajo)

Host: 190.66.1x.xxx- 2xx

Divulgación de IP interna del encabezado HTTP del servidor web: Esto puede exponer las direcciones IP internas que generalmente están ocultas o enmascaradas detrás de un firewall de traducción de direcciones de red (NAT) o un servidor proxy.

- Servidor: Apache
    - Ubicación: https://192.168.xx.xx/
- Servidor: Apache
    - Ubicación: https://172.19.xx.xx/

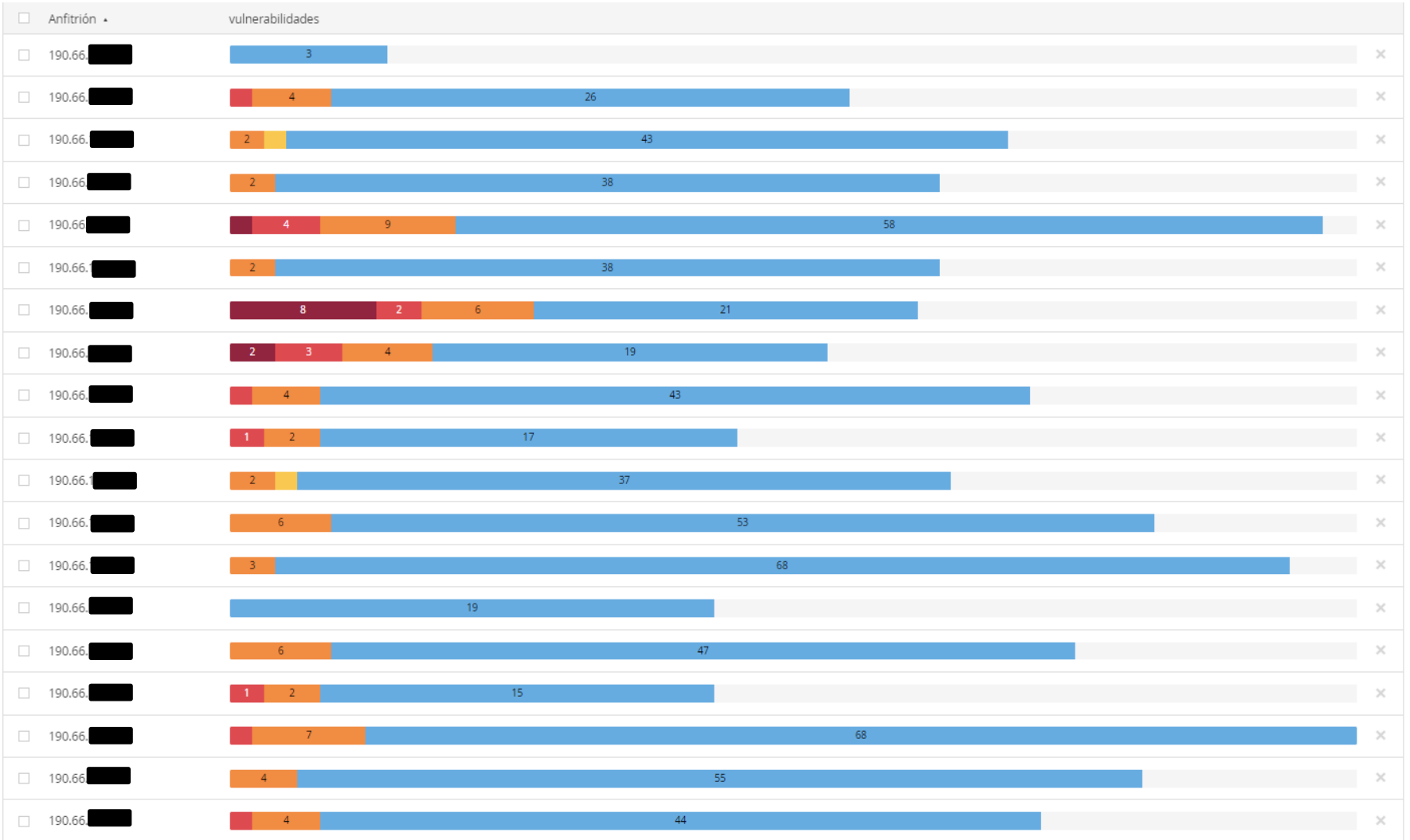
Host: 190.66.1x.1xx – 2xx – 2xx

El servidor web utiliza la autenticación básica sin HTTPS: Un atacante que espía el tráfico podría obtener nombres de usuario y contraseñas de usuarios válidos.

Solución

Asegúrese de que la autenticación HTTP se transmita a través de HTTPS

Figura 15 Vulnerabilidades Identificadas del Dominio Instituto Educación Superior .EDU.CO



Fuente: Elaboración Propia mediante la Herramienta NESSUS WEB CLIENT, 02 de julio de 202

Análisis DOFA:

Amenazas.

Dentro de las amenazas más mencionadas para el ciberespacio podemos establecer el uso del ransomware por parte de los cibercriminales, permitiendo realzar el secuestro de la información. De acuerdo con el informe desarrollado por SOPHOS el noviembre del 2021 los cibercriminales vienen implementando la metodología Ransomware as a Service (RaaS), permitiendo innovar las tácticas, técnicas y procedimientos para acceder a los sistemas de información logrando secuestrar la información y/o extorsionar por divulgación de información confidencial vulnerando la seguridad informática.

El uso de Malware permite acceder a los sistemas informáticos es muy común por parte de los cibercriminales y teniendo en cuenta los sistemas operativos que posee la institución de educación superior por ejemplo el uso del Cobalt Strike permite generar una puerta trasera denominada Beacon a los sistemas operativos Linux; de igual manera los cibercriminales pueden hacer uso del código fuente del Malware con que cuenta la plataforma Metasploit, todo estos software malicioso puede ser distribuido mediante uso de phishing, correo spam, instaladores, entre otros métodos que permitirán acceder de forma remota a los servicios informáticos afectando los principios de la disponibilidad, integridad y disponibilidad de la información.

Los cibercriminales mediante la técnica de ingeniería social desarrollan ataques a los actores internos o insiders vectores de ataque como el Phishing o BEC (Business Email Compromise), técnica de ingeniería social, estudio detallado de la víctima u objetivo, este estudio lo realiza mediante inteligencia de fuentes abiertas (OSINT) e Inteligencia de redes sociales SOCMINT, identificación de infraestructura de Red, logrando detallar información al máximo para implementar el vector de ataque Phising o BEC, afectando la institución de educación superior permitiendo

acceder a los sistemas informáticos, ataques de denegación de servicio (DoS y DDoS) , Doxxing, face new, deepfake, defacements o desconfiguración web y ataque inyección SQL.

Todas estas amenazas pueden afectar la integridad de los sistemas informáticos los cuales pueden ser afectadas la disponibilidad de los servicios e información con que cuenta la institución de educación superior teniendo en cuenta que es un instituto que brinda sus servicios de forma virtual, adicional mente pueden ser afectados los usuarios internos o externos del centro académico, generar consecuencias legales como incumpliendo a la ley de protección de datos personales; así mismo ser afectado Good will de la universidad y afectando la credibilidad y confianza de los stakeholders.

Oportunidades

De las grandes oportunidades que se puede implementar en el instituto de educación superior es capacitar y culturizar al personal integrante de la IES, mediante los diferentes cursos que brinda las diferentes entidades privadas como públicas de forma gratuita, entre ellas puede mencionar las siguientes.

CISCO Networking Academy.

- Introducción a la Ciberseguridad: https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity
- Fundamentos de ciberseguridad https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials

Instituto Nacional de Ciberseguridad INCIBE

- Ciberseguridad para microempresas y autónomos https://www.incibe.es/formacion/ciberseguridad-para-micropymes-y-autonomos

Servicio Nacional de Aprendizaje SENA

- Apropiación de los Conceptos en Ciberseguridad

- Auditoria Informática: Conceptualización
- Controles y Seguridad Informática
- Redes y Seguridad
- Desarrollo de habilidades digitales para experiencias seguras en línea https://ejecuciondelaformacion.sena.edu.co/cursos-cortos

Otras de las oportunidades con que se cuenta para el fortalecimiento de la seguridad informática son los reportes, manuales, guías y herramientas que brindan las diferentes entidades de ciberseguridad.

Centro Criptológico Nacional.

- Ciberamenazas y Tendencias https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

- Guías CCN-STIC de acceso público de defensa frente a las ciberamenazas https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html

Centro Nacional de Ciberseguridad

- Herramientas de ciberseguridad https://www.incibe.es/protege-tu-empresa/herramientas

- Guías de Ciberseguridad https://www.incibe.es/protege-tu-empresa/guias

Fortalezas

Dentro de las Fortalezas que posee la institución de educación superior cuenta con un grupo de especialista en el sistema funcional de Gerencia de Plataformas e Infraestructura Tecnológica, los cuales tiene como objetivo Planear, administrar y suministrar la infraestructura tecnológica de la UNAD, asegurando la disponibilidad de los servicios de Tecnologías de la Información requeridos por los Procesos Misionales, Estratégicos, de Apoyo y Evaluación, para el cumplimiento de los objetivos institucionales[86].

[86] Universidad Nacional Abierta y A Distancia, Gerencia de innovación y desarrollo tecnológico, [En Línea] 02 de julio de 2022 [Fecha de Consulta 05 julio de 2022]. Disponible en: https://gidt.unad.edu.co/

Como funciones principales frente la seguridad de la información establecidas por la Gerencia de Innovación y Desarrollo Tecnológico - GIDT de la UNAD se encarga de los siguientes procesos, así:[87.]

- Evaluar las condiciones técnicas de los recursos tecnológicos de la universidad y realizar su mantenimiento y actualización de manera preventiva y correctiva.
- Evaluar y proponer la incorporación planificada de nuevas y mejores tecnologías para la universidad.
- Garantizar la calidad, el uso racional, la optimización y la seguridad de las tecnologías de la información y las comunicaciones en la universidad.
- Administrar tecnológicamente el sistema integrado de información institucional en sus diferentes componentes, académico, financiero y administrativo y garantizar su seguridad, confiabilidad, precisión y actualidad.

De igual forma cuenta con una política de tratamiento de datos personales[88], como la Política de Privacidad y Condiciones de Uso del Portal del instituto de educación superior, puntualiza las normas, condiciones y las buenas prácticas del uso de la informacion e infraestructura tecnológica con que cuenta la Institución de educación superior con el objetivo de proteger los derechos de los usuarios[89], finalmente cuenta con la Resolución No. 29xx Por la cual se regulan las políticas de seguridad informática y el uso adecuado de la tecnología para el procesamiento de la información de la IES, donde se destaca, así mismo establece las prohibiciones a

[87]Universidad Nacional Abierta y A Distancia, Gerencia de innovación y desarrollo tecnológico, [En Línea] 02 de julio de 2022 [Fecha de Consulta 05 julio de 2022]. Disponible en: https://gidt.unad.edu.co/

[88] Universidad Nacional Abierta y A Distancia, Políticas de Tratamiento de Datos Personales[En Línea] 2019 [Fecha de Consulta 06 julio de 2022]. Disponible en: https://sgeneral.unad.edu.co/images/documentos/capsulas/2019/POLI_TRAT_DATO_PERS_UNAD.pdf

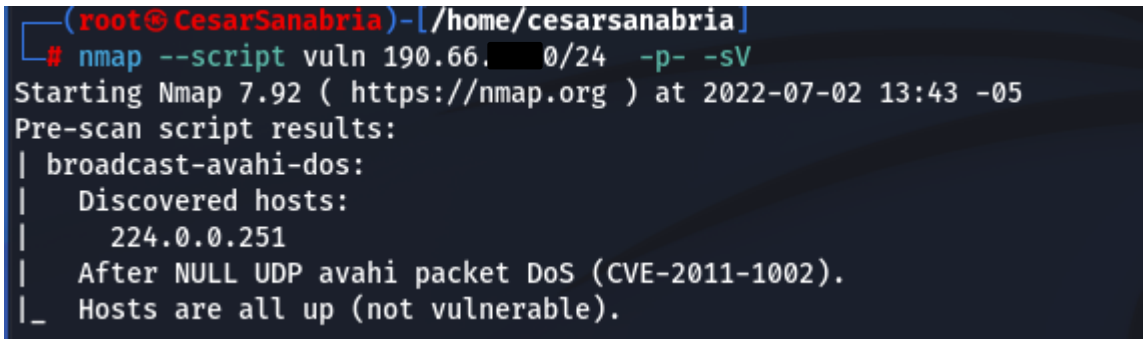
[89] Universidad Nacional Abierta y A Distancia, , [En Línea] 04 de agosto de 2009 [Fecha de Consulta 06 julio de 2022]. Disponible en https://informacion.unad.edu.co/politica-de-privacidad/

los usuarios de la tecnología de la información y las repercusiones legales, disciplinarias y administrativa[90].

De igual forma se logra evidenciar que la IES cuenta con tecnología Firewall que bloquea y limita el Escaneo de la Red a través de la herramienta nmap, en el cual nos reporta que los puertos del dominio se encuentran filtrados, así mismo se evidencia que no es vulnerable a la denegación de servicio del paquete Avahi NULL UDP (CVE-2011-1002), como se observa en la imagen.

nmap --script vuln 190.66.xx.0/24 -p- -sV

Figura 16 Escaneo de Puertos Dominio - Herramienta NMAP

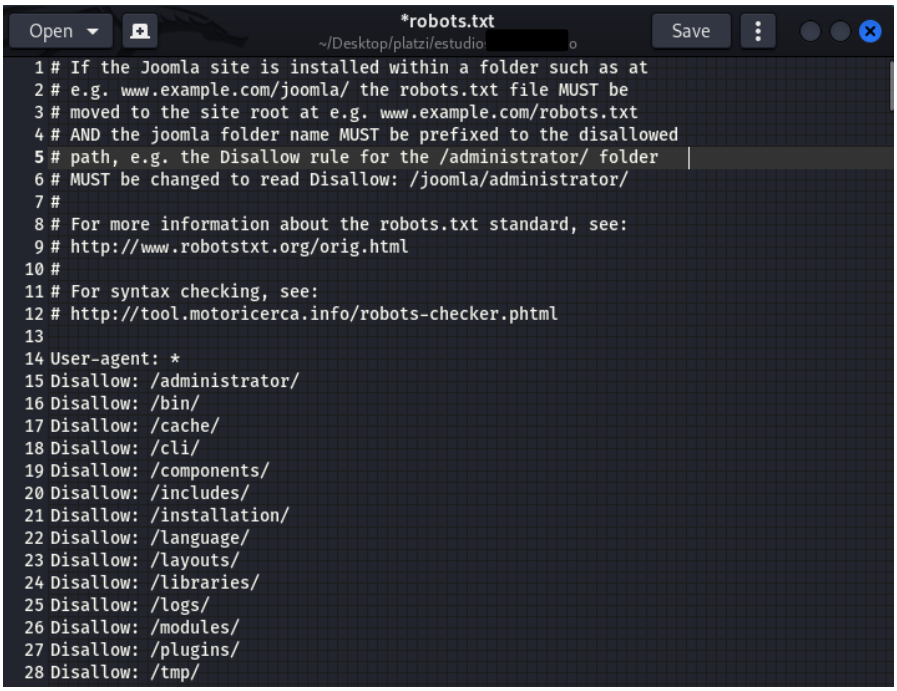


Fuente: Elaboración Propia Tomado del Reporte herramienta NMAP, 02 de Julio de 2022.

Es de rescatar la configuración desarrollada del sitio web de la IES, al momento de analizar el archivo robots.txt (ilustración 8), se encuentra configurada para bloquear el acceso a los archivos indexados, adicionalmente permite gestionar el tráfico de los rastreadores excluyendo archivos como imágenes, videos o archivos PDF.

[90]Jaime Alberto Leal Afanador, Resolución No. 2944 Universidad Nacional Abierta y A Distancia, [En Línea] 04 de agosto de 2009 [Fecha de Consulta 06 julio de 2022]. Disponible en:https://amazonia.unad.edu.co/images/stories/res_2944_2009_regula_politicas_seguridad_informatica.pdf

Figura 17 configuración del Archivo Robots.txt del Dominio



Fuente: Elaboración Propia Tomado del archivo robots.txt domino unad.edu.co del, 20 de Junio de 2022

Debilidades

La universidad cuenta con políticas de seguridad informática mediante la resolución No. 29xx del 2009, por lo anterior se encuentra desactualizada, teniendo en cuenta que ha pasado trece años de haber sido emitida por lo que hoy en día existen nuevos métodos de ataques por parte de los cibercriminales, así mismo han realizado cambio y/o actualización de la infraestructura tecnológica.

De igual forma se logra la identificación de vulnerabilidades de niveles de riesgos críticos, altos, e intermedios en los cuales pueden permitir ataques de denegación de servicios, explotación de acceso remoto a los sistemas informáticos, captación y obtención de información, los cuales no cuenta con sistema de encriptación adecuada (RAS – MD5) y certificados vencidos.

Existe sistemas operativos desactualizados como los Windows y Centos Linux, así mismo software que no contiene parches de seguridad y/o actualizaciones ente ellos

y de gran importancia los servidores Apaches, así como los softwares ofimáticos con que cuenta el instituto de educación superior.

De igual forma se encuentra expuesta informacion de integrantes de la IES, dentro de los datos expuestos podemos mencionar los nombres y apellidos completos, numero de celular, correo electrónico institucional y personal, facilitando a los ciberdelincuentes realizar ingeniería social e inteligencia de fuentes abiertas con ello gestionar vectores de ataques y acceder a los sistemas de informacion personal o institucional.

Conclusión.

Mediante la búsqueda de los datos, análisis y procesamiento de la informacion se logra evidenciar que los sistemas informáticos de la Universidad, posee un nivel intermedio de madurez en seguridad de la informática, teniendo en cuenta los aspectos que pueden incidir como las amenazas del ciberespacio, las debilidades y vulnerabilidades identificadas en los sistemas de información que requieren fortalecer y mejorar las medidas a implementar en la seguridad Informática, así mismo es de reconocer los procesos que viene desarrollan los altos directivos y el equipo de la Gerencia de Plataformas e Infraestructura Tecnológica para preservar los principios de la seguridad de la información, es por ello que se deben adoptar las medidas y guías que posee el ámbito de oportunidades del análisis DOFA e implementar la acción correctiva para minimizar los riesgos de seguridad Informática.

Ing. Cesar Augusto Sanabria Casanova
Estudiante de Especialización Seguridad Informática.
Elaboro.

Reviso:

Visto Bueno y Aprobado:

Versión	Fecha	Cambios Realizados	Responsables
0	5/6/2022	Versión Inicial Informe de Inteligencia de Ciberespacio	Ing. Cesar Augusto Sanabria