Nexo Revista Científica
Vol. 36, No. 05 (Especial), pp. 26-41/Noviembre 2023

ISSN-E 1995-9516
Universidad Nacional de Ingeniería

http://revistas.uni.edu.ni/index.php/Nexo
http://dx.doi.org/10.5377/nexo.vXXiXX.XXXX

Propuesta de creación de un (CSIRT) para el sector gubernamental

Proposal for the creation of a (CSIRT) for the government sector

Leonard Antonio Zamora Espinoza

Facultad de Electrotecnia y Computación. Universidad Nacional de Ingeniería. Managua, Nicaragua.
ing.leonardzamora1989@gmail.com

(recibido/received: 12-abril-2023; aceptado/accepted: 25-junio-2023)

RESUMEN

La presente investigación propone la creación de un centro de repuestas a incidentes cibernéticos (CSIRT), en el sector gubernamental, ante las vulnerabilidades y pérdidas económicas que sufren los gobiernos, por las amanezas de Hackeo en los ciberespacios, en clara violación a la soberanía de los sistemas y la data propia del estado gobierno, por ende esta investigación, la dirigiremos a través de un caso de estudio, en el cual determinaremos los cimientos y la viabilidad de implementación del proyecto CSIRT en el país de Nicaragua, para alcanzar nuestro objetivo desplegaremos una encuesta a funcionarios del departamento de TIC, de las entidades gubernamentales, para recolectar información detallada, en cuanto a la elaboración de los procedimientos de ciberseguridad, administrativos o lineamientos, alineados a un plan de recuperación de desastres, en la prevención y repuestas de acción a ciber ataques, clasificando los niveles de afectación, en la obstaculización del proceso de continuidad del negocio, en este caso los servicios básicos tradicionales de gobierno y en línea.

Palabras claves: Equipo de Respuesta a Incidentes de Seguridad Informática; Plan de Continuidad de Negocio; Plan de Recuperación de Desastres.

ABSTRACT

The present investigation proposes the creation of a cyber incident response center (CSIRT), in the government sector, given the vulnerabilities and economic losses suffered by governments, due to the threats of Hacking in cyberspaces, in clear violation of the sovereignty of the systems and the data of the state government, therefore this investigation, we will direct it through a case study, in which we will determine the foundations and the feasibility of implementing the CSIRT project in the country of Nicaragua, to achieve our objective we will deploy a survey of officials of the ICT department, of government entities, to collect detailed information, regarding the preparation of cybersecurity, administrative procedures or guidelines, aligned to a disaster recovery plan, in prevention and action responses to cyber-attacks, classifying the levels of affectation, in hindering the continuity process continuity of the business, in this case the basic traditional and online government services.

Keywords: Computer Security Incident Response Team; Business Continuity Plan; Disaster Recovery Plan.

1. INTRODUCCIÓN

La revolución de la tecnología de la información y comunicación (TIC), ha acelerado el proceso de globalización y periódicamente sorprende con su constante innovación, La ciberseguridad emerge ante el creciente y uso del ciberespacio como nueva dimensión para la interacción social, en algunos países de América Latina, es considerado parte de la seguridad Nacional del estado, con base jurídica, en este contexto, la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio de manera segura en torno a las ciber amenazas, en el ciberespacio, ya que se integra como un dominio vital para garantizar la seguridad nacional, así como una definición en torno a ciber amenazas al Estado, (Juan, 2020).

El incremento de la cantidad de aparatos conectados al ciberespacio, lo que ha dado origen a la denominada internet de las cosas. Asimismo, la gran cantidad de datos virtuales generados en el ciberespacio ha permitido el desarrollo de "big data" o grandes bases de datos que posibilitan almacenar ingentes cantidades de información y posibilitan el rápido análisis de grandes cantidades de datos de variable naturaleza o formato, (Carolina, 2017).

La investigación propone la creación de un centro de repuestas a incidentes cibernéticos (CSIRT), por sus siglas en inglés, ("Computer Security Incident Response Team") para contar con un plan de acción, ante los ciber ataques de grupos delictivos en su metodología como el: el pishing, watering-hole, ramsonware o ataques DDoS, en el sector gubernamental del país de Nicaragua, ante las vulnerabilidades y pérdidas económicas que sufren los gobiernos, ante las amanezas de ataque o Hackeo en los ciberespacios, en clara violación a la soberanía de los sistemas y la data propia del estado-gobierno. Los equipos de repuestas han ido evolucionando con el paso del tiempo y de acuerdo a las necesidades de las organizaciones, dentro de su portafolio de servicios están servicios de auditoría, análisis y gestión de riesgos en muchas áreas, inclusive en el combate diario contra malware y virus informáticos, se acoplan dentro de un sistema integral de gestión de seguridad que se centran en la prevención y detención de incidentes informáticos, (William, 2020).

La investigación se fundamenta desde un enfoque tipo descriptivo ya que se describirá el propósito del CSIRT y sus tipos de clasificación, el impacto positivo en materia de ciberseguridad y ciberespacio soberano en el fortalecimiento de la estrategia de seguridad Nacional, así como las iniciativas del proyecto CSIRT en el país de Nicaragua, adopción de manuales de buenas prácticas para establecer un CSIRT Nacional, propuestos por organismos internacionales como la organización de estados americanos(OEA, 2016), finalmente nuestra investigación adopta, un enfoque mixto ya que pretende enfrentar la complejidad del problema de investigación planteados en todas las ciencias y de enfocarlos de una manera holística, desde un diseño concurrente, secuencial y de conversión o de integración, según sea los logros, implicara la recolección, análisis e interpretación de datos cualitativos y cuantitativos, (Alfredo, 2018). A través del caso de estudio y su estrategia de Survey, desplegaremos una encuesta tipo cuestionario con escala de Likert, dirigida a diferentes funcionarios de los distintos organigramas del departamento de TI, del gobierno del país de Nicaragua, para determinar la viabilidad del proyecto a gran escala en términos de desarrollo tecnológico.

Desplegaremos el Survey de manera anónima, a través de la plataforma interactiva de SurveyMonkey (https://es.surveymonkey.com/), a los participantes en colaboración para recolectar información detallada, en cuanto a la elaboración de los procedimientos o alineamientos de ciberseguridad, administrativo, alineados a un plan de recuperación de desastres, en la prevención y repuestas de acción a ciber ataques, Para determinar los cimientos pioneros y la viabilidad de implementación del proyecto CSIRT en el gobierno de Nicaragua, ya que actualmente no cuenta, con una entidad centralizada para la adecuada gestión de los incidentes cibernéticos que atenten contra la defensa del espacio de ciberseguridad del Gobierno de Nicaragua, para realizar de manera eficiente la gestión de sus riesgos.

Pero a nivel internacional existen proyectos e iniciativas por organizaciones no gubernamentales e internacionales como LACNIC ("Registro de Direcciones de Internet de América Latina y Caribe"), como el proyecto Amparo en sus dos, fases al igual que la organización de los estados americanos (OEA) con guías de buenas prácticas para establecer un CSIRT Nacional, desde el proceso de análisis, gestión y puesta en marcha del CSIRT Nacional, por ende, este articulo científico estará guiado por un marco teórico en su estructuración para determinar el desarrollo del estudio.

2. MARCO TEORICO Y ESTADO DEL ARTE

La organización de estados americanos por sus siglas en español (OEA), a través del Comité interamericano contra el terrorismo (CICTE), aborda los asuntos de Seguridad Cibernética. reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio".

Destacan entre los objetivos que se han propuesto los siguientes:
El establecimiento de grupos nacionales de 'alerta, vigilancia y prevención', también conocidos como equipos de respuesta a incidentes (CSIRT) en cada país; crear una red de alerta Hemisférica que proporciona a formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética; y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio (OEA y CICTE 2017).

La gobernabilidad de todo sistema político requiere al menos considerar tres factores: seguridad como condición, institucionalidad como medio y desarrollo como objetivo. En este contexto, la ciberseguridad constituye una condición para permitir que los ciudadanos, las organizaciones e instituciones puedan beneficiarse del uso del ciberespacio como dimensión en la cual las relaciones sociales pueden efectuarse en forma más rápida y económica en comparación con otras formas conocidas de intercambio de información. (Carolina, 2017).

La organización no gubernamental e internacional LACNIC ("Registro de Direcciones de Internet de América Latina y Caribe") promueve dentro de esta organización a sus países miembros realizar los reportes en materia de ciber incidentes, siguiendo los procesos de reporte y clasificación de los ataques, hasta el nivel de criticidad, lo cual el país de Nicaragua, no forma parte de esta organización, no cuenta con un CSIRT a nivel nacional, a nivel internacional, se determinó que existen iniciativas del proyecto denominado Amparo, en 2 fases de implementación, la cual tomaremos como un marco de referencia en cuanto a la construcción del CSIRT en el país de Nicaragua ya que aún este, no forma parte de ese proyecto. (https://csirt.lacnic.net/el-proyecto-amparo).

CSIRT: La organización de los estados americanos OEA define un CSIRT como "Un equipo de respuesta a incidentes en seguridad informática, por sus siglas en inglés (CSIRT Computer Security Incident Response Team) es una organización cuyo propósito principal consiste en brindar servicios de respuesta a incidentes de seguridad informática a una comunidad en particular".
CSIRT Gubernamentales: Los equipos de respuesta gubernamentales se encargan de garantizar que todos los servicios de gobierno en Tecnologías y de la información, así como los servicios prestados a la ciudadanía cuenten con los niveles de seguridad adecuados y recomendados según sea el escenario o ambiente de desarrollo de los gobiernos, por ende, los CSIRT gubernamentales deben amoldarse a las necesidades del estado o gobierno donde se implementen, se centran en proteger la infraestructura por medio del cual el gobierno les brinda servicios a los ciudadanos.

CSIRT Nacional: Estos equipos nacionales juegan un papel de organización nacional y un punto de contacto, ante la presencia de una amenaza o evento de seguridad informática. La función de este CSIRT depende de los roles que se desempeñen, así como de la presencia de otros equipos de respuesta. Podría mencionarse este equipo de respuesta como uno que engloba a los demás equipos dentro de una nación, en donde juega un papel organizativo importante. (William, 2020).

CSIRT de Infraestructuras Críticas: Brindan sus servicios para proteger las infraestructuras críticas de un país de ataques e incidentes de seguridad de la información y pueden ser administrados por organizaciones públicas o privadas. la definición de infraestructura crítica: "son todas las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuyo proceder o destrucción el cual tendría un impacto en algunos temas como en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas" (Andrés, 2021).

Plan de Recuperación de desastre (DRP): es el proceso planificado que una organización utiliza para recuperar el acceso a su infraestructura (software, datos y / o hardware) que son necesarios para reanudar el ejercicio de las funciones normales de trabajo, críticos después del evento catastrófico; ya sea por un desastre natural o por una catástrofe causada por los seres humanos, cuyo propósito es la protección de los Datos. (Leonard y Cedrick 2020)

En el desarrollo del estado del arte documental se determinó que a nivel nacional del país de Nicaragua existe al menos un caso de estudio con fines académicos para la Universidad Nacional de Ingeniería, con la intención de documentar el posible funcionamiento de un Centro de Monitoreo de Seguridad, (SOC, por sus siglas en inglés, Security Operation Center,) y de un Equipo de Repuestas a Incidencias de Seguridad (CSIRT, por sus siglas en inglés, Computer Security Incident Response Team) (Javier, 2016), a la vez se determinó que a nivel de gobierno de Nicaragua no existe una entidad centralizada que gestione proactivamente la prevención y detención de incidentes informáticos, solo existe una ley especial de ciberdelitos para regular la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las TIC, en perjuicio de personas naturales o jurídicas. Sin embargo, a nivel de América Latina, se destacan estudios de mayor relevancia, de diseños de un Centro de Respuesta a Incidentes de Seguridad Informática para la comunidad de finanzas en el Ecuador, donde se determinan presupuestos, recursos operativos, del CSIRT, procedimientos de manejo de incidente en etapas definidas: Gestión de Registro, Gestión del Problema, Gestión de Incidentes, Gestión de Capacidad y Gestión de Servicio; de la cual se establecen lineamientos y acciones a seguir según el caso, (Danny, 2022). Iniciativas de la organización LACNIC (El Registro de Direcciones de Internet de América Latina y Caribe), con el Proyecto Amparo en dos informenes de fases para contribuir al desarrollo de Internet en la región mediante una política activa de cooperación. (LACNIC-CSIRT 2010), Así como Manuales de buenas prácticas para establecer un CSIRT Nacional, de la OEA por sus siglas en español (Organización de Estados Americanos) que promueve el desarrollo integral de las Américas. (OEA, 2016), a nivel académico proyectos de diseño y políticas que brindan los lineamientos de actuación del Centro de Respuesta a Incidentes Informáticos, (Andrés, 2021). A nivel privado referencias de casos de estudios de propuestas técnicas para la creación de un CSIRT para la empresa. cibersecurity de Colombia, Ltda. En dos fases para la elaboración del diseño de la estructura tecnológica y centro de operaciones, levantamiento de hardware y software, (Alex, 2020). Estudios de estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad Nacional aún, cuando el liderazgo descanse, en principio, en el Estado, la ciberseguridad constituye un compromiso social que demanda de articulación entre el sector público y el sector privado, por ende, la ciberseguridad tiene que ser parte de la seguridad Nacional de un país. (Juan et al. 2019).

3. DISEÑO DE INVESTIGACIÓN

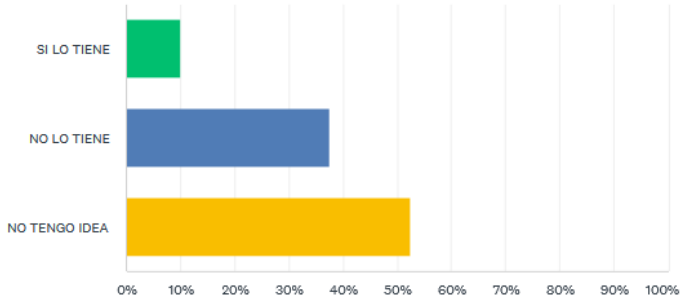
Para nuestro alcance a nivel práctico, utilizamos los métodos mixtos que proporcionan un enfoque sofisticado y complejo para la investigación que atrae a quienes están a la vanguardia de los nuevos

procedimientos de investigación, A través del método científico para generar nuevo conocimiento, la recolección de datos cuantitativos y cualitativos a través de nuestro Survey, nos permitirá analizar por separado las perspectivas extraídas de datos cuantitativos y cualitativos, (Leonard y Cedrick 2020).

La investigación se rigió, desde un enfoque tipo descriptivo ya que se describió el propósito del CSIRT y sus tipos de clasificación, el impacto positivo en materia de ciberseguridad y ciberespacio soberano en el fortalecimiento de la estrategia de seguridad Nacional, así como las iniciativas del proyecto CSIRT en el país de Nicaragua, adopción de manuales de buenas prácticas para establecer un CSIRT Nacional, propuestos por organismos internacionales, y finalmente nuestra investigación adopto un enfoque mixto ya que pretende enfrentar la complejidad del problema de investigación planteados en todas las ciencias y enfocarlos de una manera holística, desde un diseño concurrente, secuencial y de conversión o de integración, según sea los logros, implico la recolección, análisis e interpretación de datos cualitativos y cuantitativos, (Alfredo 2018). A través del caso de estudio y su estrategia de Survey, se desplego la encuesta tipo cuestionario con escala de Likert, a través SurveyMonkey (https://es.surveymonkey.com/), que es una plataforma interactiva de tecnologías de información, para aplicar encuestas en línea, se dirigió a diferentes funcionarios de los distintos organigramas del departamento de TI, del gobierno del país de Nicaragua, para determinar la viabilidad del proyecto a gran escala en términos de desarrollo tecnológico.

El componente de caso de estudio, en su estrategia de (Survey) se desarrolló y se desplego a través de la plataforma iterativa de SurveyMonkey en el periodo comprendido desde el día 03 de febrero hasta 31 de marzo del año 2023, a diferentes funcionarios del departamento de TI de principales instituciones del estado de Nicaragua, actores claves en cuanto a nivel académico, nivel de experiencia y perfil profesional, así como Docentes del programa de maestría en gestión tecnologías de Información MGTIC, de la universidad nacional de ingeniería y su facultad electrotécnica y computación, compañeros de maestría de la Edición Gobierno, que en su mayoría son funcionarios de gobierno, así como aspirantes a PhD de la Universidad de las Américas (UAM), los cuales conforman una comunidad científica en el país de Nicaragua, de cara a los avances tecnológicos, Por razones de confidencialidad se omiten, nombres de las instituciones de gobierno.

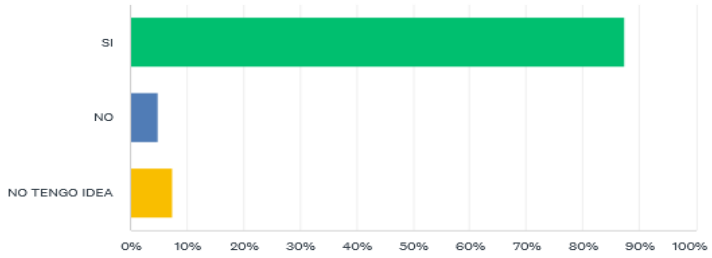
Para homogenizar nuestros objetivos, ante la problemática existente de no contar con un CSIRT Nacional en el país de Nicaragua, se aplicará las fases de desarrollo: Teoría, conceptualización, metodología y estadística, por ende, nuestra población de estudio fue de 50 funcionarios del departamento de TI, de instituciones gubernamentales, Universidades Públicas y Sector Privado, para determinar la viabilidad del proyecto. A través, de la herramienta calculadora de muestra de Surveymonkey. El tamaño de la población a estudiar fue de 50 profesionales de TI, nivel de confianza del 95 % y margen de error del 5%, nuestra, muestra representativa o estadística fue de 45 que es la cantidad de respuestas completas que la encuesta recibió, sin embargo, la plataforma Surveymonkey, debido al límite de la cuenta registrada, para recopilar información, que no es de categoría Enterprise, automáticamente te limita a 40 repuestas visibles nos refleja la cantidad de 65 participantes, 40 repuestas visibles en la práctica, de ser así, debido al condicionamiento de participación automático del sistema, según la herramienta calculadora del tamaño de la muestra (https://es.surveymonkey.com/mp/sample-size-calculator/) en cuanto al límite del tamaño de población 40 participantes, que la propia plataforma de SurveyMonkey nos condiciono, a un nivel de confianza del 95% y margen de error del +- 5%, el tamaño de la muestra es de 37 repuestas de participantes, queremos recalcar que en la practica estos datos se superaron, por ende nuestra encuesta supero el 100% de la meta de recopilación de datos de acuerdo a lo planificado, lo cual justifica la viabilidad de desarrollar el proyecto CSIRT en el país de Nicaragua, como un proyecto de vanguardia. a continuación, se presentará el Survey: Propuesta de Creación de un Centro de Repuestas a Incidentes Cibernéticos (CSIRT) Para el Sector Gubernamental (Caso de Estudio), que está conformado por 10 preguntas con repuesta en opciones de escala de Likert, a la vez se mostrara las opciones de repuesta y las repuestas en sí, con porcentajes estadísticos, este es link generado por la plataforma, con su actualización de encuesta cerrada y número de serie de la encuesta: https://es.surveymonkey.com/r/J77SCLK



OPCIONES DE RESPUESTA	RESPUESTAS	
SI LO TIENE	10,00 %	4
NO LO TIENE	37,50 %	15
NO TENGO IDEA	52,50 %	21
Total de encuestados: 40		

Figura 1, ¿Tiene conocimiento si actualmente la Administración Pública de Nicaragua, cuenta con un (CSIRT: Equipo de repuesta a Incidentes Cibernéticos), ¿ante un ciberataque en el ciberespacio a Nivel Nacional? Fuente: https://es.surveymonkey.com/r/J77SCLK

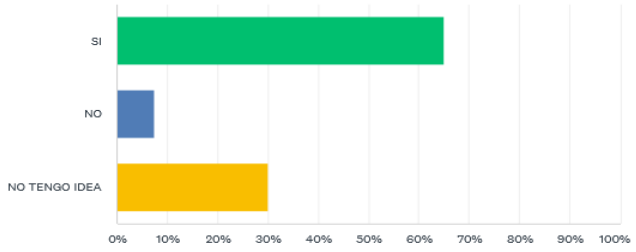
En el análisis de la figura.1 : se determina que el 50% de los participantes no tiene idea de lo que es un CSIRT, equipo de repuesta de incidentes Cibernéticos, un 40 % No tiene el conocimiento y un 10% si tiene el conocimiento.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	87,50 %	35
NO	5,00 %	2
NO TENGO IDEA	7,50 %	3
Total de encuestados: 40		

Figura. 2 ¿Considera Necesario contar con un CSIRT Nacional coordinado por alguna entidad de gobierno para asegurar los servicios TIC, en el sector gubernamental? Fuente: https://es.surveymonkey.com/r/J77SCLK

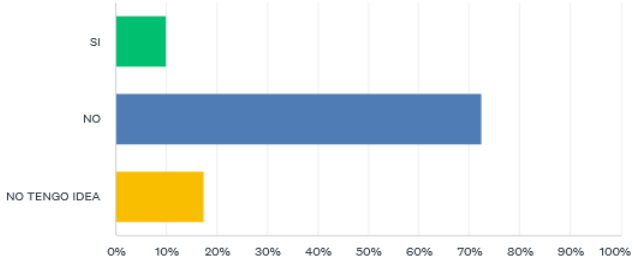
En el análisis de la figura. 2: el 90 % de los participantes, consideran necesario contar con un CSIRT Nacional, coordinado por alguna entidad de gobierno, un 5% No está de acuerdo y un 10% No tiene idea.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	65,00 %	26
NO	7,50 %	3
NO TENGO IDEA	30,00 %	12
Total de encuestados: 40		

Figura. 3 ¿Su Organización está dispuesta a conformar el equipo CSIRT a Nivel Nacional, si fuera invitada por el Gobierno? Fuente: https://es.surveymonkey.com/r/J77SCLK

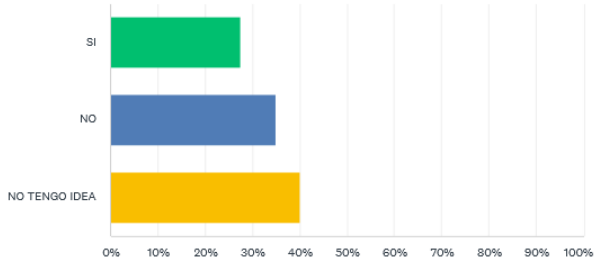
En el análisis la Figura.3: el 65 % de los participantes los cuales representan a las instituciones que están dispuestos a conformar el equipo CSIRT a nivel nacional, un 5% de participantes No está de acuerdo y el 30% de los participantes No tiene idea.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	10,00 %	4
NO	72,50 %	29
NO TENGO IDEA	17,50 %	7
Total de encuestados: 40		

Figura. 4 ¿Según la información disponible y de acuerdo a su experiencia, considera que están preparadas las Instituciones gubernamentales para detectar a tiempo una amenaza Nacional, del ciberespacio? Fuente: https://es.surveymonkey.com/r/J77SCLK

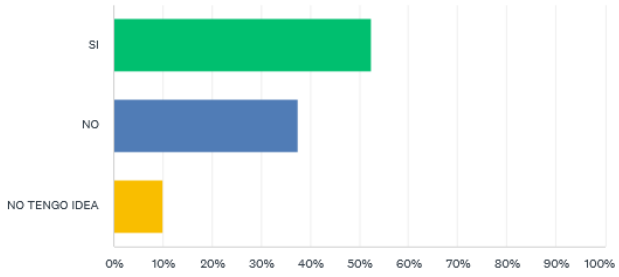
En el análisis de la Figura.4: el 10% de los participantes consideran que las instituciones de gobiernos están preparadas para detectar a tiempo una amenaza en el ciberespacio, el 75% consideran que No están preparadas y el 18 % No tiene idea.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	27,50 %	11
NO	35,00 %	14
NO TENGO IDEA	40,00 %	16
Total de encuestados: 40		

Figura. 5 ¿Existen políticas, procesos o procedimientos para un centro de repuestas de incidentes informáticos que contemple las Normas Técnicas de Control Interno (NTCI)? Fuente: https://es.surveymonkey.com/r/J77SCLK

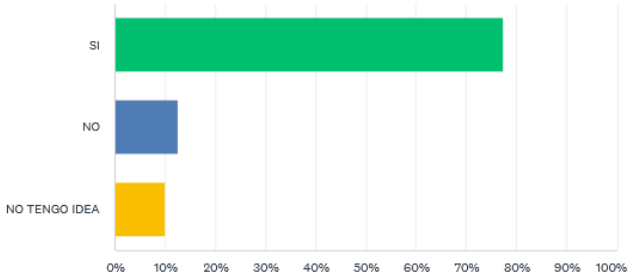
En el análisis de la Figura.5: se determina que el 40 % de los participantes no tiene idea, en cuanto a los procesos o procedimientos para un CSIRT que contemple las normas técnicas de control interno, un 35 % de participantes No cuentan con procesos y un 28% de participantes dicen que si cuentan con procesos.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	52,50 %	21
NO	37,50 %	15
NO TENGO IDEA	10,00 %	4
Total de encuestados: 40		

Figura. 6 ¿Tiene Conocimiento del marco normativo legal respecto a la seguridad informática del ciberespacio a Nivel Nacional? Fuente: https://es.surveymonkey.com/r/J77SCLK

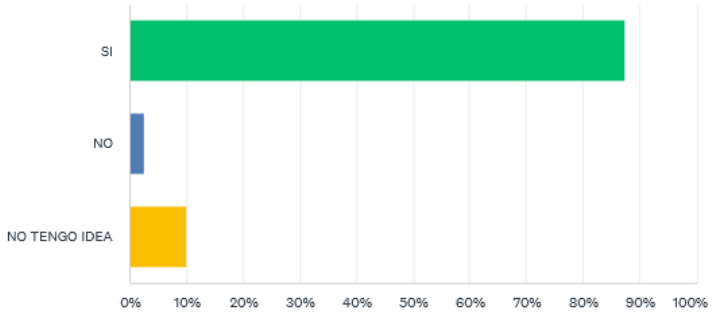
En el análisis de la Figura. 6: el 53% de participantes, determino que Si tiene conocimiento del marco normativo legal, respecto a la seguridad informática del ciberespacio, un 37 % No tiene conocimiento y un 10% No tiene idea del marco Jurídico.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	77,50 %	31
NO	12,50 %	5
NO TENGO IDEA	10,00 %	4
Total de encuestados: 40		

Figura. 7 ¿Considera usted que, al momento de contar con un CSIRT Nacional, las administraciones de TI, estarían brindando un mejor servicio gubernamental, así como contribuiría a la buena gestión de alineamiento estratégico? Fuente: https://es.surveymonkey.com/r/J77SCLK

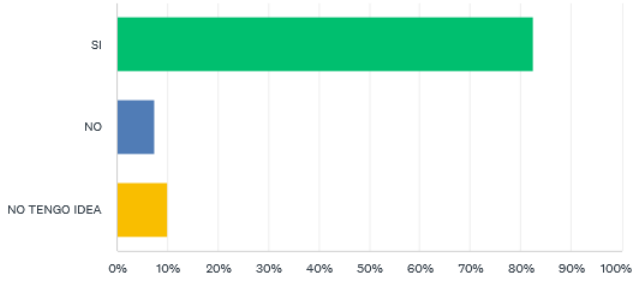
En el análisis de la Figura. 7: el 79 % de los participantes, consideran que al momento de contar con el CSIRT Nacional, las instituciones gubernamentales, estarían brindando un mejor servicio y contribuiría al alineamiento estratégico de cada plan estratégico institucional, un 12 % No esta de acuerdo y un 10 % no tiene idea.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	87,50 %	35
NO	2,50 %	1
NO TENGO IDEA	10,00 %	4
Total de encuestados: 40		

Figura. 8 ¿Es importante para usted contar con un (DRP: ¿Plan de Recuperación Ante Desastre), como plan de contingencia para asegurar el ciberespacio ante un ciber incidente a nivel nacional en las administraciones públicas del gobierno de Nicaragua? Fuente: https://es.surveymonkey.com/r/J77SCLK

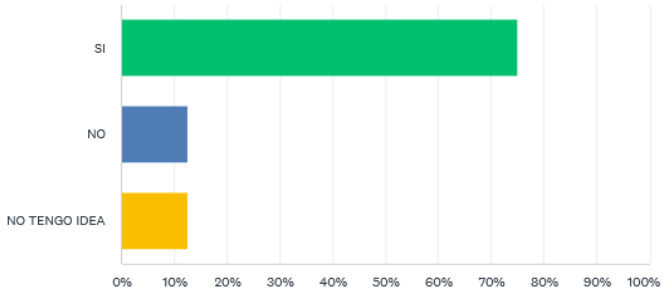
En el análisis de la Figura. 8: se determina que el 89 % de los participantes, están de acuerdo de contar con un DRP para asegurar el ciberespacio, ante un ciber incidente en las instituciones del estado, esto como un plan de contingencia, así como un 2% No esta de acuerdo y 10 % no tiene idea del beneficio de contar con un plan de recuperación ante desastres, de restablecimientos de las tecnologías de la información.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	82,50 %	33
NO	7,50 %	3
NO TENGO IDEA	10,00 %	4
Total de encuestados: 40		

Figura. 9 ¿Conoce usted los riesgos o amenazas cibernéticas, las cuales pueden impactar significativamente en las diferentes plataformas de servicios de TI, así como la interrupción de los servicios de gobierno en línea? Fuente: https://es.surveymonkey.com/r/J77SCLK

En el análisis de la Figura. 9: se determino que el 82 % de los participantes conoce los riesgos o amenazas cibernéticas, las cuales pueden impactar significativamente los servicios de TI, de las instituciones gubernamentales entre ellos servicios tradicionales y en línea, un 8% No conoce los riesgos y un 10 % de los participantes no tiene idea.



OPCIONES DE RESPUESTA	RESPUESTAS	
SI	75,00 %	30
NO	12,50 %	5
NO TENGO IDEA	12,50 %	5
Total de encuestados: 40		

Figura. 10 ¿Considera Usted que una vez implementado el Proyecto CSIRT en el sector gubernamental de Nicaragua, estaría abriéndose paso al e-Gobierno: (Gobierno Electrónico) para mejorar la calidad de los servicios públicos? Fuente: https://es.surveymonkey.com/r/J77SCLK

En el análisis de la Figura. 10: se determino que el 76 % de los participantes, consideran que una vez la puesta en marcha del proyecto CSIRT nacional en el país de Nicaragua, este mismo se estaría abriendo paso, al e- Gobierno: Gobierno Electrónico, para mejorar la calidad de sus servicios, un 10 % No y un 12 % no tiene idea de la brecha de beneficios.

4. RESULTADOS Y DISCUSIÓN

A través del método científico y el método de investigación del Survey, nos dio la oportunidad preliminar de analizar sistemáticamente la información generada por la plataforma de TI. Surveymonkey, en la homogenización de nuestros objetivos, ante la problemática existente de no contar con un CSIRT Nacional en el país de Nicaragua, se aplicó las fases de desarrollo: Teoría, conceptualización, metodología y estadística, por ende, nuestra población de estudio abarco instituciones gubernamentales, universidades Públicas y Sector Privado del país de Nicaragua, los resultados estadísticos reflejados anteriormente, consideramos de vital importancia, ya que nos determina la viabilidad del proyecto. A pesar de que contamos con una cuenta comercial limitada en la plataforma de SurveyMonkey, el sistema automáticamente nos limita a analizar 40 participantes, sin embargo, en la práctica, sobrepasamos nuestras metas, de ser así como anteriormente mencionamos, debido al condicionamiento automático de procesamiento de repuestas del sistema, según la herramienta calculadora del tamaño de la muestra (https://es.surveymonkey.com/mp/sample-size-calculator/) en cuanto al límite del tamaño de población asumiendo los 40 participantes, que la propia plataforma de SurveyMonkey nos condiciono, a un nivel de confianza del 95% y margen de error del +- 5%, el tamaño de la muestra es de 37 repuestas de participantes, queremos recalcar que en la práctica estos datos se superaron, por ende nuestra encuesta supero el 100% de la meta de recopilación de datos recopilados de acuerdo a lo planificado.

Debido a la naturaleza de nuestro proyecto investigativo, para determinar el nivel de pertinencia y valoración de la propuesta modélica este se realizó directa e indirectamente a través del criterio de expertos del método Delphi, a través del Survey, sin embargo para estudios a futuros se recomienda realizar dos etapas, la primera etapa: cuestionario para los expertos: recopilación de datos generales, institución donde labora, años de experiencia y nivel académico, auto evaluación a través de la argumentación, La argumentación para determinar el coeficiente de argumentación. La segunda etapa: Selección de los Expertos: determinar la cantidad de expertos a participar, calidad o competencia de expertos, retroalimentación con todas las entidades gubernamentales. (Félix et al. 2021) y finalmente presentar Informenes ejecutivos, todos los resultados, encontrado oficialmente al gabinete de gobierno del país de Nicaragua.

Hemos decido innovar en este articulo científico, debido a que la inteligencia artificial (IA), ha pasado la barrera del campo académico, su trascendencia en el campo de la gestión, administración pública y gobierno, (Ocaña et al, 2021), por lo tanto, hemos tomado en cuenta la argumentación o consulta de las herramientas de Inteligencia Artificial, como lo es el ChatGPT: (https://chat.openai.com/) se preguntó ¿Es posible implementar un Proyecto CSIRT en el país de Nicaragua? El cual respondió: Sí, es posible implementar un proyecto CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática, por sus siglas en inglés) en Nicaragua. A continuación, te mencionaré algunos elementos que se necesitan para implementar un proyecto CSIRT:

Financiamiento: Es necesario contar con un presupuesto que permita el establecimiento y operación del proyecto CSIRT. Esto incluye la contratación de personal especializado, la adquisición de equipos y herramientas, así como la realización de capacitaciones y entrenamientos.

Personal especializado: Es fundamental contar con un equipo de expertos en seguridad informática que puedan responder de manera efectiva a los incidentes de seguridad que se presenten. Este equipo debe estar conformado por profesionales con conocimientos en áreas como la detección y análisis de incidentes, la gestión de vulnerabilidades, la gestión de incidentes y la respuesta a incidentes.

Infraestructura: Se requiere de una infraestructura adecuada para el almacenamiento de registros y datos de seguridad, así como para el monitoreo de la red y la detección de amenazas.

Procedimientos y políticas: Es importante contar con procedimientos y políticas bien definidas para la gestión de incidentes de seguridad. Estos documentos deben establecer los protocolos de actuación y las responsabilidades del equipo de CSIRT.

Coordinación: El proyecto CSIRT debe coordinarse con otros equipos y entidades que trabajan en seguridad informática en Nicaragua, como, por ejemplo, la policía nacional, las empresas de telecomunicaciones, entre otros.

Conciencia de seguridad: Es importante generar conciencia en la población y en las empresas sobre la importancia de la seguridad informática y la necesidad de reportar incidentes de seguridad.

A continuación, segunda repuesta de consulta de ChatGPT: (https://chat.openai.com/):

Para establecer un equipo de respuesta a incidentes de seguridad informática a nivel nacional en el gobierno de Nicaragua, se necesitan varios elementos clave:

1. Financiamiento: El gobierno de Nicaragua debe asignar recursos financieros adecuados para la creación y operación del CSIRT.
2. Personal capacitado: Se requiere personal con experiencia y habilidades técnicas en seguridad informática y gestión de incidentes.
3. Infraestructura: El CSIRT debe tener una infraestructura de tecnología de la información adecuada para realizar sus actividades, incluyendo hardware, software y comunicaciones.
4. Procedimientos y políticas: El equipo debe contar con procedimientos y políticas claras y bien definidas para la gestión de incidentes y la coordinación con otras agencias del gobierno y del sector privado.
5. Relaciones interinstitucionales: Es importante establecer relaciones inter institucionales con otros organismos y organizaciones nacionales e internacionales para compartir información y conocimientos sobre seguridad informática.
6. Capacitación y concientización: El equipo debe estar comprometido en proporcionar capacitación y concientización a otros departamentos y agencias gubernamentales, así como al público en general, sobre los riesgos de seguridad informática y las mejores prácticas para protegerse contra ellos.
7. Evaluación y mejora continua: El CSIRT debe realizar evaluaciones periódicas de sus capacidades y procesos, y tomar medidas para mejorar su eficacia y eficiencia.

En resumen, para establecer un CSIRT Nacional en el gobierno de Nicaragua, es necesario contar con el respaldo financiero adecuado, personal capacitado y una infraestructura de tecnología de la información adecuada, además de contar con políticas y procedimientos claros, relaciones interinstitucionales y un compromiso de mejora continua.

El compromiso político es esencial para establecer un CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) en el país de Nicaragua. La creación de un CSIRT a nivel nacional es una iniciativa estratégica y política que requiere la voluntad política y el apoyo del gobierno de Nicaragua para llevarla a cabo.

El compromiso político se manifiesta en la asignación de recursos financieros, la promoción de una cultura de seguridad informática, la elaboración de políticas y estrategias nacionales de ciberseguridad, la promoción de alianzas con otros países y organizaciones internacionales, y el establecimiento de marcos legales que faciliten la acción del CSIRT.

Además, la creación de un CSIRT puede ser parte de la estrategia del gobierno de Nicaragua para fortalecer su capacidad de respuesta a amenazas cibernéticas, proteger los intereses nacionales, y promover el desarrollo sostenible y la estabilidad económica. En conclusión, el compromiso político es necesario para establecer un CSIRT en el país de Nicaragua y garantizar su éxito a largo plazo.

La siguiente pregunta que se realizó al ChatGPT: (https://chat.openai.com/)

¿Contar con un CSIRT Nacional en el país de Nicaragua, estaría fortaleciendo la Agenda 2030?

La creación de un CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática) nacional en Nicaragua podría contribuir a fortalecer la Agenda 2030 en varios aspectos. En primer lugar, la seguridad informática es un aspecto clave para el desarrollo sostenible, ya que la ciberseguridad es esencial para proteger la privacidad y los derechos digitales de los ciudadanos, así como para garantizar la continuidad de los servicios esenciales, como la salud y la educación.

En segundo lugar, el establecimiento de un CSIRT nacional podría mejorar la capacidad del país para prevenir, detectar y responder a los incidentes de seguridad informática, lo que podría contribuir a reducir los riesgos de ciberseguridad para las empresas y los ciudadanos. Esto podría a su vez fomentar el crecimiento económico y el desarrollo tecnológico, que son objetivos importantes de la Agenda 2030.

Por último, el establecimiento de un CSIRT nacional también podría contribuir a mejorar la cooperación regional e internacional en materia de ciberseguridad, lo que es un elemento clave para lograr los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030.

En resumen, contar con un CSIRT nacional en Nicaragua podría contribuir significativamente a fortalecer la Agenda 2030 en varios aspectos clave relacionados con la seguridad informática, el desarrollo económico y la cooperación internacional.

La siguiente pregunta que se realizó al ChatGPT: (https://chat.openai.com/)

¿Cuáles son esos aspectos claves relacionados de implementación del proyecto CSIRT en el país de Nicaragua?

La implementación de un proyecto CSIRT en Nicaragua requeriría abordar varios aspectos clave para asegurar su éxito y contribuir al fortalecimiento de la seguridad informática y la Agenda 2030. Algunos de estos aspectos podrían incluir:

1. Marco legal: Es importante contar con un marco legal claro y robusto que establezca las funciones, responsabilidades y autoridad del CSIRT. Además, se deben establecer mecanismos

claros para garantizar la protección de los derechos digitales de los ciudadanos y la privacidad de los datos personales.

2. Financiamiento: El financiamiento es un aspecto clave para la implementación y sostenibilidad del CSIRT. Es importante contar con un presupuesto adecuado para el personal, la infraestructura y el equipamiento necesario para el funcionamiento del CSIRT.
3. Personal capacitado: El éxito de un CSIRT depende en gran medida de la experiencia y la capacitación de su personal. Es importante contar con un equipo multidisciplinario que incluya expertos en seguridad informática, análisis de datos, gestión de incidentes y comunicación.
4. Infraestructura y herramientas: El CSIRT necesita contar con la infraestructura y las herramientas necesarias para monitorear, detectar y responder a los incidentes de seguridad informática. Esto incluye sistemas de alerta temprana, herramientas de análisis de datos, software de seguridad y sistemas de comunicación.
5. Cooperación y coordinación: El CSIRT debe establecer mecanismos de cooperación y coordinación con otros organismos nacionales e internacionales de seguridad informática, para garantizar una respuesta rápida y efectiva a los incidentes de seguridad informática y para promover la cooperación regional e internacional en materia de ciberseguridad.

En resumen, la implementación de un proyecto CSIRT en Nicaragua requeriría abordar aspectos clave como el marco legal, el financiamiento, el personal capacitado, la infraestructura y herramientas y la cooperación y coordinación para garantizar el éxito y contribuir al fortalecimiento de la seguridad informática y la Agenda 2030.

La responsabilidad de la implementación del CSIRT en Nicaragua recae en el gobierno y las autoridades encargadas de la seguridad informática y ciberseguridad del país. Es importante que exista un compromiso y liderazgo por parte de las autoridades para impulsar y respaldar la implementación del proyecto CSIRT.

En cuanto al financiamiento del proyecto CSIRT, es posible obtener recursos sin aumentar la deuda externa del país. Una opción sería buscar financiamiento a través de cooperación internacional y acuerdos de colaboración con otros países y organismos internacionales. Además, se podría explorar la posibilidad de buscar financiamiento a través de la inversión del sector privado y la colaboración con universidades y centros de investigación.

En el caso de que se opte por la cooperación internacional, es importante tener en cuenta que existen programas y fondos específicos para el desarrollo de capacidades en ciberseguridad, los cuales pueden ser una fuente de financiamiento para el proyecto CSIRT. Estos programas suelen contar con una amplia gama de recursos, incluyendo asistencia técnica, capacitación y transferencia de tecnología.

En cuanto al bajo PIB del país, esto puede ser un desafío para la implementación del proyecto CSIRT, pero también puede ser una oportunidad para buscar soluciones creativas y eficientes para el uso de los recursos disponibles. Por ejemplo, se podría considerar la colaboración con otros países de la región para compartir recursos y conocimientos en materia de ciberseguridad, o bien, la colaboración con organizaciones internacionales para aprovechar su experiencia y recursos en este ámbito.

5. CONCLUSIONES

Los resultados de la estrategia de Survey como componente del caso de estudio para nuestro articulo científico y sobre todo la valoración del criterio de expertos del método Delphi, directo e indirectamente, nos permitió determinar la viabilidad del proyecto CSIRT en el país de Nicaragua, pero también es necesario determinar la factibilidad financiera, talento humano, simulación y ciclo de los procesos de gestión, en un posible escenario de operatividad, para que el Proyecto CSIRT, sea una realidad en la era

Digital, del país de Nicaragua y se abra paso al desarrollo tecnológico a nivel latino americano y caribeño es necesario la inversión y apoyo del Ejecutivo, del presidente de la Nación, un consenso entre las organizaciones privadas y públicas, así como organizaciones internacionales, para la defensa del Gobierno, en términos de ciberespacio soberano, con el objetivo de realizar de manera eficiente la gestión de sus riesgos y proteger los activos tecnológicos en cuanto a data, sistemas de TI y artefactos, ya que hay una constante evolución de los ciberataques a nivel mundial, de esta manera el gobierno país, en su estrategia nacional, lograra fortalecer las capacidades públicas, para enfrentar las amenazas latentes en el ciberespacio, apostando por la estandarización internacional, de esta manera adoptara un modelo de seguridad y privacidad de las tecnologías de información y comunicación en el país de Nicaragua.

REFERENCIAS

Alex, A.B.C. 2020 Propuesta técnica para la creación de un centro de repuesta a incidentes de cibernéticos para la empresa Caso de estudio Cibersecurity de Colombia Ltda. Tesis de Pregrado Universidad Nacional Abierta a Distancia UNAD, Bogotá.

Alfredo, O. O. 2018 Enfoques de investigación Tabla de Contenido Universidad del Atlántico

Andrés, V. N. 2021 Diseño de las políticas principales para la actuación del centro de repuesta a incidentes informáticos de la universidad nacional abierta a distancia CSIRT-UNAD. Tesis de pregrado, Bogotá D.C.

Carolina, S. H. 2017, Ciberseguridad. Presentación del dossier, URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20 - Quito, junio 2017 - pp. 8-15, ISSN 1390-4299.

Danny, J.A.C. 2022 Propuesta de creación de Centros de Respuesta a Incidentes de Seguridad Informática como Estrategia de Ciberseguridad para medios de pagos digitales Tesis de la Universidad de Guayaquil. DOI: http://dx.doi.org/10.17141/urvio.20.2017.2859

Félix, O. Sixto R. 2021 método Delphi Dirigido a la Validación de un Modelo de Evaluación Institucional Revista Científica Scientiarium, (2), Universidad Fermín Toro Venezuela, ISSN No :18568688

Javier, A.G.V. 2016 Propuesta de diseño e implementación de un Centro de Operaciones de Seguridad (SOC) y un Centro de Repuesta a Incidencias (CSIRT) para la Universidad de Ingeniería, Tesis de Maestría en Gestión de la Seguridad de la Información, UNI.

Juan, M. A. A. 2020 Presente y futuro de los retos de la ciberseguridad en México, una propuesta para la seguridad nacional", Revista Legislativa de Estudios Sociales y de Opinión Pública, vol. 13, 2020 pp. 83-120 (fcpys) de la Universidad Nacional Autónoma de México.

Juan, O. Israel, B. 2019 Estrategias Integradas de Ciberseguridad para el fortalecimiento de la seguridad Nacional Tesis Doctoral, centro de altos estudios nacionales, escuela de posgrados CAEN. Lima Perú.

LACNIC, CSIRT, 2010. Proyecto AMPARO Fortalecimiento de la Capacidad Regional de atención de incidentes de Seguridad en América Latina y el Caribe, Número de Donación de IDRC: 105237 Sitio web: https://csirt.lacnic.net/el-proyecto-amparo

Leonard, A.Z.E. Cedrick, D. 2020 Plan de Recuperación de Desastres y Restablecimiento de las Tecnologías de Información en el Sector Gubernamental ISLA 2020 Proceedings. 14. https://aisel.aisnet.org/isla2020/14

Ocaña F. Yolvi, V. Fernández, L. A. Vera, F. Miguel, A. Rengifo, L. Raúl, A. 2021 Inteligencia artificial (IA) aplicada a la gestión pública, Revista Venezolana de Gerencia, 2021, vol. 26, núm. 94, ISSN: 1315-9984.

OEA, 2016, [En línea] Buenas Prácticas para establecer un CSIRT nacional. [Consulta 10 de marzo del 2023]. Disponible en: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

William, A. F. R. 2020 Diseño de un centro de repuesta a incidentes de seguridad informática CSIRT en la empresa Platino Sistemas, Tesis de la Universidad Nacional Abierta a Distancia UNAD TUNJA-BOYACA.

SEMBLANZA DE LOS AUTORES

Leonard Antonio Zamora Espinoza: Obtuvo el grado de Ingeniero Electrónico en la Universidad Nacional de Ingeniería, Nicaragua, en el año 2012, posteriormente estudios de posgrados en gerencia estratégica de las TIC, en el año 2017, Título de Especialista en Tecnologías de Información y Comunicación en el año 2018, Certificación Internacional MSS/SOC por Deloitte cyber Academy en el año 2019, Egresado del programa de Maestría en Gestión Tecnologías de Información y Comunicación de la Facultad de Electrotécnica y Computación UNI-FEC, en el año 2020, Conferencista Internacional del evento AMCIS-ISLA2020 LACAIS, Asociación de Tecnologías de Información de América Latina y el Caribe, obteniendo el certificado de reconocimiento, como uno de los mejores videos de investigación de la conferencia. Siete años de experiencia profesional comprobada en el ámbito de Tecnologías de Información, en cuatro instituciones del estado de Nicaragua.