RESUMEN – TRABAJO DE GRADO

AUTORES	**Didier Fernando Guerrero Sumalave**
FACULTAD	**Facultad de Ingenierías**
PLAN DE ESTUDIOS	**Maestria en Gobierno de TI**
DIRECTOR	**Torcoroma Velásquez Pérez** **Co-director Luis Manuel Palmera Quintero**
TÍTULO DE LA TESIS	**Modelo De Gestión De Ciberseguridad Para Resolver Incidentes En Instituciones De Educación Superior**
TITULO EN INGLES	**Cybersecurity Management Model to Resolve Incidents in Higher Education Institutions**

RESUMEN
(70 palabras)

La implementación de un modelo que permita la gestión de incidentes recomienda el establecimiento de medidas apoyadas en los estándares y normas necesarios que permitan asegurar que la red, servidores, voz y datos afectados, los sistemas de información, así como los recursos técnicos necesarios para su correcto funcionamiento. funcionamiento de la entidad, y todo lo posible La relación de la persona que actúa sobre ellos. En la actualidad los ciberataques se han incrementado significativamente, entre los cuales es importante realizar un proyecto encaminado a desarrollar un modelo de localización y orientación de las vulnerabilidades a las que pueden estar expuestas las instituciones de educación superior

RESUMEN EN INGLES

The implementation of a model that allows the management of incidents recommends the establishment of measures supported by the necessary standards and norms that make it possible to ensure that the network, servers, voice and data affected, the information systems, as well as the technical resources necessary for its correct operation. operation of the entity, and as much as possible The relationship of the person acting on them. At present, cyber attacks have increased significantly, among which it is important to carry out a project aimed at developing a model for the location and orientation of vulnerabilities to which higher education institutions may be exposed.

PALABRAS CLAVES	Gestión-Ciberseguridad, Incidente, Educación Superior
PALABRAS CLAVES EN INGLES	Management-Cybersecurity, Incident, Higher Education

CARACTERÍSTICAS

PÁGINAS: 138	PLANOS:	ILUSTRACIONES:	CD-ROM:

Modelo De Gestión De Ciberseguridad Para Resolver Incidentes En Instituciones De Educación Superior

Autor:

Didier Fernando Guerrero Sumalave

Facultad de Ingenierías, Universidad Francisco de Paula Santander Ocaña

Maestría en gobierno de Tecnología de la Información

Doc. Torcoroma Velásquez Pérez

Doc. Luis Manuel Palmera Quintero

Ocaña, Marzo de 2023

Índice

Lista de figuras

Lista de tablas

Capitulo 1. Modelo de gestión de ciberseguridad para resolver incidentes en Instituciones de Educación Superior

1.1 Planteamiento del problema

La industria de la seguridad de la información se enfrenta actualmente a desafíos sin precedentes debido a diversas amenazas que surgen en el entorno digital. El 73% de las empresas del mundo han sufrido un ciberataque y muchas ni siquiera se dan cuenta. Entonces, los avances tecnológicos han tenido un gran impacto y durante el último año, con el auge de la tecnología y los cambios por los que ha tenido que pasar toda la humanidad debido al covid-19, ha generado la adopción de nuevos modelos de negocios como el trabajo remoto adaptado. (Portafolio, 2022) Por otro lado, Troya (2023) explica que se estima que más de 1,5 millones de usuarios en todo el mundo son víctimas de ciberdelincuencia todos los días, lo que lleva a un aumento del 28 % de los ciberataques en el tercer trimestre de 2022.

La ciberseguridad en la educación superior es una tarea interminable, ya que no es raro que sus departamentos de TIC tengan exceso de trabajo y, a veces, escasez de personal. Si bien los ataques cibernéticos contra instituciones de educación superior datan de varios años, las universidades han visto un aumento en la cantidad de ataques cibernéticos contra instituciones de educación superior en los últimos dos años. Así lo revela Manjarres (2022), donde muestra: En 2021, la industria de la educación reportó un total de 1241 incidentes, de los cuales 282 fueron filtraciones de datos confirmadas, y las amenazas externas fueron el principal incidente, representando el 75 % del número total de casos. De manera similar, Verinzon (2022) explicó que las brechas de seguridad de datos aumentaron en más del 30 % en el mismo año y encontró

que el 34 % de los errores identificados por el departamento se debieron a que los correos electrónicos se enviaron a la persona equivocada o con un archivo adjunto incorrecto.

Las instituciones educativas de educación superior y primaria son cada vez más atacadas por ransomware, según una encuesta realizada por la revista Eleconomista (2022), que muestra que el 60% de las instituciones serán atacadas en 2022, en comparación con 2021. La proporción es del 44%. Las instituciones de educación superior informaron la mayor probabilidad de impacto comercial y operativo de un ataque de ransomware, y el 97 por ciento de los encuestados en el estudio informaron que el ataque afectó su capacidad para operar.

Biddle (2017) señaló que los colegios y universidades a menudo son entornos densamente poblados que requieren acceso a diversos recursos y publicaciones en línea para realizar investigaciones, así como aplicaciones y soluciones de software para registrar, presentar y compartir resultados de investigación, dado este fenómeno. , a nivel internacional, en el año 2020, en la Universidad Mayor de San Andrés, Bolivia, se realizó una encuesta denominada "Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT", cuyo principal objetivo es seguir los lineamientos de la norma ISO 27035 Política para hacer frente adecuadamente a las ciberamenazas que se están dando actualmente dentro de la empresa. (Vargas, 2020, p. 1)

A nivel nacional, en la Fundación Universitaria Unipanamericana - Compensar en Bogotá, Colombia, se llevó a cabo un proyecto de grado denominado "Modelo de Ciberseguridad de la Corporación Colombiana de Carga Espacial (SPC)", cuyo objetivo principal fue crear un modelo de seguridad basado en el estándar ISO 27002, la seguridad en Internet permite a las empresas obtener un mayor control sobre la seguridad informática de la organización. (Gómez et al., 2019, p. 17) Por otro lado, a nivel local de la Universidad Francisco de Paula Santander - Ocaña, se desarrolló una carrera denominada "Modelo de Ciberseguridad para Entidades

Financieras Alineado al Marco de Referencia de Gestión TI" Proyectos y Governance"; donde se realizan mapeos consistentes con el marco de referencia más aceptado a nivel mundial para fortalecer la segunda línea de defensa de las entidades financieras, permitiendo la construcción de modelos de ciberseguridad relacionados con la gestión y el gobierno de TI. (Barbosa, 2020, p. 16)

No hace mucho, la Universidad Popular Cesar - Seccional Aguachica fue golpeada por un ataque tipo ransomware que no pudo ser detectado y mitigado, lo que ocasionó pérdidas importantes de información, riesgos ocasionales en la red y ataques informáticos que intentaron acceder a la computadora resultando en robo de información. o daño al sistema. De acuerdo con el modelo, se espera implementar medidas de seguridad informática dentro de la organización para dar soporte al SGSI (Sistema de Gestión de Seguridad de la Información) de la Universidad.

1.2 Formulación del problema

¿Cuáles deben ser los componentes que conformen un modelo de ciberseguridad que permita una adecuada gestión de incidentes en las instituciones de educación superior?

1.3 Objetivos

1.3.1 Objetivo General

Diseñar un Modelo de ciberseguridad para la gestión de incidentes en instituciones de educación superior.

1.3.2 Objetivos específicos

- Examinar el estado actual de los riesgos inherentes en que se encuentran las instituciones de educación superior.

- Establecer los lineamientos y características para el diseño del modelo de ciberseguridad para resolver incidentes en las instituciones de educación superior.

- Validar el modelo propuesto para la gestión de incidentes en la Universidad popular del cesar seccional Aguachica.

1.4 Justificación

Cualquier organización que gestione sistemas y tecnologías de la información está expuesta a riesgos y ciberataques que pueden poner en peligro su correcto funcionamiento. Para proteger la información se deben poner en práctica normas, reglamentos, leyes, acuerdos, políticas y demás información que ayuden a gestionar la información Ciberseguridad, para proteger los sistemas de información e infraestructura, optimizar estos recursos que contribuyen al crecimiento y es desarrollar La base de la estrategia organizacional. Una de las formas en que se puede utilizar para determinar la postura de seguridad de una empresa es a través de una evaluación de riesgos. (Gómez et al., 2019)

La implementación de un modelo que permita la gestión de incidentes recomienda el establecimiento de medidas apoyadas en los estándares y normas necesarios que permitan

asegurar que la red, servidores, voz y datos afectados, los sistemas de información, así como los recursos técnicos necesarios para su correcto funcionamiento. funcionamiento de la entidad, y todo lo posible La relación de la persona que actúa sobre ellos. En la actualidad los ciberataques se han incrementado significativamente, entre los cuales es importante realizar un proyecto encaminado a desarrollar un modelo de localización y orientación de las vulnerabilidades a las que pueden estar expuestas las instituciones de educación superior, analizando la situación actual y los recursos informáticos con los que cuentan actualmente. tener, para que pueda determinar el modelo de negocio adecuado Modelos de aseguramiento de redes y contribuciones a los campos de sistemas y telecomunicaciones, teniendo en cuenta datos relevantes para fortalecer la gestión de seguridad de redes. (Remolina, 2019, p. 10)

Desde el punto de vista de Rodríguez (2019), las instituciones que reducen las inversiones en gestión de riesgos pueden encontrar que no pueden ajustar fácilmente sus capacidades si se imponen nuevos requisitos. Visto desde esta perspectiva, nos muestra que las instituciones están buscando un enfoque más amplio, coordinado e innovador para gestionar con éxito las oportunidades y los desafíos derivados del riesgo, como un factor innovador que tiene el poder de transformar la gestión de eventos para controlar los riesgos emergentes Capacidad.

De esta manera, la ciberseguridad en el entorno de las instituciones educativas cobra gran relevancia, considerando que la institución tiene como objetivo de negocio la optimización de los servicios que brinda. Así, como una optimización de los procesos administrativos asociados al cumplimiento de las normas, reglamentos y estándares relacionados con las amenazas. (Palafox, 2019)

Para la Universidad del Cesar Popular - Seccional Aguachica, la adecuada gestión de los eventos de riesgo derivados de ataques de ciberseguridad sería un factor innovador dentro de las instituciones educativas el cuales brindan una estructura sólida, y estan sustentada en políticas y

controles para la seguridad de la información, esto se brindará dentro de la institución un qué hacer para prevenir futuros ciberataques. Además, este proyecto de investigación será de gran beneficio para otras instituciones educativas y para la Universidad Francisco de Paula Santander - Ocaña, donde servirá como referencia teórica que podrá ser replicada en futuros estudios o en otras universidades.

1.5 Delimitaciones

1.5.1 Delimitación Operativa

El desarrollo del proyecto establece desde el punto operativo una metodología de tipo cuantitativa, el cual brindara herramientas para recolectar información el cual es fundamental para las instituciones de educación superior.

1.5.2 Delimitación Conceptual

Se obtendrá información de los conceptos existentes limitando a trabajar con la aplicación de estándares asociados al uso adecuado de las tecnologías de la información, Cobit 2019, ciberseguridad, gestión de incidentes y riesgos inherentes.

1.5.3 Delimitación Geográfica

En cuanto a la posición geográfica donde se realizará este modelo de ciberseguridad es en la Universidad Popular del Cesar – Seccional Aguachica de la ciudad de Aguachica, Cesar.

1.5.4 Delimitación Temporal

Esta tesis de grado tiene como objetivo la aprobación de la investigación en un periodo de estudio que será de 12 (doce) meses a partir de la aprobación del proyecto.

Capítulo 2. Marco Referencial

2.1 Antecedentes

La ciberseguridad tiene como objetivo proteger la información digital en los sistemas interconectados, incluida la información dentro de los límites de seguridad, y lograr la protección de los activos de información al abordar las amenazas que ponen en riesgo la información procesada, almacenada y transmitida por los sistemas de información interconectados en las instituciones educativas. Para visualizar mejor los referentes teóricos relacionados con los estudios, se tomaron en cuenta estudios internacionales, nacionales y locales de la siguiente manera:

2.1.1 Ámbito Internacional

El proyecto de grado realizado por Santolaria, denominado “Desarrollo de una metodología para la gestión de incidentes de ciberseguridad en una organización”, en la ciudad de Catalunya, España Su principal objetivo es abordar cuestiones incuestionables en la gestión de riesgos de ciberseguridad y respuesta a incidentes, brindando la orientación necesaria para el cumplimiento de la obligación de reportar los incidentes de ciberseguridad ocasionados por las entidades. (2022, p. 7)

La metodología utilizada por los autores se basa en un estándar denominado ENS (Event Response Capability for Security) de correcta implementación para fortalecer la seguridad. Por lo tanto, desarrollar políticas y procedimientos adecuados para implementar las medidas previstas en la norma, registrando cada incidente que ocurra. Esta investigación es de tipo procedimental,

permitiendo el análisis para poner en práctica una serie de procesos y creando estrategias para construir métodos. (Santolaria, 2022)

El autor concluye que es necesario invertir en seguridad, contar con sistemas que faciliten la gestión protegiendo contra ataques inminentes y la disponibilidad de recursos humanos. Por lo tanto, hacer saber a las personas que la comunicación es clave para una adecuada gestión de crisis, identificar todos los grupos de interés debe identificarse de antemano, y siempre hay que saber qué decir a quién y cómo. (Santolaria, 2022, p. 53)

Robayo (2022) realizó un proyecto denominado “Modelo para Mejorar la Ciberseguridad en la Provincia de Tungurahua” en Ambato, Ecuador. Su principal objetivo es desarrollar un modelo que permita identificar los modelos de ciberseguridad existentes desde una perspectiva técnica, posibilitando su síntesis y generación de buenas prácticas al interior de las organizaciones para proteger los activos de información de las entidades gubernamentales.

Los métodos utilizados en el desarrollo de este estudio fueron: Descriptivo, Documental y Analítico, ya que se estudiaron los tipos, formas y consecuencias de los ciberataques, ayudando a entender su información de manera clara y concisa, para de esta manera permitir el desarrollo de modelos para mejorar la ciberseguridad de las entidades gubernamentales, comprobando o refutando las hipótesis planteadas en la investigación. La metodología empleada en el estudio es cualitativa ya que se enfoca en comprender el fenómeno de la realidad investigada desde diferentes perspectivas, lo que incentiva el proceso inductivo del estudio. (Robayo, 2022, p. 44)

el autor logra concluir que, con base en las respuestas obtenidas a través de encuestas a los profesionales que trabajan en el gobierno, es preocupante que las autoridades gubernamentales no estén preparando al personal para ataques cibernéticos contra los funcionarios involucrados en su trabajo Peligros potenciales para los activos de información. (Robayo, 2022, p. 109)

De la misma manera, Vilcarromero & Vilchez (2018) realizaron un proyecto de grado el que fue titulado “Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones”; teniendo como un elemento clave de la investigación es dotar al dominio SOC de un marco de ciberseguridad para generar una solución que le permita implementar, operar, monitorear, revisar y mejorar los controles de ciberseguridad para ser más competitivo a nivel empresarial.

El tipo de investigación utilizado en este proyecto es cuantitativo-experimental en tanto se trata de una investigación concluyente que logra su propósito buscando medir el problema y evitando cualquier juicio de valor subjetivo. La cuantificación del problema permite a los autores hacer predicciones para poblaciones más grandes utilizando métodos estadísticos y matemáticos. Y experimental, porque la aplicación del modelo a proponer es un experimento donde se puede variar la variable independiente para observar cambios en la variable dependiente, que es donde se da soporte a la continuidad del negocio. (Vilcarromero & Vilchez, 2018, p. 37)

A través del análisis, comparación y armonización de diferentes estándares, los autores concluyen que el modelo de gestión de riesgos de TI es adecuado para organizaciones que brindan servicios de información bajo el centro de operaciones SOC, estableciendo así un procedimiento para identificar riesgos clave. Procesos en una organización que forman una parte esencial de la mejora continua del negocio, lo que permite que una organización proteja todos los activos de información y aplique procesos de gestión de riesgos de manera efectiva mientras mantiene su continuidad. (Vilcarromero & Vilchez, 2018)

2.1.2 Ámbito Nacional

El trabajo realizado por Díaz, Coronado & Gómez, titulado “Diseño plan de respuesta a incidentes de ciberseguridad para la infraestructura cibernética del sector eléctrico colombiano”; El objetivo principal es diseñar un plan que pueda responder de manera operativa a los incidentes con procesos que permitan una rápida resolución para posibilitar el análisis y priorización de los incidentes, permitiendo desarrollar un escenario donde se puedan demostrar las mejoras. sigue adelante. (2021, p. 29)

Los autores desarrollaron el proyecto a través del tipo investigación acción, ya que es "un estudio científico autorreflexivo de las prácticas de mejora profesional". El diseño de investigación se basa en un enfoque cualitativo “centrado en abordar el proceso de investigación”. Desde esta perspectiva, divide el diseño de investigación cualitativa en teoría fundamentada, diseño etnográfico, diseño narrativo, diseño fenomenológico, diseño de investigación acción y estudio de caso cualitativo. (Díaz, Coronado & Gómez, 2021)

Los autores concluyeron que existe una interacción directa entre los dominios técnico y operativo en la respuesta a incidentes donde los de recursos humanos y de seguridad de la infraestructura tecnológica son partes interesadas que deben ser informadas de las medidas de mejora tras la resolución de cualquier incidencia. Las empresas de la industria energética mantendrán la disponibilidad y confiabilidad de los servicios que brindan mediante el desarrollo de planes de respuesta para incidentes de ciberseguridad en su infraestructura crítica. (Díaz, Coronado & Gómez, 2021)

Molina (2020) realizó un proyecto de grado denominado “Modelo de gobierno y gestión de riesgos TI para las universidades públicas de Colombia: Caso de estudio Universidad Popular del Cesar, en la ciudad de Barranquilla; Su alcance principal cubre específicamente todo el

dominio de TI, por lo que busca establecer un conjunto de actividades y procesos para gestionar adecuadamente los riesgos de TI con el fin de caracterizar los riesgos más relevantes asociados con el ciberdelito.

Para desarrollar el proyecto la autora utilizó un enfoque que le permitió trabajar por etapas y establecer cada parámetro importante para la investigación, principalmente en la primera fase estableció la investigación y exploración del marco de cada obra existente, la segunda En la tercera etapa, se evalúan los riesgos que se pueden realizar en la tercera etapa, y se elabora el modelo de gobierno y gestión de la transformación digital de la universidad y los riesgos TI, para que en la cuarta etapa se formule el plan de implementación del modelo. (Molina, 2020, p. 55)

La autora concluye que el abordaje del modelo parte de una buena base, ya que, mediante el estudio y comprensión de matrices de riesgo, mapas de riesgo y demás información perteneciente a la Universidad, se identifican factores de riesgo relevantes para la investigación, además de tener que ser controlados. para reducir la probabilidad de eventos y eventos Diferentes amenazas de impacto organizacional. (Molina, 2020, p. 96)

Por otra parte, Panche, Gutiérrez & Ardila, realizaron un proyecto de grado titulado "Metodología para la evaluación de madurez en gestión de incidentes de ciberseguridad"; Definir y desarrollar una metodología comprensible y flexible para diagnosticar la madurez de la gestión de incidentes de ciberseguridad. De esta forma se logran las mejores prácticas para una adecuada gestión de las amenazas emergentes, teniendo en cuenta los principales criterios de abordaje de cada amenaza. (Panche, Gutiérrez & Ardila, 2022)

Los autores implementaron la metodología de evaluación de madurez de gestión de incidentes porque su objetivo es ayudar a las organizaciones a comprender su nivel y si sus procesos están alineados con las buenas prácticas en la gestión de procedimientos. Incidentes Implementados, esto es posible mediante la creación de herramientas que permitan a las

organizaciones realizar autoevaluaciones, determinando así su estado de madurez, y una vez que tengan los resultados, puedan tomar acciones para fortalecer sus procesos de gestión de incidentes. (Panche, Gutiérrez & Ardila, 2022)

Al final, pudieron concluir que actualmente se están produciendo altos niveles de intentos de ciberataques y que la gestión de incidentes es fundamental para responder a estos incidentes y estar preparados cuando están sujetos a ellos, un enfoque que les permitiría identificar o responder. a Cada fase propuesta realiza una autoevaluación del nivel de madurez de sus procesos internos. (Panche, Gutiérrez & Ardila, 2022, p. 72)

2.1.3 Ámbito Local

Asimismo, Barbosa realizó en la ciudad de Ocaña un estudio titulado “Modelos de Ciberseguridad para Entidades Financieras, Integrando con Marcos de Gestión y Gobernanza TI”, cuyo eje fundamental fue diseñar un modelo de ciberseguridad para fortalecer la segunda línea de defensa mediante Mapeo consistente de marcos de referencia ampliamente aceptados para proteger a las instituciones financieras. Por ello, Innovation Factor tiene como objetivo optimizar el desarrollo de procesos dentro de cualquier organización. (Barbosa, 2020)

El autor utiliza la investigación cuantitativa bajo el enfoque descriptivo que constituye el paradigma positivista, debido a la consideración de normas generales para explicar la naturaleza del objeto de estudio a través de la observación, la verificación y la experiencia, proporcionando representaciones numéricas o estadísticas verificables. Analizando los resultados experimentales. (Barbosa, 2020, p. 47)

2.2 Marco conceptual

2.2.1 Modelo de ciberseguridad

Los modelos de ciberseguridad son marcos, estándares, leyes y regulaciones que se pueden proponer a nivel nacional e internacional, como COBIT (Objetivos de control para sistemas de información y tecnologías relacionadas) de ISACA (Asociación de auditoría y control de sistemas de información), que también se encuentra en NITS. (Instituto Nacional de Estándares y Tecnología de EE. UU.), que propone una estrategia de buenas prácticas para mejorar los procesos y operaciones de ciberseguridad, que desarrolla un plan de seguridad de activos de información. (ISACA, 2018)

2.2.2 Riesgos en la ciberseguridad

El riesgo es la posibilidad de que una amenaza se convierta en realidad, definida por Ramos, Arango y Amador (2020) como “la probabilidad que se presenta en la operación de un daño tecnológico”.

2.2.3 Vulnerabilidad en los sistemas de información

Las vulnerabilidades se refieren a cualidades que pueden estar sujetas a daños físicos o mentales y son debilidades en la tecnología o en los procesos relacionados con la información, por lo que se consideran características de un sistema de información o de la infraestructura que lo contiene. (Tarazona, 2017, p. 137)

2.2.4 Amenazas cibernéticas

Las ciberamenazas se definen como “aquellas actividades realizadas en el ciberespacio con la finalidad de utilizar la información transmitida a través de él para cometer distintos delitos mediante su uso, manipulación, control o robo”. (Tamayo y González, 2020) Para Ortiz (2020), las amenazas a los sistemas informáticos pueden ser causadas por las personas, la lógica de los sistemas involucrados y la explotación de las debilidades físicas.

2.2.5 Gestión de la seguridad de la información

La información es un activo que, al igual que otros activos comerciales, es esencial para una empresa y, como tal, debe protegerse adecuadamente. Vargas (2020) afirmó que la gestión de la seguridad de la información busca proteger la confidencialidad, integridad y disponibilidad de los datos y los bienes que los contienen o procesan.

2.2.6 Confidencialidad

significa un acuerdo entre una empresa y un cliente con respecto a cómo se procesará y divulgará la información de identificación personal. Esto debe describir la política para mantener la confidencialidad de los datos identificables, incluidos los controles sobre el almacenamiento, el procesamiento y el intercambio de datos personales para minimizar el riesgo de divulgación de información. (Cepal, 2020)

2.2.7 Amenaza

Una amenaza se entiende como un evento que puede afectar negativamente las operaciones de una organización o sus activos a través del acceso no autorizado a los sistemas de información, destrucción, divulgación o modificación de información y/o denegación de servicios internos de la empresa. (Fajardo, 2017)

2.2.8 Ingeniería social

Es un tipo de ataque que aprende información clave haciendo a las personas una serie de preguntas para descubrir datos que pueden ser utilizados como objetivo para lograr algún tipo de beneficio económico y/o conocimiento perteneciente a un individuo u organización. Es el acto de manipular a una persona a través de técnicas psicológicas y sociales para lograr un objetivo específico. (Novoa, 2018)

2.2.9 Delito informático

Los delitos informáticos se refieren a actos ilícitos cometidos mediante el uso indebido de la tecnología, violación de la privacidad de la información de terceros, destrucción o extracción de cualquier tipo de datos almacenados en un servidor. (Acosta. Benavides & García, 2020)

2.2.10 Gestión documental

Comprende la aplicación de tecnologías y procedimientos que permitan establecer un acceso uniforme a la información generada en una organización, a través de actividades administrativas y técnicas que permitan la coordinación y control de la creación, recepción, organización, almacenamiento, conservación, acceso y difusión de la información. Información durante su ciclo de vida para facilitar su uso en procesos de posible intervención dentro de la empresa, así como su conservación. (Fajardo, 2017)

2.3 Marco Contextual

2.3.1 Objetivos organizacionales.

La Universidad Popular del Cesar – Seccional Aguachica define sus objetivos organizacionales a través de sus programas de educación institucional de la siguiente manera:

- Esforzarse por garantizar la calidad y la excelencia mediante la implementación de procesos de autoevaluación, acreditación de programas y autorregulación para garantizar que la comunidad logre su misión y visión para la calidad de la educación.
- Cumplir con una función pedagógica para generar y difundir conocimiento a través de un método que interrelacione las humanidades y las tecnologías en los estudios de cada profesión, para dar contexto a actividades interdisciplinarias, multidisciplinarias e interdisciplinarias en el marco de la educación general.

- Fortalecer la competitividad, impulsando los procesos de innovación, coordinando y dando seguimiento a los proyectos de investigación, asegurando una estrecha interacción entre el Sistema Nacional de Ciencia, Tecnología e Innovación, la Universidad Popular César y el sector productivo.
- Promover el conocimiento de la sociedad colombiana mediante el fortalecimiento de la comunidad de investigadores en ciencias básicas, aplicadas, sociales y humanas.
- Realizar labores de extensión científica, cultural y de servicio social orientadas a la comunidad.
- Formación de alto nivel científico, pedagógico, técnico y artesanal del personal docente e investigador para garantizar una educación de calidad en todos los niveles y modalidades de formación.
- Promover la formación de comunidades académicas y científicas en redes de conocimiento altamente especializadas en el contexto de la educación superior, incorporando respectivamente las nuevas tecnologías de la información y la comunicación.
- Ampliar los programas académicos a nivel regional para satisfacer las necesidades sociales, culturales, económicas, políticas y educativas de las comunidades pertinentes.
- Consolidar e inspirar el apoyo de la comunidad académica upecista para fortalecer las capacidades individuales y colectivas para generar conocimiento educativo, científico, social, económico y cultural relevante.
- Además de los fines antes mencionados, la Universidad Popular César también cumplirá con los objetivos de regulación de la educación superior establecidos en la Constitución y las leyes colombianas.

- Profundizar la formación integral de los colombianos en cuanto a modelos y calidades de educación superior, capacitándolos para desempeñar las funciones profesionales, investigativas y de servicio social que requiere el país.
- Contribuir a la creación, desarrollo y difusión del conocimiento en todas sus formas y manifestaciones, promoviendo su aplicación en todos los campos para atender las necesidades de la nación.
- Servicio de calidad a la comunidad, referido a la producción académica, los medios y procesos utilizados, la infraestructura institucional, sus dimensiones cualitativas y cuantitativas, y las condiciones en que se desarrolla cada institución.
- Ser factor de desarrollo científico, cultural, económico, político y moral a nivel nacional y regional, en coordinación con otras instituciones educativas y de formación.
- Contribuir al desarrollo de los niveles educativos anteriores para la consecución de su correspondiente finalidad.
- Contribuir a la formación y consolidación de la academia y el trabajo en red con pares a nivel regional, nacional e internacional.
- Promover la protección de un medio ambiente sano y fomentar la educación y la cultura ecológica.
- Proteger y promover el patrimonio cultural del país.

2.3.2 Misión y Visión.

Misión. La Universidad Popular del César – Seccional Aguachica, como institución de educación superior oficial del orden del Estado, produce personas social y culturalmente

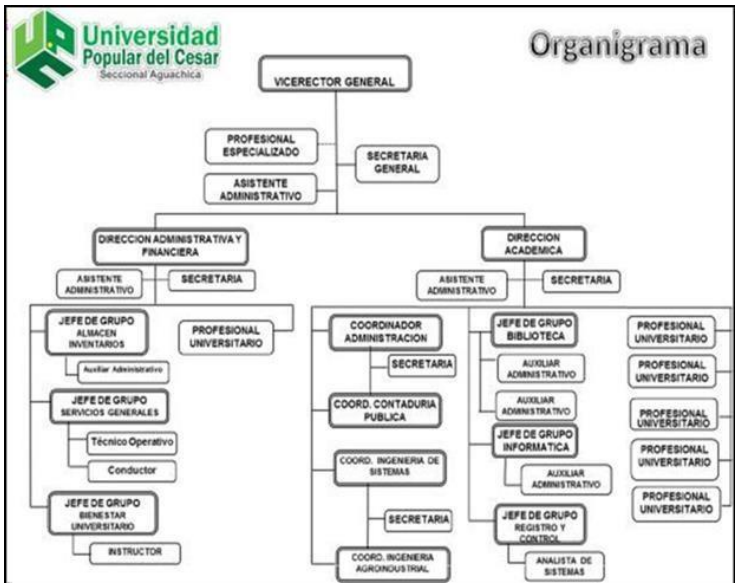
responsables; con calidad, educación integral e inclusiva, ciencia y tecnología; a través de diferentes modos y métodos educativos, a través de programas pertinentes al contexto, dentro de la diversidad de campos disciplinares, en el marco de la libertad de pensamiento, esto consolida la construcción del conocimiento, contribuye a la resolución de problemas y conflictos en un entorno sostenible, y tiene visibilidad nacional e internacional.

Visión. Para el 2025, la Universidad Popular del Cesar será una institución de educación superior de calidad, inclusiva y transformadora, comprometida con el desarrollo sostenible de la región, con reconocimiento nacional e proyección internacional.

2.3.3 Estructura.

2.3.3.1 Organigrama General. La estructura general de la Universidad Popular del Cesar Aguachica Seccional es jerárquica, estando el más alto nivel conformado por los Vicerrectorados Divisionales, de los cuales emergen dos grandes departamentos, a saber, el Departamento de Administración y Finanzas y el Departamento Académico. Cada uno de ellos lidera otras áreas de la institución a nivel funcional y operativo.

Figura 1. Organigrama de la Universidad Popular del Cesar Seccional Aguachica



Fuente: Universidad Popular del Cesar Seccional Aguachica.

2.4 Marco Teórico

En seguridad informática, es importante analizar y clarificar los muchos conceptos teóricos propuestos, permitiendo así una visión más amplia y profunda capaz de abordar cualquier problema actual, que puede incluir ataques cibernéticos, cualquier ataque contra redes (SI). El sistema de información del servicio, puede haber riesgos, y se filtra información valiosa de la empresa, y este daño puede ocurrir en bases de datos, páginas web, servidores y dispositivos móviles con los que interactúan los usuarios, y que tienen como finalidad principal la obtención de datos personales y realizar delitos económicos a particulares como el robo Estos ataques pueden llevarse a cabo a través de malware, que es cualquier tipo de programa o software creado para cometer delitos informáticos o causar daños a software o hardware.

Estos virus informáticos explotan vulnerabilidades que surgen y pueden propagarse o replicarse si se codifican para tal fin, este tipo de malware se conoce como gusano o caballo de Troya y el daño que causan depende de su estructura y propósito para el que fueron creados; o usted también puede atacar a través de phishing, que es un intento de suplantar su identidad y obtener credenciales (como números de tarjetas de crédito, datos bancarios personales o contraseñas de cuentas personales) para obtener acceso a los datos mediante el enrutamiento de datos a través de phishing, persuasión o permiso de correos electrónicos falsos. intentar.

Algunos de los ataques más comunes se llevan a cabo a través de la ingeniería social, que es un conjunto de técnicas utilizadas para engañar a los usuarios del sistema oa las personas para que obtengan el objetivo del ataque. Esta técnica de ataque incluye otras propuestas y muchas otras similares. Otro ataque que ocurre con mayor frecuencia y con información irrecuperable es el conocido como ransomware, un tipo de malware troyano que encripta los datos para inutilizar la información de los dispositivos y computadoras. Los atacantes utilizan la extorsión hasta que el dueño del sistema paga el rescate y lo descifra, muchos de estos programas han sido mitigados porque en la web hay personas llamadas hackers blancos encargadas de aportar su seguridad y conocimientos informáticos para poder neutralizar el impacto de los ataques y ataques informáticos. Delitos Todos los daños causados por la red.

Para combatir todos estos ataques, aplicar la ciberseguridad, acciones, políticas, controles y demás medidas utilizadas e implementadas por SI para mitigar vulnerabilidades y ciberriesgos, instalar firewalls, etc., es importante contar con un plan de seguro ante cualquier ciberataque. Un control de seguridad perimetral aplicado dentro de una LAN de sistemas informáticos que está configurado para determinar qué usuarios o dispositivos tienen credenciales para acceder a datos internos.

De esta forma, es posible proteger la infraestructura de accesos no autorizados, bloquear páginas o aplicaciones que detectan un determinado tipo de ataque, alertar sobre conexiones no autorizadas y controlar el tráfico de la red; o aplicaciones de control de acceso cuya función principal es gestionar la entrada y salida de usuarios. de los sistemas e infraestructura de una organización a través de un dispositivo, software y administrador de servicios, brindando acceso o restricciones prescritas por la misma organización, algunos de los dispositivos utilizados son: Lectores Biométricos, Lectores de Tarjetas, Lectores de QR y Código de Barras, contraseñas, sistemas de control de acceso mediante móvil teléfonos o el Internet de las Cosas, etc.

La implementación de procesos de gestión de la seguridad de la información requiere una comprensión de la especificidad del contenido protegido, como la infraestructura técnica, los recursos técnicos, los documentos y la información, que pueden ser críticos, valiosos y sensibles dentro de la empresa, para que los administradores puedan identificar cada activo La especificidad del valor , lo cual es fundamental para prevenir futuros riesgos y vulnerabilidades en la infraestructura tecnológica de la compañía.

En lo que respecta a la ciberseguridad, es cierto que su principal objetivo es proteger a los equipos organizacionales, servidores de situaciones en las que se toman medidas preventivas contra los ciber riesgos, lo cual es propio del dominio compuesto de la gestión de la seguridad y la construcción de modelos. Actitud defensiva, progresividad y resiliencia, inicialmente desconocidas e infrautilizadas en la política corporativa. La ciberseguridad o también conocida como seguridad informática, sustentada en software y recursos técnicos, se utiliza para proteger la infraestructura técnica de los delitos informáticos de los usuarios, con el objetivo de prevenir y/o reducir daños a todos los sistemas de información, activos o daños. Efectos físicos en equipos de cómputo.

Al equilibrar la reducción de vulnerabilidades dentro de la empresa con una gestión de contraseñas adecuada, la gestión de acceso privilegiado no debe tomarse a la ligera, por lo que se deben tomar medidas para proteger adecuadamente los dispositivos de los usuarios, la infraestructura tecnológica y los datos confidenciales.

Debe enfatizarse que los actos de ciberdelincuencia afectan a la sociedad en su conjunto, no solo a las organizaciones legítimas. Las organizaciones con un buen SGSI (Sistema de Gestión de Seguridad de la Información) pueden advertir de ataques informáticos, mostrar cómo reducir el riesgo de posibles ataques y reducir las vulnerabilidades dentro de la empresa. Además, se deben implementar estrategias de recuperación ante desastres y continuidad comercial para que las operaciones comerciales vuelvan a la normalidad.

La norma ISO 27002 es una recopilación de buenas prácticas implementadas por las empresas, que permite consolidar la confianza en la empresa a través de recomendaciones para reducir los riesgos que representan los activos de la empresa, minimizar los daños y asegurar la continuidad de los procesos en caso de incidente de protección, reduciendo así las Amenazas. y Riesgos.

Un modelo de seguridad de la información es un conjunto de métodos y políticas que se utilizan para proteger la información. El objetivo es brindar servicios de TI de manera eficaz y eficiente. La seguridad informática en general es la rama de la informática destinada a garantizar la seguridad de las infraestructuras informáticas, y en particular la seguridad de los datos. Para avanzar en esta ciencia, necesitamos estándares, metodologías, leyes y reglamentos, protocolos y varias herramientas para minimizar los riesgos que pueden enfrentar nuestra infraestructura y datos.

2.5 Marco Legal

Ley 1712 de 2014

Art. 1 La presente ley tiene por objeto regular el derecho de acceso a la información pública, el procedimiento para ejercer y garantizar este derecho y las excepciones a la divulgación de la información.

Art. 2 Principios máximos emitidos para tenedores generales. Toda la información en posesión, control o custodia de un sujeto obligado es pública y no podrá ser retenida o restringida salvo lo requerido por la Constitución o la ley.

Ley 1581 de 2012

Campo de aplicación. Los principios y disposiciones contenidos en esta Ley se aplicarán a los datos personales registrados en cualquier base de datos que sea susceptible de tratamiento por parte de entidades públicas o privadas. La presente ley se aplicará al tratamiento de datos personales que se realice en el territorio de Colombia o a la legislación cuando el responsable del tratamiento o el responsable del tratamiento se encuentre fuera del territorio nacional. (Congreso de la República, 2012)

Decreto 338 de 2022

Creó modelos y ejemplos de gobernanza de la seguridad digital con el fin de establecer lineamientos generales para fortalecer la gobernanza de la seguridad digital a través de la regulación del sector TIC. (Congreso de la República, 2022)

Ley 1273 de 2009

Artículo 269A: *Acceso abusivo a un sistema informático*. El que acceda en todo o en parte a un sistema informático, protegido o no por medidas de seguridad, sin autorización o al margen del convenio, o permanezca en él contra la voluntad de quien tenga derecho a excluirlo, será sancionado con cuarenta y ocho (48) a noventa y seis (96) meses y sanción de 100 a 1.000 del salario mínimo mensual legal vigente.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que impida o impida el funcionamiento o el normal acceso a un sistema informático, a los datos informáticos contenidos en él o a una red de telecomunicaciones sin autorización, será sancionado con cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 Multa de hasta 1.000 salarios mínimos legales vigentes para el mes en curso, siempre que el hecho no constituya delito sancionado con pena mayor.

Artículo 269C: *Interceptación de datos informáticos*. El que, sin previa orden judicial, intercepte datos informáticos en su origen, destino o dentro de un sistema informático, o intercepte radiaciones electromagnéticas de un sistema informático transmisor de datos, incurrirá en pena de treinta y seis (36) a setenta y seis años. dos (72) meses.

Artículo 269D: *Daño Informático*. El que sin autorización destruya, dañe, borre, degrade, altere o suprima datos informáticos o sistemas de procesamiento de información o sus partes o componentes lógicos, será reprimido con prisión de cuarenta y ocho (48) a noventa y seis (96) meses y sanción de 100 a 1.000 del salario mínimo mensual legal vigente.

Artículo 269E: *Uso de software malicioso*. El que sin autorización produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga malware u otros programas informáticos dañinos del territorio de este país, será sancionado con pena privativa de libertad desde los cuarenta y ocho (48) años hasta los noventa años. - seis (96) meses y multa de 100 a 1.000 del salario mínimo mensual legal vigente.

Artículo 269F: Violación de datos personales. El que adquiera, recopile, sustraiga, ofrezca, venda, permute, envíe, compre, intercepte, divulgue, modifique o utilice claves personales, datos personales contenidos en ficheros, archivos, bases de datos o similares, incurrirá en prisión de cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1000 del salario mínimo mensual legal vigente.

Artículo 269G: Suplantar un sitio web para obtener datos personales. El que diseñe, desarrolle, trafique, venda, implemente, programe o envíe páginas electrónicas, enlaces o ventanas emergentes con fines ilícitos y sin autorización, incurrirá en prisión de cuarenta y ocho (48) a noventa años - seis (96) meses. y multa de 100 a 1.000 del salario mensual legal vigente, siempre que el hecho no constituya delito sancionado con pena más grave.

Capítulo 3. Diseño metodológico

3.1 Tipo de investigación

De acuerdo a las características del proyecto se adopta el tipo de investigación cuantitativa y se adopta el método descriptivo. El propósito de cuantificar resultados es poder describir, explicar, verificar y predecir fenómenos (causalidad), generar y probar teorías. Para ello, los datos fueron recolectados utilizando instrumentos estandarizados validados para demostrar su confiabilidad, de tal manera que la información fue separada intencionalmente y las variables de estudio fueron medidas con precisión. (Martínez & Martínez, 2020) El método para realizar la investigación de manera descriptiva se realiza cuando se quiere describir todos los componentes principales de una realidad. La investigación descriptiva es un tipo de investigación causal que no solo intenta describir o resolver un problema, sino que también intenta especificar la causa del problema. (Guevara, Verdesoto y Castro, 2020, p. 3).

En el trabajo de investigación se utilizó un diseño de investigación acción, pretendiendo ser muy efectivo en su proceso implementando un enfoque de ciberseguridad, además de visualizar la mejora de lineamientos para las instituciones de educación superior, más seguridad de vulnerabilidades y riesgos, la investigación se basa en las observaciones, la reflexión y la acción para completar. De acuerdo con Hernández, Fernández y Baptista (2014), la investigación-acción participativa se enfoca en informar y preparar decisiones para reformas de programas, procesos y estructurales, y los colaboradores deben involucrarse en la revisión y mejora de sus procesos de implementación, juzgando los resultados.

3.2 Seguimiento metodológico del proyecto

Tabla 1. Alcance actividades

Objetivos de la investigación	Actividades por objetivo	Indicador por actividad
Examinar el estado actual de los riesgos inherentes en que se encuentran las instituciones de educación superior.	Act 1. Estructurar instrumento de recolección de datos	Ind 1. Técnica de recolección de datos
	Act 2. Aplicar instrumento	Ind 2. Sistematizar los datos
	Act 3. Analizar resultados	Ind 3. Estado actual
Caracterizar los principales riesgos de ciberseguridad existentes para identificar modelos que puedan ayudar a minimizar los incidentes dentro de la empresa.	Act 4. Búsqueda de literatura gestión de incidentes	Ind 1. Gestión de incidentes, ciberseguridad
	Act 5. Establecer estándar	Ind 2. Estándares Ind 3. Controles, políticas de seguridad
Validar una propuesta de modelo en el que se establezcan controles para la	Act 6. Estructurar modelo	Ind 1. Buenas prácticas
	Act 7. Validar modelo	Ind 2. Validación del modelo

gestión de incidentes en las instituciones de educación superior.	

Fuente: elaboración propia.

3.3 Población y muestra

Teniendo en cuenta el tipo de estudio escogido, se procede a establecer el conjunto de elementos a estudiar definidos de la siguiente manera:

Tabla 2. Población y Muestra

Población	Muestra
En cuanto a la población objeto de estudio se toman en cuenta las instituciones de educación superior que se encuentran dentro del Cesar como lo son la Universidad Abierta y a Distancia UNAD, Universidad del Área Andina, Universidad UDES, Universidad Nacional sede la Paz, Universidad Popular del Cesar – Sede Valledupar y Universidad Popular del Cesar – Seccional Aguachica.	Como muestra de la investigación se toma como referente el personal administrativo de la Universidad Popular del Cesar – seccional Aguachica, para lograr establecer un diagnóstico de inicial de como está su nivel de conocimiento en temas de ciberseguridad y lograr plantear un modelo que se adapte y sea escalable en otras IES (Instituciones de educación superior)

Fuente: elaboración propia.

3.4 Técnicas de recolección de la información

Para el desarrollo del proyecto se utilizará como técnicas de recolección de la información, una encuesta el cual recolecte los datos necesarios sobre las actividades que se desarrollan en la Universidad Popular del Cesar – Seccional Aguachica.

Tabla 3. Técnicas de Recolección de la Información

Fuentes primarias	Fuentes secundarias
La información primaria se obtendrá a través de la encuesta realizada a los administrativos de la universidad. Se incluirá la observación directa de cada una de las actividades que se desarrollan en las oficinas de la institución, permitiendo identificar cada uno de los procesos y los riesgos que se presentan dentro de ella.	Para lograr realizar una búsqueda bibliográfica extensa se toma en cuenta información valiosa de proyectos de investigación relacionados con ciberseguridad, noticias y artículos de revistas indexadas que sirvan de fuente fidedigna para la construcción del modelo.

Fuente: elaboración propia.

3.5 Análisis de la información

Para poder analizar los datos recolectados a través de la encuesta a los directivos de la Universidad Popular del Cesar, se realiza la actividad 3 para lograr el cumplimiento del objetivo 1, la cual puede arrojar información valiosa sobre los riesgos inherentes o ciberataques en determinadas áreas de tiempo. Para lograr el objetivo 2, la actividad 4 busca primero referentes teóricos que sustenten la descripción de la mayoría de los riesgos existentes en las instituciones de educación superior, por lo que finalmente se logra el objetivo 3 a través de la actividad 6, es

decir, la construcción del modelo para su posterior verificación por parte de expertos en la actividad 7.

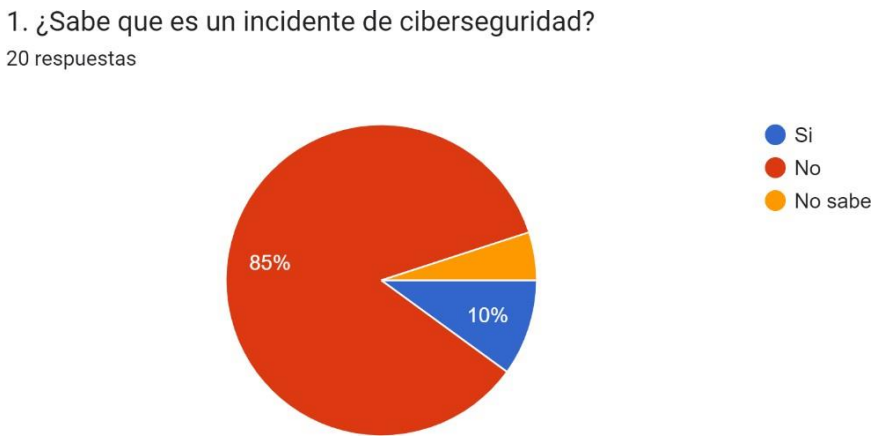
Capítulo 4. Resultados

Con base en el contenido establecido en la matriz de operación de variables, ver Anexo (A), tomando como referencia COBIT 2019, con base en el proceso de indicadores de apoyo al logro de metas e indicadores de implementación de buenas prácticas, por el proceso inicial de BAI02, su función principal es apoyar la gestión Las capas definen los requisitos básicos de la organización, y cabe señalar que los procesos y subprocesos MEA01 y DSS se utilizan para establecer estándares que fortalecen la estructura técnica de la organización.

4.1 Encuesta del estado actual de los riesgos inherentes dentro de la Universidad Popular del Cesar – Seccional Aguachica

La técnica de recolección de datos utilizada para recabar la información necesaria fue la encuesta, la cual constó de 13 preguntas que permitieron determinar el estado actual de la Universidad Popular Cesar - seccional Aguachica; en cuanto a conocimientos de ciberseguridad, incidentes ocurridos dentro de la institución, y así según los resultados obtenidos se utilizan para el diagnóstico. La encuesta fue dirigida a los administradores de la universidad (20), quienes respondieron a través de un formulario de Google para agilizar el proceso de recopilación de información, quienes respondieron completamente a la documentación enviada.

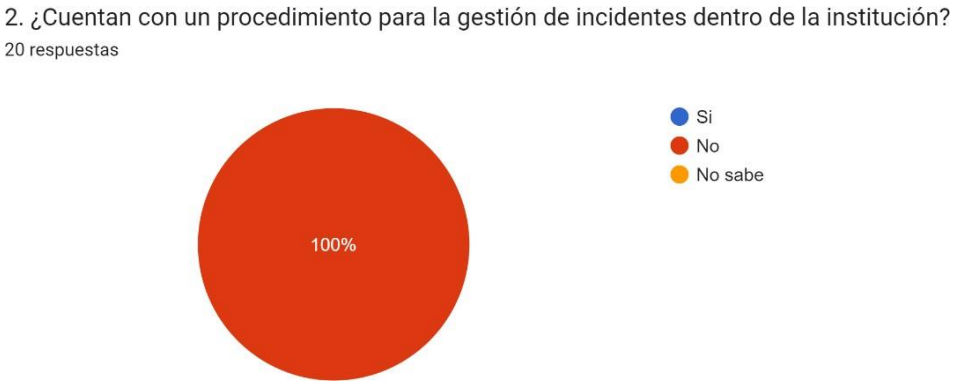
Figura 2. Pregunta. Conocimientos previos



Fuente: elaboración propia.

Como se muestra en la Figura 2, es claro que el 90% del personal administrativo no tiene conocimiento sobre que son los incidentes de ciberseguridad, siendo preocupante no saberlo ya que se pueden generar incidentes dentro de la institución que se puedan pasar por alto. Ya que la tecnología está en constante avance y trae consigo un sin número de amenazas.

Figura 3. Procedimientos para la gestión

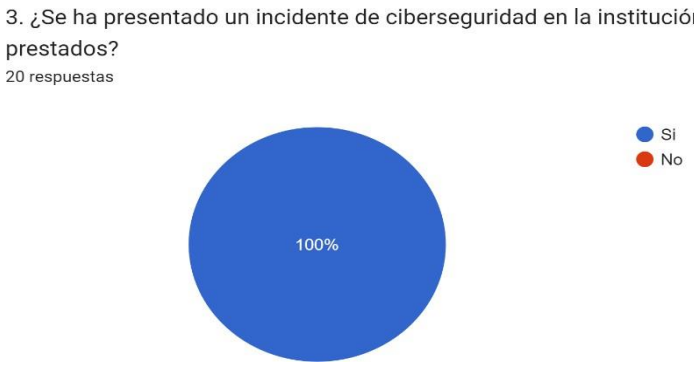


Fuente: elaboración propia.

En la pregunta realizada al personal administrativo, como se muestra en la Figura 3, es claro que el 100% de los encuestados responden que no tienen establecido un medio en donde

puedan establecer el incidente que está ocurriendo para su posterior solución. Es importante que cada institución educativa cuente con un medio donde se puedan establecer estos incidentes que permita llevar una bitácora.

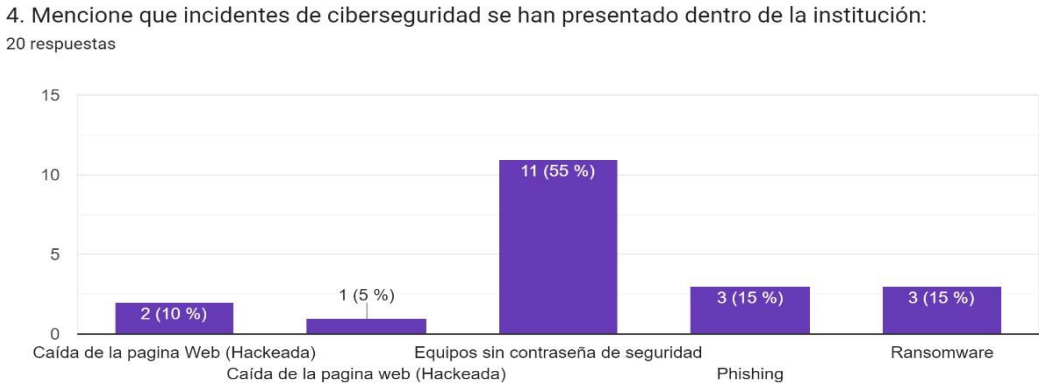
Figura 4. Incidentes de ciberseguridad



Fuente: elaboración propia.

De acuerdo a la Figura 4, se observa que el 100% de los encuestados afirman que se han presentado incidentes de ciberseguridad, siendo esto algo preocupante para cualquier institución de orden nacional, donde se pueden ver vulnerados los activos de la información, la confidencialidad de los datos, entre otros factores.

Figura 5. Incidentes presentados



Fuente: elaboración propia.

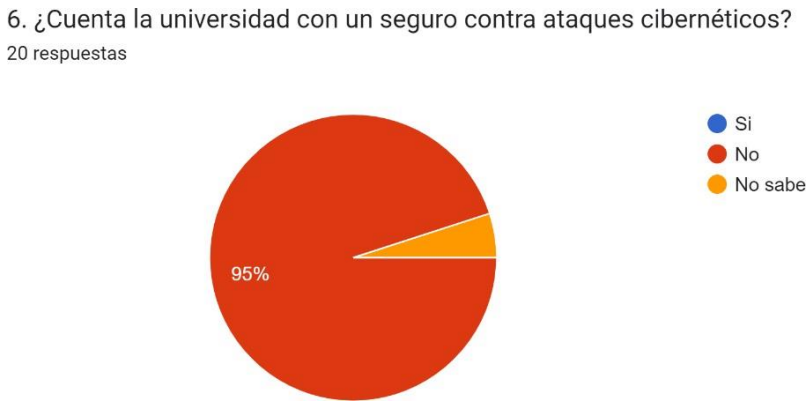
En esta pregunta realizada, se observa que cada uno de los encuestados expuso algún incidente que se presenta dentro de la institución siendo el más común con el 55% el encontrarse con equipos sin contraseñas de seguridad permitiendo que algún tercero logre vulnerar y sacar información, también se observa que han sido hackeados un ejemplo claro es que tumbaron la página web de la institución y se han presentado casos de Phishing y ransomware.

Figura 6. ¿Estándar dentro de la universidad?

Fuente: elaboración propia.

El personal administrativo encuestado, el 100% afirma que no cuentan con un marco de referencia o guías que permitan realizar buenas prácticas para realizar una adecuada gestión de incidentes, siendo un factor perjudicial para el cumplimiento de cada uno de los procesos que se realizan dentro de la institución.

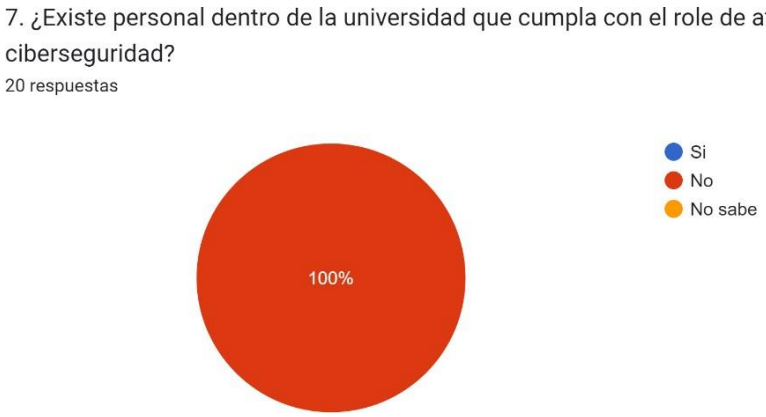
Figura 7. Protección de ciberseguridad



Fuente: elaboración propia.

En esta pregunta que se realizó al personal administrativo el 95% de los encuestados responde que la institución no cuenta con un seguro o una protección contra los ataques cibernéticos, mientras que el 5% no sabe que tengan algún seguro.

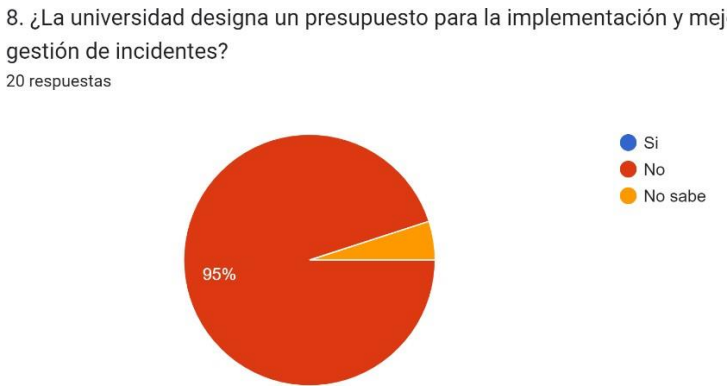
Figura 8. ¿Personal Adecuado?



Fuente: elaboración propia.

Según la figura 8, el 100% de los encuestados manifiesta que no cuentan con personal dentro de la universidad que cumpla con el rol adecuado para gestionar problemas de ciberseguridad, lo que resulta ser preocupante ya que no tener alguien capacitado para este tipo de incidentes deja abierta las posibilidades a nuevas amenazas y vulnerabilidades.

Figura 9. Pregunta. Presupuesto para la ciberseguridad



Fuente: elaboración propia.

De acuerdo a lo expuesto en la Figura 9, el 95% de los encuestados afirman que no se designa un presupuesto, mientras que el 5% no sabe si se implementa algún presupuesto dentro de la institución.

Figura 10. Pregunta. Identificación de incidentes

Fuente: elaboración propia.

El 100% de los encuestados no sabe cómo identificar, ni como reportar un incidente de ciberseguridad, esto podría generar conflicto con algún servicio prestados dentro de la universidad y generaría un cese de actividades.

Figura 11. Pregunta. Políticas existentes

Fuente: elaboración propia.

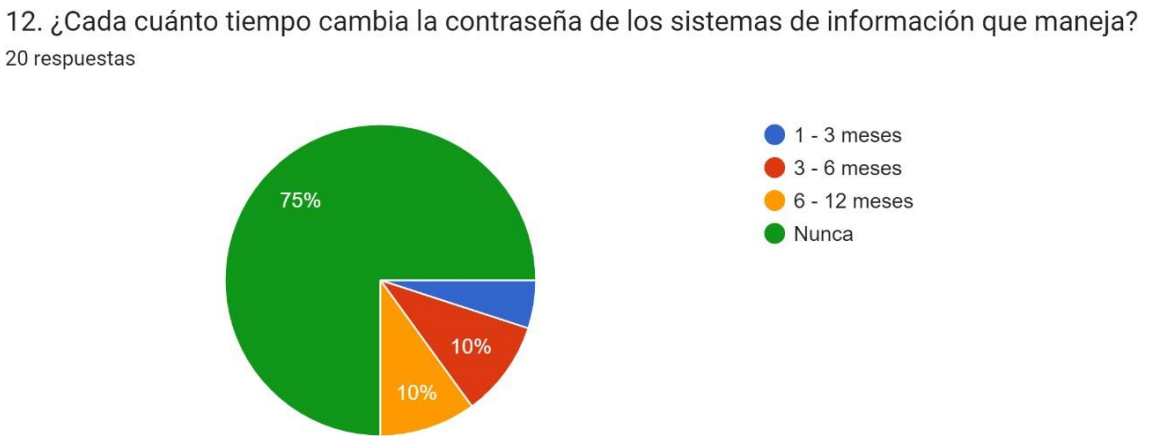
De acuerdo a la Figura 11, el 100% del personal administrativo afirma que no cuentan con políticas relacionadas con la seguridad de la información dentro de la universidad, afectando así como se debería proteger los activos de la misma.

Figura 12. Pregunta. Importancia de la información

Fuente: elaboración propia.

El 95% de los encuestados afirma que es importante la seguridad de la información y la ciberseguridad, ya que estos cubrirán aspectos importantes sobre la continuidad de la universidad y será un factor clave para la infraestructura tecnológica.

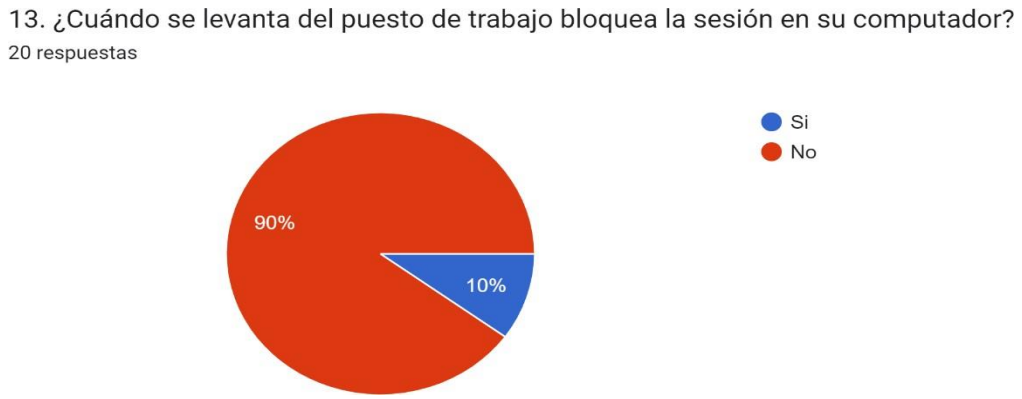
Figura 13. Pregunta. Seguridad de contraseñas



Fuente: elaboración propia.

Como se muestra en la Figura 13, el 75% del personal nunca realiza cambio de contraseñas a sus equipos asignados, frente al 10% que hace cambios periódicos de 3 a 6 meses y el 10% restantes de 6 a 12 meses, lo que genera una amenaza para la información con la que cuentan.

Figura 14. Pregunta. Seguridad física de los equipos



Fuente: elaboración propia.

El 90% del personal administrativo afirma que cuando deja su lugar de trabajo no bloquea la sesión en la que está trabajando, frente al 10% del personal que si realiza esta acción para prevenir alguna vulnerabilidad.

4.1.1 Principales riesgos de ciberseguridad

Las propias instituciones de educación superior se ven amenazadas por desastres que no saben cuándo ocurrirán, y lo que es más grave es que en ellos se concentran los datos personales de los estudiantes, con poco o ningún conocimiento para actuar en situaciones de emergencia y evitar estas amenazas; riesgo la gestión es la clave para mejorar la educación Formas para que los profesionales de las agencias transformen las condiciones vulnerables en las que viven y su capacidad para prepararse y responder a las emergencias.

La evaluación tiene cinco criterios de evaluación y cada nivel estará acompañado de unos objetivos de control, se considerarán unos criterios de evaluación y se determinará un resultado en el proceso, por lo que la efectividad dependerá mucho de la sinceridad con que se haga funcionar cuando se responda. Una vez que todo el formato de evaluación esté completo, graficará los resultados y proporcionará estados clave donde las agencias pueden enfocarse en aquellos que se encuentran deficientes o bajos.

De esta forma, los criterios establecidos para la medición y gestión del riesgo se basan en la norma ISO 30001apoyada en las directrices de la norma 73:2009, que permite una base inicial para establecer una adecuada gestión de incidentes, donde criterios como: servicios prestados, tecnología vs. Se evalúa la instalación, teniendo en cuenta el valor de cada situación, determinado por su impacto o probabilidad de recurrencia del evento, de la siguiente manera:

Tabla 4. Impacto de incidente

Descripción	Rango
Catastrófica	9-10
Altos	7-8
Medios	5-6
Bajos	3-4
Relevantes	1-2

Fuente: Basado en la Norma ISO 3001 – guía 73:2009.

Tabla 5. Probabilidad de incidente

Descripción	Rango
Constantes	5
Moderadas	4
Ocasionada	3
Posibles	2
Improbables	1

Fuente: Fuente: Basado en la Norma ISO 3001 – guía 73:2009.

Tabla 6. Rango de Niveles

Niveles	Valores
NC (Nivel Critico)	50
NA (Nivel Alto)	30 – 49
NM (Nivel Medio)	10 – 29
NB (Nivel Bajo)	0 – 10

Fuente: elaboración propia.

4.1.2 Riesgos

Tabla 7. Riesgos identificados.

Descripción	Abreviatura	Evento	Impacto	Ocurrencia	Nivel
Red	**RI1**	Conexiones no autorizadas LAN y WLAN	Catastrófica	Posible	Alto
Red	**RI2**	Ataques de malware	Alto	Moderado	Medio
Red	**RI3**	Puertos de red expuestos	Medio	Posible	Medio
Red	**RI4**	Ataque de secuencia a TCP	Bajo	Ocasionada	Bajo
Servidor	**RI5**	Sustracción de información por acceso no autorizados	Catastrófica	Posible	Alto
Servidor	**RI6**	Inyección de SQL	Alto	Posible	Alto
Infraestructura y Servidores	**RI7**	Desastres naturales	Bajo	Posible	Bajo

Servidor	**RI8**	OS FingerPrinting	Medio	Posible	Medio
Infraestructura	**RI9**	Acceso no autorizado a salas	Medio	Posible	Medio
Infraestructura	**RI10**	Acceso no autorizado a equipos de computo	Medio	Posible	Medio
Correo electrónico	**RI11**	Suplantación de identidad	Medio	Posible	Medio
Correo electrónico	**RI12**	Phishing	Medio	Posible	Medio
Correo electrónico	**RI13**	Ransomware	Medio	Posible	Medio

Fuente: elaboración propia.

4.1.2.1 Matriz de riesgos

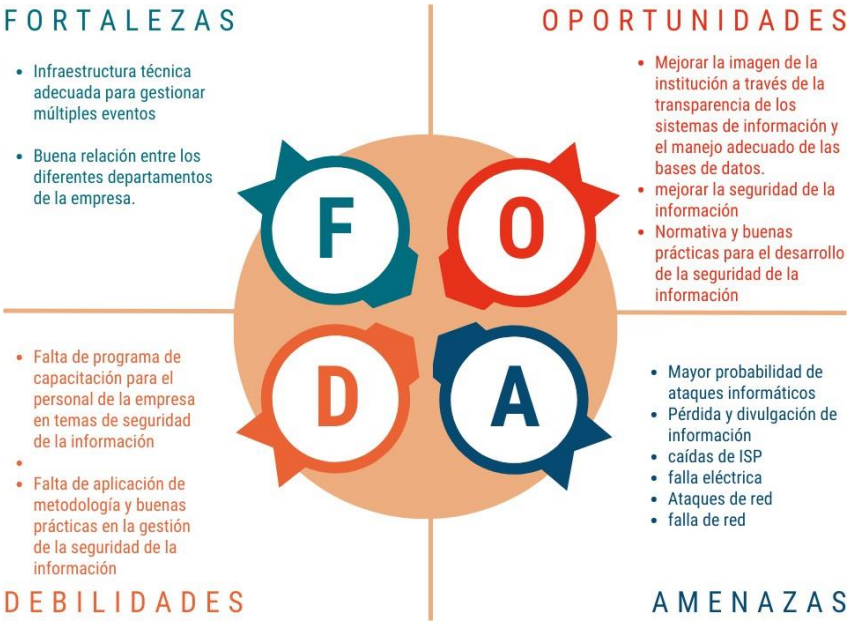
Tabla 8. Mapeo de los riesgos

	UNIVERSIDAD POPULAR DEL CESAR				CÓDIGO: 102-180-MAP03
	Mapa de riesgos				VERSIÓN: 2
Valoración de riesgos					
	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)

Probabilidad	Raro (1)	1	2	3	4	5
	Improbable (2)	2	4	6	8	10
	Posible (3)	3	6	9	12	15
	Probable (4)	4	8	12	16	20
	Casi seguro (5)	5	10	15	20	25
B: Zona de riesgo Baja: Asumir el riesgo						
M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo						
A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir						
E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir						

Fuente: elaboración propia.

Figura 15. Matriz FODA



Fuente: elaboración propia.

Al implementar un ambiente organizacional basado en la matriz FODA, su objetivo es demostrar cómo ejercer la máxima autoridad en materia de seguridad, y sus funciones incluyen formular, controlar y promover el cumplimiento de las normas de seguridad nacional. Posteriormente, se debe determinar el contexto de los riesgos a evaluar con base en las necesidades expresadas al interior de la institución.

4.1.3 Análisis de los riesgos

Los ataques a la red muestran una tendencia de incrementarse significativamente año tras año, es solo cuestión de tiempo que ocurra algún accidente en cualquier institución educativa, por lo que es muy importante distinguir qué es la seguridad de la información en este momento, y lo más importante es lo que podemos prevenir y prevenir. la seguridad cibernética. Esto permitirá

abordar de manera efectiva los controles adecuados y enfocar los esfuerzos en mitigar los riesgos que enfrenta la organización, ya que los ciberataques ocurren todos los días y deben ser cubiertos y monitoreados continuamente para cerrar brechas y tomar acciones oportunas cuando se detecten amenazas.

Para establecer un modelo de gestión de ciberseguridad para atender incidentes dentro de las instituciones educativas, se utilizará los marcos COBIT 2019 con apoyo de la ISO 27035, ya que permiten establecer la protección de datos ante incidentes de seguridad que puedan comprometer información no deseada o no esperada de la universidad. Procesar y amenazar la seguridad de los activos de información. En resumen, cuando se diagnostica, la seguridad de la información engloba todo el espectro de protección de cualquier medio que la contenga, mientras que la ciberseguridad se enfoca únicamente en proteger la información en formato digital.

Asimismo, se determinó que la universidad no contaba con un plan de manejo de incidentes que fuera un factor relevante y fundamental en sus procesos o metas organizacionales, por lo que se debe aumentar la importancia de cada proceso según se requiera. Entonces, al validar cómo las universidades están preparadas para manejar incidentes, muestran que no tienen los recursos para administrar los incidentes de seguridad que puedan ocurrir, y no tienen suficientes controles para incorporar grandes cantidades de ciberdelincuentes en su tecnología. Analice cada uno de ellos simultáneamente. respuesta del administrador Una ola de intentos de infraestructura.

La metodología para evaluar la madurez de la gestión de incidentes está diseñada para ayudar a las organizaciones cuando necesitan comprender en qué nivel se encuentran y si sus procesos están alineados con las buenas prácticas para los programas de gestión de incidentes implementados, esto se puede lograr mediante la creación de una herramienta que La herramienta permite universidades para realizar autoevaluaciones, determinando así su estado de madurez, y

una vez que los resultados estén disponibles, puedan tomar acciones para fortalecer sus procesos de gestión de incidentes.

Definir cada fase de la gestión de incidentes de ciberseguridad con referencia a las mejores prácticas a través de un proceso de autoevaluación que permita medir el nivel de madurez de las instituciones de educación superior, con base en los principios de eficacia y cumplimiento. Teniendo en cuenta que se trata de un pilar fundamental de la protección de la información, se considera por tanto un elemento esencial en la toma de decisiones en los ámbitos estratégico y técnico.

Como se mencionó anteriormente, el método elegido para establecer los criterios y fases fue el modelo CMMI (Capability Maturity Model Integration) porque es un modelo de procesos y comportamiento que ayuda a las organizaciones a optimizar la mejora de los procesos y fomenta el comportamiento y la eficiencia de la producción, reduciendo así los riesgos internos. (Becerra, 2021) Con el fin de que las organizaciones determinen su nivel de madurez en la gestión de incidentes de ciberseguridad, se construyeron los siguientes niveles según CMMI:

Tabla 9. Nivel de madurez CMMI

Niveles	Definición
1. No existe	Ausencia total de cualquier proceso o actividad identificable para gestionar incidentes de ciberseguridad. La empresa ni siquiera reconoció que había un problema que solucionar.
2. Inicial	Existe evidencia de que la empresa reconoce que existe un problema y que debe abordarse. Sin embargo, no existe un proceso estandarizado. El enfoque general para gestionar los procesos de gestión de incidentes es fortuito.

3. Definido	Los procedimientos de gestión de incidentes de ciberseguridad están estandarizados y documentados, y se difunden a través de una capacitación limitada. Sin embargo, depende de la persona utilizar estos procedimientos y es poco probable que se detecte un sesgo.
4. Administrado	La entidad cuenta con métricas de apego al plan de gestión de incidentes y mejoras basadas en buenas prácticas sectoriales aplicadas a instituciones educativas, testeando para asegurar la efectividad del proceso.
5. Optimizado	Con base en los resultados de la mejora continua y los modelos probados con otras empresas, el proceso de gestión de incidentes de seguridad cibernética se ha perfeccionado al nivel de las mejores prácticas.

Fuente: adaptado de (Baldonedo, 2017)

4.1.4 Caracterización de los principales riesgos de ciberseguridad existentes que puedan ayudar a minimizar los incidentes dentro de la IES (Instituciones de educación superior).

Los riesgos de ciberseguridad existen en todo tipo de empresas que disponen de tecnologías que pueden vulnerar la protección de toda la información que existe en la organización que se gestiona con el objetivo de pasar estos datos a terceros malintencionados. Con el fin de identificar los principales riesgos, amenazas, debilidades y vulnerabilidades que se puedan presentar, se parte de un inventario de la infraestructura técnica de la Universidad del Cesar Popular - Aguachica, de cada uno de los bienes que posee la Universidad para posibilitar el

normal funcionamiento de los servicios que se brindan, el principal es construir el nivel clave como se muestra a continuación:

Niveles de criticidad para incidentes de ciberseguridad

Para cada evento que ocurre se establece, estructura y describe el impacto según la situación de la siguiente manera: NCA (criticidad alto), NCM (criticidad medio), NCB (criticidad bajo).

Tabla 10. Niveles de criticidad de incidentes

Niveles	Rango	Descripción
Alto	**6 - 10**	Uno o más incidentes detectados.
Medio	**3 – 6**	Requiere revisión para prevenir amenazas.
Bajo	**0 - 3**	Sin impacto

Fuente: elaboración propia.

4.1.5 Infraestructura Tecnológica de la Universidad Popular del Cesar Seccional Aguachica.

La dependencia estableció 5 nodos en puntos estratégicos para poder conectarse a cualquier dependencia dentro del área general de trabajo, estos nodos se establecieron de la siguiente manera:

Tabla 11.Características nodo principal (Llegada del canal dedicado)

Nombre	Descripción
Topologías de red física	Estrella extendida

Canales dedicados Colombus fibras ópticas	80 megas
Routers	Cisco catalist 3560-X
Balanceadores	Peplink Balance 560
Controladoras Wifis	Ruckus Factor 1200
Routers	Raisecom Fibra Colombus
Ubicación	Segundo Piso
Tipos de Racks	Armario bastidor 42 Ru
Servidores	HP Proliant

Fuente: elaboración propia.

Tabla 12. Características nodo Sala de Informática.

Nombre	Descripción
Topología de red física	Estrella extendida
Routers	Cisco catalist 2960
Tipo de Rack	Armario bastidor 30 Ru

Fuente: elaboración propia.

Tabla 13. Características nodo Bienestar Universitario

Nombre	Descripción
Topología de red física	Estrella extendida
Router	Cisco catalist 2960
Ubicación	Bienestar Universitario
Tipo de Rack	Armario bastidor 30 Ru

Fuente: elaboración propia.

Tabla 14. Características nodo Registro y control

Nombre	Descripción
Topología de red física	Estrella extendida
Router	Cisco catalist 3560-X
Ubicación	Registro y Control
Tipo de Rack	Armario bastidor 11 Ru

Fuente: elaboración propia.

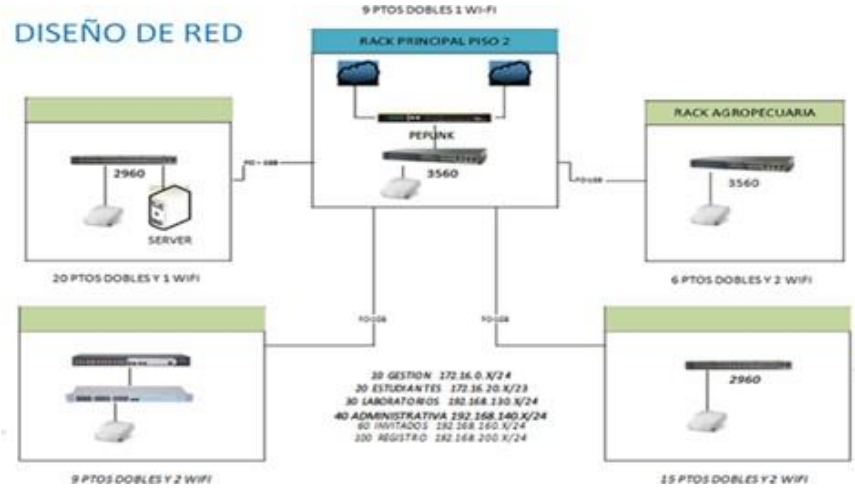
Tabla 15. Características nodo Laboratorio de Redes y Telecomunicaciones

Nombre	Descripción
Topologías de red física	Estrella extendida
Routers	Cisco catalist 3560-X
Ubicación	Laboratorio de Redes y telecomunicaciones
Tipo	Rack de piso

Fuente: elaboración propia.

Esquema lógico de la red

Figura 16. Distribución de la red



Fuente: elaboración propia.

4.1.6 Sistemas de información

Tabla 16. Sistemas de información usados por la Universidad Popular del Cesar Aguachica

Nombre	Característica
Academusoft	El sistema de información integra una gran cantidad de módulos para la gestión funcional de los diversos componentes administrativos y académicos de la institución. El campus cuenta con módulos como: Admisiones, Expedientes Académicos, Recursos Académicos, Carga Académica, Admisiones Académicas, Admisiones Financieras, Recursos Físicos, Horarios, Grados,

	Egresados, etc. Este sistema es utilizado por diversas oficinas, para mecanismo.
Sysman	Software de registro de inventario utilizado localmente almacén
Hemeroteca - Siibupc	Sistema de la biblioteca para registrar, inventariar, clasificar, controlar, prestar y devolver elementos bibliográficos relacionados.

Fuente: elaboración propia.

4.1.7 Servidores

Tabla 17. Servidores de la UPC

	Función	**Referencia**	**Sistema Operativo**
Servidor 1	Aula Virtual de aprendizaje AVA	Dell	Virtualizado (Windows, Debían)
Servidor 2	Practica para Laboratorios	Hp Proliant	Virtualizado (Ubuntu Server)

Fuente: elaboración propia.

4.2 Definición del modelo de ciberseguridad para resolver incidentes en las (IES) Instituciones de educación superior

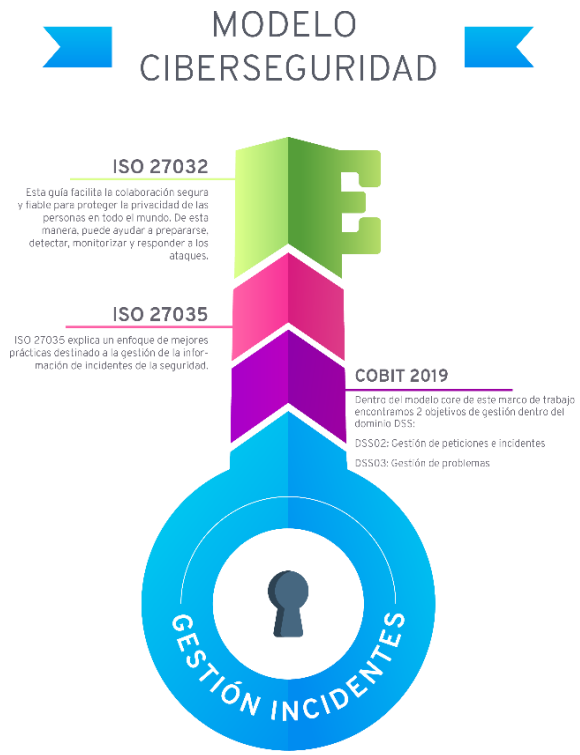
4.2.1 Modelo de ciberseguridad para resolver incidentes en las instituciones de educación superior

4.2.1.1 Introducción. En este capítulo se presenta la propuesta del modelo que da solución a la problemática presentada anteriormente, adoptando las mejores prácticas de TI de los marcos internacionales que permiten dar un cumplimiento a los objetivos planteados en el proyecto.

Las guías de trabajo que se utilizaran son COBIT 2019 que permite dentro de sus principios abordar hacen referencia a DSS02 Gestión de peticiones e incidentes y DSS03 Gestión de problemas, también se estableció un apoyo con la norma ISO 27032 y la ISO27035 para lo que tiene que ver con el manejo del riesgo en la ciberseguridad y la gestión de incidentes en el area de TI.

Dentro de este capítulo se realizarán unos entregables que son elaborados con el fin de cumplir con el objetivo general de la investigación, con el que se pretende generar una mejora en los procesos de la gestión de incidentes, se incluyen dos procesos en base a las actividades que menciona COBIT 2019, de igual manera se presenta el detallado del procedimiento para el apoyo de gestión de cada proceso mencionado.

Figura 17. Estructura del modelo de Ciberseguridad



Fuente: elaboración propia.

4.2.2 Alcance del modelo

Inicialmente, se debe establecer el contexto de la institución de educación superior elegida con el objetivo principal de identificar las principales causas de riesgo que ocurren dentro de la entidad, y luego el contexto de los riesgos a evaluar para determinar las necesidades. Durante el mismo proceso se caracterizan los riesgos de mayor criticidad y la organización debe implementar políticas y/o controles para reducir su incidencia. Armados con toda esta información, comenzamos a construir modelos para brindar escalabilidad y adaptabilidad para cada proceso realizado dentro de la universidad y terminamos con la validación de los modelos.

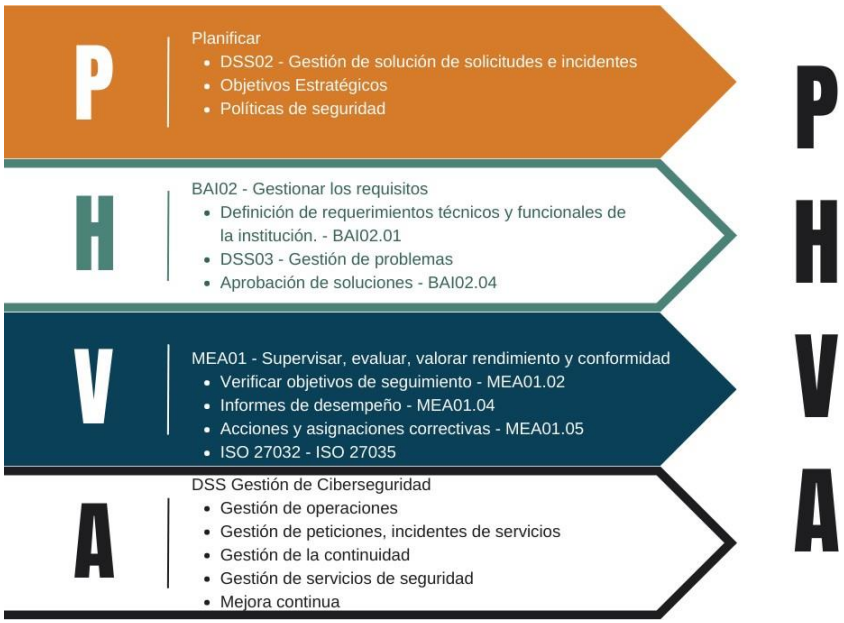
El alcance del modelo propuesto pretende mejorar la gestión de la ciberseguridad para el abordaje de incidentes que se basa en el estándar COBIT 2019, ya que considera una estructura

adecuada para gestionar los requisitos y brindar la factibilidad de las soluciones, y se apoya en el estándar ISO 27032 para promover una seguridad y protección en la seguridad y en la ISO 27035 en donde se estipulan mejores prácticas y orientación para ejecutar un plan de gestión de incidentes de ciberataques y prepararse para una respuesta adecuada que brinde una solución dentro de un marco de tiempo específico. El modelo busca que su correcta aplicación pueda ayudar a mejorar la ciberseguridad de la organización, y su objetivo es precisamente apuntar a los componentes de la infraestructura de red, comunicación, servidor, aplicación web y factores humanos, mediante el apoyo de diversas herramientas y procesos, para lograr una mayor eficiencia y la transparencia de su implementación.

4.2.3 Aplicación del modelo de ciberseguridad

Para aplicar el modelo de ciberseguridad es necesario prepararse de acuerdo a las fases de la metodología PHVA (planificación, ejecución, verificación y acción), utilizando la información obtenida en las fases anteriores, es momento de definir e implementar técnicas y herramientas. para corregir errores y/o mitigar vulnerabilidades descubiertas. Como se ilustra en la Figura 20 a continuación, la importancia de esta fase se basa en mejorar la implementación de tecnología y la ejecución de herramientas de ciberseguridad de la agencia:

Figura 18. Ciclo PHVA



Fuente: elaboración propia

4.2.3.1 Planificar - DSS02: Gestión de solución de solicitudes e incidentes

Proceso para Gestionar solicitudes e Incidentes de servicio – DSS02

Teniendo en cuenta lo anterior se presenta el detallado del primer entregable que hace referencia al proceso COBIT 2019 DSS02 Gestionar solicitudes e Incidentes de Servicio.

1. Registro del proceso

Tabla 18. Registrar procesos de incidentes

Código	N° versión	Fecha	Autor	Detalles
IC01	**1.0**	**07/03/2023**	**Departamento TIC**	**Documentación inicial**
IC02	**1.0**	**07/03/2023**	**Departamento TIC**	**Documentación Inicial**

Fuente: elaboración propia.

2. Descripción del proceso

Proporcionar de forma efectiva una respuesta oportuna a los usuarios de sus incidentes y proveer una solución a las solicitudes realizadas de todo tipo. Restaurar el servicio de forma normal, y registrar las solicitudes que el usuario realice.

3. Propósito del proceso

Lograr una minimización de las interrupciones y una mayor productividad en la resolución de los casos o peticiones que se presenten por parte de los usuarios, de igual manera evaluar el grado de impacto en los cambios y enfrentar los incidentes. Resolver las solicitudes de los usuarios y restaurar los procesos o servicios como una rápida respuesta al incidente.

4. Características del proceso

En la siguiente tabla se muestran las principales características del proceso DSS02.

Tabla 19. Características de los procesos.

Características del proceso DSS02	
Líder del proceso	Jefe de Gestión TIC
Servicio que genera	Sistema y herramientas de seguimiento de incidentes
Medio de comunicación de información	Software de Help Desk / Correo electrónico /
Apoyo al macroproceso que genera	Fomentar la prevención Permitir a los usuarios poder identificar incidentes correctamente y con un plazo adecuado para escalar con las rutas adecuadas. Resolver y responder de forma rápida incidentes

Habilidades	Gestión de incidentes
	Servicio de atención al cliente
	Soporte a usuarios
	Soporte de redes
	Soporte de aplicaciones
Políticas	Política de Resolución de problemas
	Política de solicitud de servicio

Fuente: elaboración propia.

5. Riesgos del proceso

- Recursos insuficientes en tecnologías de la información, o personal con pocas habilidades o sin personal.
- Resistencia de la alta gerencia o miembros de los departamentos lideres para involucrarse en los procesos de TI.
- Limitación de recursos tecnológicos que evitan un adecuado proceso de mejora continua.

6. Alineamientos con los objetivos estratégicos

- Resolver las peticiones de incidentes para no afectar el normal flujo continuo del negocio.
- La resolución de incidentes debe estar adecuadamente alineada con los objetivos misionales de la institución.

7. Indicadores clave de desempeño (KPIs)

En la siguiente tabla se detallan las posibles métricas para la evaluación y desempeño del proceso DSS02.

Tabla 20. Indicadores de desempeño.

ID	Factor Crítico del Éxito	Indicador	Detalle	Frecuencia	Profesional responsable
1	Los procesos del negocio no se ven afectados por los incidentes	Número de incidentes que causan interrupción en los procesos del negocio	Cantidades de incidentes que causaron interrupción en los procesos del negocio	Mensual	Jefe de TIC
2	Los procesos del negocio no se ven afectados por incidentes	Porcentaje de incidentes que causan interrupción en los procesos del negocio	$\frac{Cantidad\_incidentes}{Total\_incidentes\_periodo}$	Mensual	Jefe de TIC
3	El flujo de operaciones del	Número de solicitudes	Cantidad de solicitudes que	Mensual	Jefe de TIC

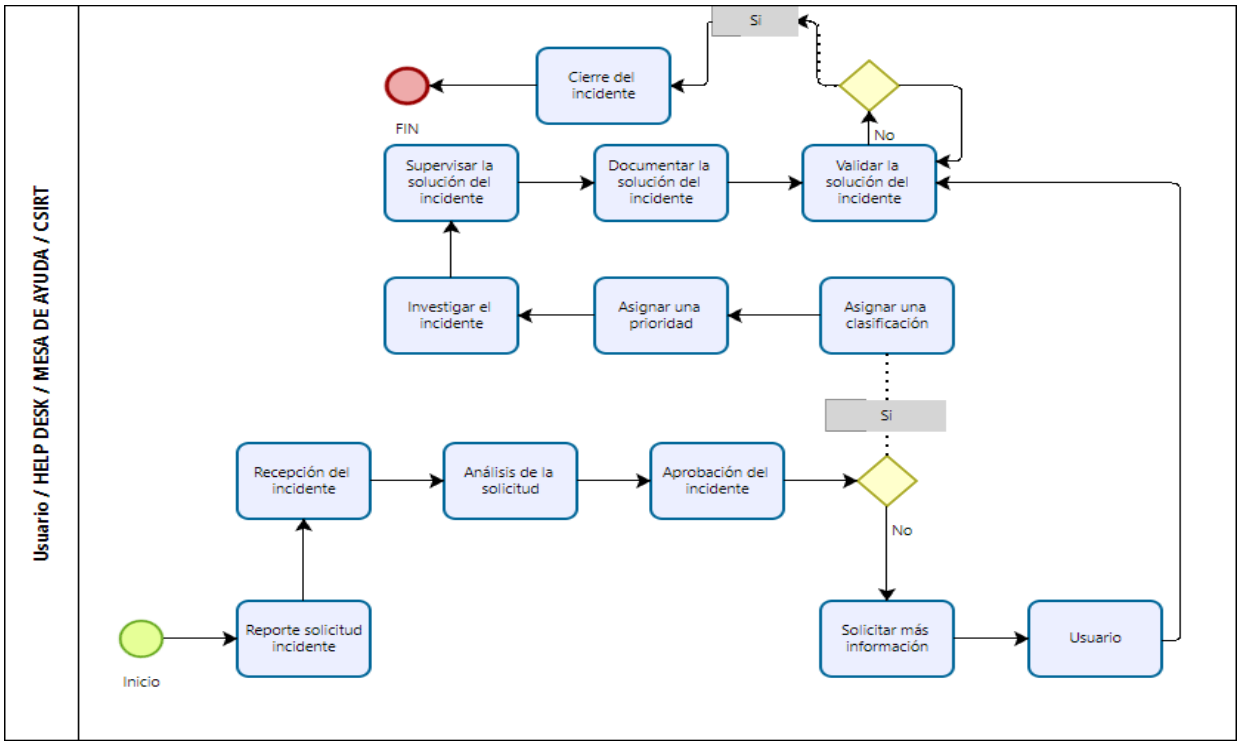
	negocio no se ve afectado por las solicitudes	generadas que afectan el flujo de operaciones del negocio	afectaron el flujo de las operaciones del negocio		
4	Las solicitudes reportadas se resuelven dentro de los tiempos acordados en los acuerdos de nivel de servicio (SLA)	Tiempo promedio de resolución de incidentes menor o igual al acordado	$\frac{Tiempo\_resolucion\_solicitudes}{T\_de\_peticiones\_atentidas\_periodo}$ SLA	Mensual	Jefe de TIC
5	Los usuarios demuestran alto grado de satisfacción por los servicios de gestión de incidentes	Porcentaje de satisfacción por parte de los usuarios con el tiempo de respuesta de resolución	$\frac{Cant\_usuarios\_satisfechos}{}$	Mensual	Jefe de TIC

	de las solicitudes

Fuente: elaboración propia.

8. Diagrama en notación BPM utilizando las mejores prácticas que describe COBIT 2019 para DSS02

Figura 19. BPM para la gestión de incidentes



Fuente: elaboración propia.

9. Procedimiento del proceso

Importancia

Este procedimiento debe tener el debido seguimiento para todos los miembros del equipo de TI en donde se involucra la gestión de las peticiones realizadas por los usuarios como incidentes.

Propósito

El objetivo de este proceso es definir las actividades específicas que permitan una adecuada gestión del proceso DSS02 Gestión de peticiones e incidentes de servicio, que sirva como guía para la correcta gestión del proceso.

Detalle de las actividades del procedimiento DSS02: Gestionar peticiones en incidentes de servicio:

N°	Actividad	Tarea – descripción	Práctica de gestión COBIT 2019	Responsable
1	Recepción de la solicitud o incidente	Con base en los criterios establecidos en la política del proceso, el responsable valida si la solicitud aplica para departamento de TI.	DSS02.03	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
2	Análisis de la solicitud o incidente	El responsable debe analizar la solicitud en búsqueda de determinar si los datos que recibe están completos y elaborados de forma correcta.	DSS02.03	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
3	Aprobación de la solicitud o incidente	Una vez se realice el análisis el responsable encargado debe valorar si el detalle de la solicitud o petición es completa o suficiente	DSS02.03	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico

		para continuar con el flujo del proceso. • Si no es completo el detalle, ir al flujo 4 • Si es completo el detalle ir al flujo 5		Especializado
4	Resolver los detalles de la solicitudes o incidentes	Una vez el responsable solicita más detalles respecto a la solicitud o petición, el usuario debe describir lo más detallado posible respecto a la solicitud inicial reportada.	DSS02.03	Usuario
5	Revisión y validación de los esquemas y modelos existentes	El responsable revisa y valida los esquemas y modelos existentes para validar si la solicitud puede ser gestionada a través de los esquemas y modelos que se definieron previamente.	DSS02.01	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
6	Asignación de clasificación de la solicitud o incidente	El responsable debe asignar una clasificación a la solicitud teniendo en cuenta: • Establecer la clasificación que el usuario asigno en los detalles de la solicitud. • Establecer una nueva clasificación con base en el modelo de la solicitud.	DSS02.02	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado

7	Asignar la prioridad a la solicitud o incidente	El responsable deberá asignar una prioridad a la solicitud enviada, teniendo en cuenta: • Establecer la prioridad que el usuario asigno en los detalles de la solicitud • Establecer una nueva prioridad con base en el modelo de la solicitud.	DSS02.02	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
8	Evaluar la solicitud o incidente	La alta gerencia evalúa la solicitud o incidente con base en los criterios definidos por la organización	DSS02.03	Alta gerencia
9	Aprobación de la solicitud o incidente	Una vez se realice la evaluación de la solicitud, la alta gerencia genera un criterio sobre el estado de la solicitud • Si se aprueba, ir al flujo 10 • Si no, informar al usuario la razón del rechazo de la solicitud.	DSS02.03	Alta gerencia
10	Investigar la solicitud o incidente	• El responsable investiga la solicitud o incidente validando los errores o síntomas conocidos,	DSS02.03	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico

		también analiza las posibles causas raíz de la solicitud o incidente. • El responsable aplica acciones correctivas de ser necesario. • En caso de ser necesario se deben asignar la solicitud o el incidente al especialista si se requiere una mayor habilidad con base a la política de servicio. DSS02		Especializado
11	Supervisar la solicitud o incidente	Una vez se identifica que el incidente es un problema, se debe establecer mediante la política del proceso DSS03 COBIT 2019: Política de resolución de problemas. El responsable realiza el seguimiento del caso y solicita si es pertinente los procedimientos de manejo del incidente para progresar en la resolución de este.	DSS02.07	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
12			DSS02.05	Jefe de TIC, Profesional

	Documentar la solicitud o incidente	El responsable debe realizar las operaciones que sean necesarias para proponer una solución con base en la información recolectada durante la gestión de la solicitud o incidente. El responsable debe documentar si la solución propuesta es temporal o definitiva.		especializado, Profesionales Contratistas, Técnico Especializado
13	Validación por parte del usuario la solución propuesta	El usuario revisa la solución propuesta y verifica la validez de esta.	DSS02.06	Usuario
14	Cerrar la solicitud o incidente	Una vez el responsable resuelve la solicitud o incidente y es aprobada, se realiza el cierre formal de la solicitud o incidente gestionado.	DSS02.06	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
15	Enviar encuesta de satisfacción	El responsable de TI debe enviar una encuesta por formulario o correo electrónico una encuesta de satisfacción en atención de la solicitud o incidente solucionado.	DSS02.07	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado

Fuente: elaboración propia.

4.2.3 Hacer – BAI02 - Políticas de solicitud de servicios

A continuación, se define una política generalizada para el proceso bajo en nombre DSS02 COBIT 2019: Política de solicitud de servicio.

1. **Descripción**

Determinar los fundamentos y directrices para la recepción de solicitudes de servicios e incidentes y su respectiva documentación, a su vez contiene los lineamientos a seguir para la correcta gestión de los procesos BAI02 - DSS02 y los recursos asignados junto con la asignación de roles y responsabilidades en las actividades definidas en el proceso.

2. **Objetivo**

Determinar los lineamientos que ejecuten de manera correcta las solicitudes e incidentes de servicio que sean recibidas por el equipo o departamento de TI de la institución.

3. **Alcance**

Esta política aplica para todos los miembros del equipo o departamento de TI de la institución.

4. **Lineamientos**

4.1 Lineamientos de administración de solicitudes

4.1.1 Las solicitudes generadas por usuarios del entorno de la institución serán aceptadas siempre y cuando estén relacionadas con elementos tecnológicos ya sean temas de hardware o software.

4.1.2 Las solicitudes deben ser recibidas por el aplicativo de Help Desk implementado por la institución y/o correo electrónico.

4.1.3 Para realizar el análisis de la solicitud se debe verificar que contenga los datos completos del usuario que la genera, la categoría y la prioridad establecida, así como el detalle completo de la solicitud, si es necesario se deben solicitar mas detalles al usuario.

4.1.4 Se debe establecer la prioridad de las solicitudes utilizando como base los modelos definidos y acordados en los Service Level Agreement teniendo en cuenta el impacto y la premura del negocio.

4.1.5 Las solicitudes que sea rechazadas por la alta gerencia, generan un mensaje con él porque del rechazo y se debe enviar al usuario.

4.1.6 En el momento que se obtenga la aprobación de la solución de la solicitud, se debe cerrar el incidente y se le debe enviar al usuario la encuesta de satisfacción.

4.1.7 Cuando se cierre de la solicitud el responsable de TI debe establecer si es necesario agregar información importante para fortalecer las fuentes de conocimiento sobre las solicitudes.

4.2 Lineamientos de administración de incidentes

4.2.1 Los incidentes generados por usuarios del entorno de la institución serán aceptadas siempre y cuando estén relacionadas con elementos tecnológicos ya sean temas de hardware o software.

4.2.2 Los incidentes deben ser recibidas por el aplicativo de Help Desk implementado por la institución.

4.2.3 Para realizar el análisis del incidente se debe verificar que contenga los datos completos del usuario que la genera, la categoría y la prioridad establecida, así como el detalle completo del incidente, si es necesario se deben solicitar más detalles al usuario.

4.2.4 Se debe establecer la prioridad de los incidentes utilizando como base los modelos definidos y acordados en los Service Level Agreement teniendo en cuenta el impacto y la premura del negocio.

4.2.5 Los incidentes que sean rechazados por la alta gerencia, generan un mensaje con él porque del rechazo y se debe enviar al usuario.

4.2.6 En el momento que se obtenga la aprobación de la solución del incidente, se debe cerrar el incidente y se le debe enviar al usuario la encuesta de satisfacción.

4.2.7 Cuando se cierre el incidente el responsable de TI debe establecer si es necesario agregar información importante para fortalecer las fuentes de conocimiento sobre los incidentes.

5. Recursos asignados

Personal con habilidades y conocimientos en:

- Soporte de aplicaciones
- Gestión de incidentes
- Soporte de redes
- Soporte de usuarios

6. Responsabilidad y roles

En la tabla 21 se muestra una matriz donde se detallan las actividades con las responsabilidades en los diferentes roles establecidos.

Tabla 21. Roles y responsabilidades

MATRIZ RACI					
R: Responsable **A: Aprueba** **C: Consulta** **Practica clave de gobierno**	**Usuario**	**Jefe TIC**	**Profesional especializado**	**Contratista especializado**	**Técnico especializado**
Recepción de la solicitud o incidente			**A**	**C**	**C**

Análisis de la solicitud o incidente		**R**	**A**	**C**	**C**
Aprobación de la solicitud o incidente		**R**	**A**	**C**	**C**
Resolver los detalles de la solicitudes o incidentes	**A**	**R**	**A**	**C**	**C**
Revisión y validación de los esquemas y modelos existentes		**R**	**A**	**C**	**C**
Asignación de clasificación de la solicitud o incidente		**R**	**A**	**C**	**C**
Asignar la prioridad a la solicitud o incidente		**R**	**A**	**C**	**C**
Evaluar la solicitud o incidente		**R**	**A**	**C**	**C**
Aprobación de la solicitud o incidente		**R**	**A**	**C**	**C**
0. Investigar la solicitud o incidente		**R**	**A**	**C**	**C**
1. Supervisar la solicitud o incidente		**R**	**A**	**C**	**C**
2. Documentar la solicitud o incidente		**R**	**A**	**C**	**C**
3. Validación por parte del usuario la solución propuesta		**R**	**A**	**C**	**C**
4. Cerrar la solicitud o incidente		**R**	**A**	**C**	**C**
5. Enviar encuesta de satisfacción	**A**	**R**	**A**	**C**	**C**

Fuente: elaboración propia.

4.2.4 DSS03: Gestión de problemas

Gestión problemas – DSS03

Teniendo en cuenta lo anterior se presenta el detallado del primer entregable que hace referencia al proceso COBIT 2019 DSS03 Gestionar problemas.

4.2.4.1 Definición del proceso

A. Registro del proceso

Tabla 22. Gestión de problemas

Código	N° versión	Fecha	Autor	Detalles
IC01	**1.0**	**07/03/2023**	**Departamento TIC**	**Documentación inicial**
IC02	**1.0**	**07/03/2023**	**Departamento TIC**	**Documentación inicial**

Fuente: elaboración propia.

B. Descripción del proceso

Proporcionar de forma efectiva una respuesta oportuna a los usuarios de los problemas reportados y proveer una solución a los problemas reportados de todo tipo. Restaurar el servicio de forma normal, y registrar los problemas que el usuario reporte.

C. Propósito del proceso

Lograr una minimización de las interrupciones y una mayor productividad en la resolución de los problemas reportados que se presenten por parte de los usuarios, de igual manera evaluar el grado de impacto en los cambios y enfrentar los problemas. Resolver los problemas de los usuarios y restaurar los procesos o servicios como una rápida respuesta al problema.

D. Características del proceso

En la siguiente tabla se muestran las principales características del proceso DSS03.

Tabla 23. Características de los procesos para resolución de problemas

Características del proceso DSS03	
Líder del proceso	Jefe de Gestión TIC
Servicio que genera	Sistema y herramientas de seguimiento de incidentes
Medio de comunicación de información	Software de Help Desk / Correo electrónico /
Apoyo al macroproceso que genera	Fomentar la solución de gestión de problemas Aumentar la cultura de gestión de problemas utilizando la detección, acción y prevención definiendo los roles de manera clara. Crear un entorno eficaz para reportar e informar sobre problemas.
Habilidades	Soporte de problemas Soporte de redes Soporte de aplicaciones
Políticas	Política de Resolución de problemas Política de solicitud de servicio

Fuente: elaboración propia.

E. Riesgos del proceso

- Resistencia de la alta gerencia o miembros de los departamentos lideres para involucrarse en los procesos de TI.
- Poco apoyo administrativo para la gestión del proceso

- Poca relación técnica entre las áreas de TI y los usuarios lo que genera una mala comunicación entre ambas partes
- Cambios organizaciones en otras áreas sin contemplar el departamento de TI

F. Alineamientos con los objetivos estratégicos

- Resolver las peticiones de incidentes para no afectar el normal flujo continuo del negocio.
- La solución propuesta debe resolver totalmente los problemas sin afectar las operaciones del negocio.

G. Indicadores clave de desempeño (KPIs)

En la siguiente tabla se detallan las posibles métricas para la evaluación y desempeño del proceso DSS03.

Tabla 24. Indicadores de desempeño (Problemas)

ID	Factor Crítico del Éxito	Indicador	Detalle	Frecuencia	Profesional responsable
01	Los procesos del negocio no se ven afectados por los problemas	Número de problemas que causan interrupción en los procesos del negocio	Cantidades de problemas que causaron interrupción en los procesos del negocio	Mensual	Jefe de TIC
02	Los procesos del negocio no	Porcentaje de	$\frac{Cantidad\_problemas}{Total\_problemas\_periodo}\ x\ 100$	Mensual	Jefe de TIC

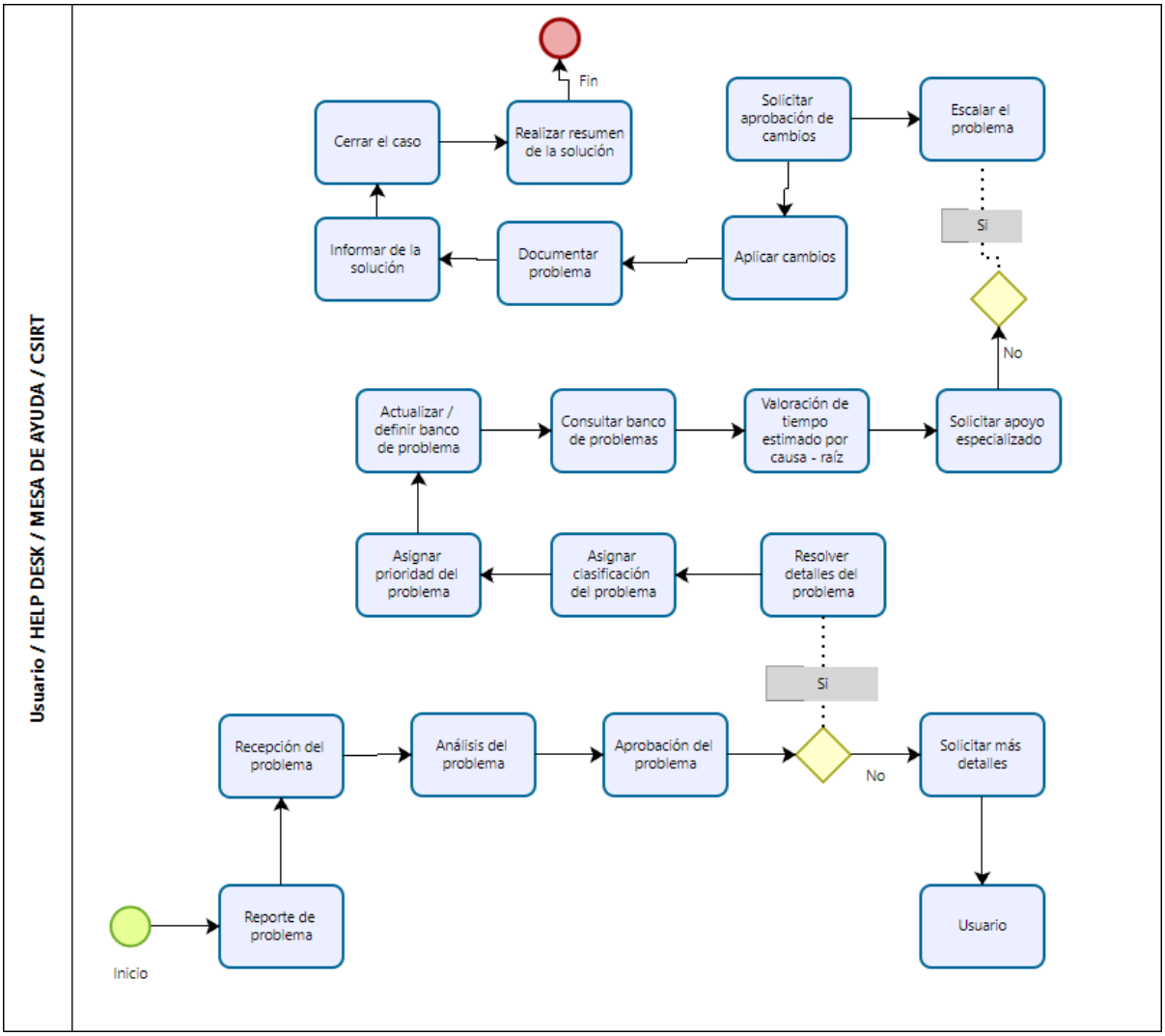
	se ven afectados por problemas	problemas que causan interrupción en los procesos del negocio			
03	El flujo de operaciones del negocio no se ve afectado por los problemas	Número de problemas generadas que afectan el flujo de operaciones del negocio	Cantidad de problemas que afectaron el flujo de las operaciones del negocio	Mensual	Jefe de TIC
04	Los problemas reportados se resuelven dentro de los tiempos acordados en los acuerdos de nivel de servicio (SLA)	Tiempo promedio de resolución de problemas menor o igual al acordado	$\frac{Tiempo\_resolucion\_problemas}{SLA} \leq$	Mensual	Jefe de TIC

05	Los usuarios demuestran alto grado de satisfacción por los servicios de gestión de problemas	Porcentaje de satisfacción por parte de los usuarios con el tiempo de respuesta de resolución de los problemas	$\frac{Cant\_usuarios\_satisfechos}{T\_usuarios\_encuestados} x\ 100$	Mensual	Jefe de TIC

Fuente: elaboración propia.

H. Diagrama en notación BPM utilizando las mejores prácticas que describe COBIT 2019 para DSS03

Figura 20. BPM Gestión de problemas



Fuente: elaboración propia.

I. Procedimiento del proceso

Importancia

Este procedimiento debe tener el debido seguimiento para todos los miembros del equipo de TI en donde se involucra la gestión problemas reportados por los usuarios.

Propósito

El objetivo de este proceso es definir las actividades específicas que permitan una adecuada gestión del proceso DSS03 Gestión problemas, que sirva como guía para la correcta gestión del proceso.

Detalle de las actividades del procedimiento DSS02: Gestionar peticiones en incidentes de servicio:

Tabla 25. Gestionar peticiones de incidentes

N°	Actividad	Tarea – descripción	Practica de gestión COBIT 2019	Responsable
1	Recepción del problema reportado	Con base en los criterios establecidos en la política del proceso, el responsable valida si la solicitud aplica para departamento de TI.	DSS03.01	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
2	Análisis del problema reportado	El responsable debe analizar el problema en búsqueda de determinar	DSS03.01	Jefe de TIC, Profesional

		si los datos que recibe están completos y elaborados de forma correcta.		especializado, Profesionales Contratistas, Técnico Especializado
3	Aprobación del problema reportado	Una vez se realice el análisis el responsable encargado debe valorar si el detalle del reporte del problema es completo o suficiente para continuar con el flujo del proceso. Si no es completo el detalle, ir al flujo 4 Si es completo el detalle ir al flujo 5	DSS03.01	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
4	Resolver los detalles del problema reportado	Una vez el responsable solicita más detalles respecto al problema, el usuario debe describir lo más detallado posible respecto al problema inicial reportado.	DSS03.01	Usuario
5	Revisión y validación de los esquemas y modelos existentes	El responsable revisa y valida los esquemas y modelos existentes para validar si el problema puede ser gestionado a través de los esquemas y	DSS03.01	Jefe de TIC, Profesional especializado, Profesionales

		modelos que se definieron previamente.		Contratistas, Técnico Especializado
6	Asignación de clasificación del problema reportado	El responsable debe asignar una clasificación al problema teniendo en cuenta: Establecer la clasificación que el usuario asigno en los detalles del problema reportado. Establecer una nueva clasificación con base en el modelo del problema reportado.	DSS03.01	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
7	Asignar la prioridad al problema reportado	El responsable deberá asignar una prioridad al problema reportado, teniendo en cuenta: Establecer la prioridad que el usuario asigno en los detalles del problema reportado	DSS03.01	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado

		Establecer una nueva prioridad con base en el modelo del problema reportado.		
8	Actualizar / definir banco de problemas	Al contar con una prioridad para el problema se debe actualizar o definir el banco de problemas para realizar el registro del problema con base en la política del proceso DSS03 COBIT 2019: Política de resolución de problemas	DSS03.01	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
9	Consultar banco de problemas	Una vez actualizada o definido el banco de problemas, el responsable del proceso debe consultar el banco de problemas para encontrar similitudes con incidentes, errores y problemas que ya fueron solucionados.	DSS03.02	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
10	Determinar la causa – raiz	El responsable del proceso verifica si la información recolectada luego de	DSS03.02	Jefe de TIC, Profesional

		utilizar un proceso de ingeniería inversa y consultar el banco de problemas determina la causa – raíz, de no ser así podría volver a consultar el banco de problemas.		especializado, Profesionales Contratistas, Técnico Especializado
11	Valoración del tiempo estimado por causa – raíz	El responsable del proceso valora si la causa – raíz del problema reportado podrá ser identificado sin consumir más tiempo del estimado para la verificación, esto se indica en la política del proceso DSS03 COBIT 2019: Política de resolución de problemas, de lo contrario deberá recibir apoyo de un especialista dentro del equipo de trabajo. Si es positiva la acción ir al flujo 12 Si es negativa la acción ir al flujo 13	DSS03.01 DSS03.02	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
12	Definir los detalles del problema reportado	El responsable del proceso debe realizar lo siguiente:		

		Debe realizar los registros del error del problema. Debe asociar los elementos de configuración afectados con el error establecido. Producir un informe para evidenciar el progreso según lo establecido en la política del proceso DSS03 COBIT 2019: Política de resolución de problemas.	DSS03.02 DSS03.03	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
13	Resolver solicitud de apoyo de especialista	El especialista basado en sus habilidades investiga y genera la identificación de la causa – raíz del problema reportado.	DSS03.01 DSS03.02	Profesional especializado
14	Validar si el problema reportado debe ser escalado	Si teniendo en cuenta el apoyo del especialista y validando las propuestas de solución disponibles o soluciones alternas implementadas no se resuelve el problema reportado según el proceso DSS03 COBIT	DSS03.04	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado

		2019: Política de Resolución de problemas. Si no se resuelve se debe escalar, continue el flujo 14 Si no se debe escalar, continue el flujo 15		
15	Escalar el problema reportado	El especialista en apoyo con el responsable del proceso escala el problema a aun siguiente nivel de soporte, cambiando la prioridad del ticket con base en el impacto y urgencia del negocio.	DSS03.04	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
16	Validar si se requieren cambios como solución al problema	Si el problema reportado no debe ser escalado, se debe valor si se requieren cambios como solución al problema. Si, ir al flujo 16 No, ir al flujo 17	DSS03.04	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico

				Especializado
17	Solicitar aprobación de gestión de cambios	Para los problemas identificados que requieran cambios se debe realizar la respectiva solicitud de aprobación de cambios a través de la gestión de cambios.	DSS03.04	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
18	Documentar solución del problema	Cuando se tenga la solución al problema reportado, sea temporal, permanente o se halla solicitado un cambio a la gestión del problema, se debe documentar de manera clara todo el proceso, indicando los procedimientos realizados, insumos utilizados o cualquier otro recurso que el responsable considere importante y relevante.	DSS03.04 DSS03.05	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
19	Informar solucionar del problema reportado	El responsable del proceso debe realizar los informes correspondientes a las soluciones acordadas para cada problema	DSS03.04 DSS03.05	Jefe de TIC, Profesional especializado, Profesionales

		gestionado, incluyendo la gestión de cambios de TI que involucren la resolución del problema.		Contratistas, Técnico Especializado
20	Cerrar el problema	Cuando la propuesta de solución al problema fue aceptada por las partes afectadas, el responsable del proceso debe realizar el cierre formal del problema gestionado.	DSS03.04	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado
21	Realizar resumen del problema reportado	El responsable del proceso debe realizar lo siguiente: Cerrado el problema reportado se debe realizar un resumen que incluya una recopilación de los datos recolectados durante el proceso. Se debe incluir la información relacionada con cambios e incidentes de TI	DSS03.05	Jefe de TIC, Profesional especializado, Profesionales Contratistas, Técnico Especializado

Fuente: elaboración propia.

4.2.5 Política de solicitud de servicio

A continuación, se define una política generalizada para los procesos bajo el nombre de BAI02 - DSS03 COBIT 2019: Resolución de problemas.

1. **Descripción**

Determinar los fundamentos y directrices para la recepción de reporte de problemas y su respectiva documentación, a su vez contiene los lineamientos a seguir para la correcta gestión del proceso DSS03 y los recursos asignados junto con la asignación de roles y responsabilidades en las actividades definidas en el proceso.

2. **Objetivo**

Determinar los lineamientos que ejecuten de manera correcta la solución a los problemas reportados por los usuarios para el equipo o departamento de TI de la institución.

3. **Alcance**

Esta política aplica para todos los miembros del equipo o departamento de TI de la institución.

4. **Lineamientos**

4.1 Lineamientos de administración de solicitudes

4.1.1 Los problemas reportados por usuarios del entorno de la institución serán aceptadas siempre y cuando estén relacionadas con elementos tecnológicos ya sean temas de hardware o software.

4.1.2 Los problemas reportados deben ser recibidos por el aplicativo de Help Desk implementado por la institución y/o correo electrónico.

4.1.3 Para realizar el análisis del problema reportado se debe verificar que contenga los datos completos del usuario que la genera, la categoría y la prioridad establecida, así como el detalle completo del problema, si es necesario se deben solicitar más detalles al usuario.

4.1.4 Los problemas reportados deben contar con los detalles completos para su resolución, de no ser así el responsable debe solicitarle al usuario mas detalles sobre el problema reportado.

4.1.5 Se debe validar mediante los esquemas y/o modelos existentes los problemas reportados para encontrar posibles soluciones que faciliten la gestión del problema de manera oportuna y rápida.

4.1.6 Se debe asignar una clasificación para el problema reportado.

4.1.7 Se debe establecer la prioridad al problema reportado utilizando como base los modelos definidos y acordados en los Service Level Agreement teniendo en cuenta el impacto y la premura del negocio.

4.1.8 Luego de que el problema reportado cuente con una clasificación y una prioridad se deben actualizar y/o definir el banco de problemas para realizar el debido registro del problema reportado.

4.1.9 Se debe consultar el banco de problemas reportados para realizar una comparación y buscar similitudes con resoluciones a problemas que ya fueron solucionados.

4.1.10 Se debe determinar la causa – raíz realizando consultas al banco de problemas.

4.1.11 El responsable verifica si la causa – raíz puede ser identificada sin consumir más tiempo del estimado, de no ser así debe solicitar apoyo de un especialista con que se cuente dentro del equipo de trabajo.

4.1.12 Se deben definir los detalles del problema reportado, registrando el error del problema, de igual manera se deben asociar los elementos de configuración afectados con el error

establecido y se debe producir un informe que evidencie el progreso de la resolución del problema reportado.

4.1.13 Resolver el problema reportado con apoyo y/o ayuda de un especialista dentro del equipo de trabajo.

4.1.14 En caso de no lograr mediante apoyo del especialista la resolución del problema reportado se debe validar si este debe ser escalado a una area con un nivel más alto.

4.1.15 Luego de la validación para realizar el escalado y de ser afirmativa el especialista escala el problema a un siguiente nivel y debe cambiar la prioridad del ticket teniendo como base el impacto y urgencia del negocio.

4.1.16 Se debe validar si se requieren cambios para la resolución del problema reportado.

4.1.17 Se debe solicitar aprobación para gestionar los cambios, esto se debe realizar mediante la gestión de cambios y solo el jefe de la oficina de TIC puede dar aprobación para esta situación.

4.1.18 El responsable debe documentar la solución del problema reportado incluyendo procedimientos realizados, insumos utilizados o cualquier otro recurso que el responsable considere importante y relevante.

4.1.19 El responsable del proceso debe realizar los informes correspondientes a las soluciones acordadas para cada problema gestionado, incluyendo la gestión de cambios de TI que involucren la resolución del problema.

4.1.20 El problema reportado debe ser cerrado si la propuesta solución es aceptada por las partes interesadas en este caso el responsable de atender la solicitud y el usuario que reporta el problema.

4.1.21 El responsable debe realizar un resumen del problema en donde se recopilen los datos relevantes que obtuvo durante el proceso, se debe incluir información relacionada con los cambios e incidentes de TI.

4.2 Lineamientos de administración de incidentes

4.2.1 Los problemas reportados por usuarios del entorno de la institución serán aceptadas siempre y cuando estén relacionadas con elementos tecnológicos ya sean temas de hardware o software.

4.2.2 Los problemas deben ser recibidos por el aplicativo de Help Desk implementado por la institución y/o correo electrónico autorizado.

4.2.3 Para realizar el análisis del problema se debe verificar que contenga los datos completos del usuario que la genera, la categoría y la prioridad establecida, así como el detalle completo del problema, si es necesario se deben solicitar más detalles al usuario.

4.2.4 Se debe establecer la prioridad del problema utilizando como base los modelos definidos y acordados en los Service Level Agreement teniendo en cuenta el impacto y la premura del negocio.

4.2.7 Cuando se cierre el problema el responsable de TI debe establecer si es necesario agregar información importante para fortalecer las fuentes de conocimiento sobre las resoluciones realizadas.

5. Recursos asignados

Personal con habilidades y conocimientos en:

- Soporte de aplicaciones
- Soporte de redes
- Soporte de usuarios

6. Responsabilidad y roles

En la siguiente tabla matriz se detallan las actividades con las responsabilidades en los diferentes roles establecidos.

Tabla 26. Matriz RACI

MATRIZ RACI					
R: Responsable A: Aprueba C: Consulta Practica clave de gobierno	**Usuario**	**Jefe TIC**	**Profesional especializado**	**Contratista especializado**	**Técnico especializado**
Recepción del problema			**R**	**A**	**C**	**C**
Análisis del problema			**R**	**A**	**C**	**C**
Aprobación del problema			**R**	**A**	**C**	**C**
Resolver los detalles del problema reportado	**A**		**R**	**A**	**C**	**C**
Revisión y validación del problema reportado en los esquemas y modelos existentes			**R**	**A**	**C**	**C**
Asignación de clasificación al problema reportado			**R**	**A**	**C**	**C**
Asignar la prioridad al problema reportado			**R**	**A**	**C**	**C**
Actualizar / definir banco de preguntas			**R**	**A**	**C**	**C**
Consultar banco de preguntas			**R**	**A**	**C**	**C**
. Determinar la causa – raíz			**R**	**A**	**C**	**C**
. Validación del tiempo estimado por causa – raíz			**R**	**A**	**C**	**C**
. Definir los detalles del problema reportado			**R**	**A**	**C**	**C**
. Resolver solicitud de apoyo del especialista			**R**	**A**	**C**	**C**
. Validar si el problema necesita ser escalado			**R**	**A**	**C**	**C**

. Escalar el problema reportado a un siguiente nivel	**A**	**R**	**A**	**C**	**C**
. Validar si se requieren cambios como solución al problema		**R**	**A**	**C**	**C**
. Solicitar confirmación de jefe de TIC para realizar cambios, estos cambios deben solicitarse por intermedio de gestión de cambios.		**R**	**A**	**C**	**C**
. Documentar solución del problema reportado		**R**	**A**	**C**	**C**
. Informar sobre la solución del problema reportado		**R**	**A**	**C**	**C**
. Cerrar el caso del problema reportado		**R**	**A**	**C**	**C**
Realizar resumen de la resolución que genera afirmativa una gestión correcta del problema reportado		**R**	**A**	**C**	**C**

Fuente: elaboración propia.

4.2.6 Verificar – MEA01 - ISO 27032. La aplicación de la norma ISO 27032 con apoyo de los procesos de MEA01 permitirá conocer la situación actual de la IES con referencia a sus políticas, lineamientos, procesos y procedimientos orientados a la adecuada gestión de los incidentes de seguridad de la información. Durante este proceso se realiza la correlación del cumplimiento de los controles establecidos para la gestión de incidentes de seguridad de la información, a continuación, se detallan el dominio 16:

Tabla 27. Actividades a realizar apoyadas en el Dominio A16 - ISO 27032

DOMINIO 16: GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras
16.1.1 Responsabilidades y procedimientos.

16.1.2 Reporte de eventos de seguridad de la información.
16.1.3 Reporte de debilidades de seguridad de la información.
16.1.4 Evaluación y decisión sobre eventos de seguridad de la información
16.1.5 Respuesta a incidentes de seguridad de la información
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recolección de evidencias

Fuente: elaboración propia.

4.2.7 ISO 27035

Para el correcto establecimiento del modelo dentro de la institución de educación superior nos basaremos en el enfoque previsto por la ISO 270035:2017, la cual divide su implementación en 5 fases que permiten el cumplimiento de los objetivos previstos, las cuales se detallan a continuación.

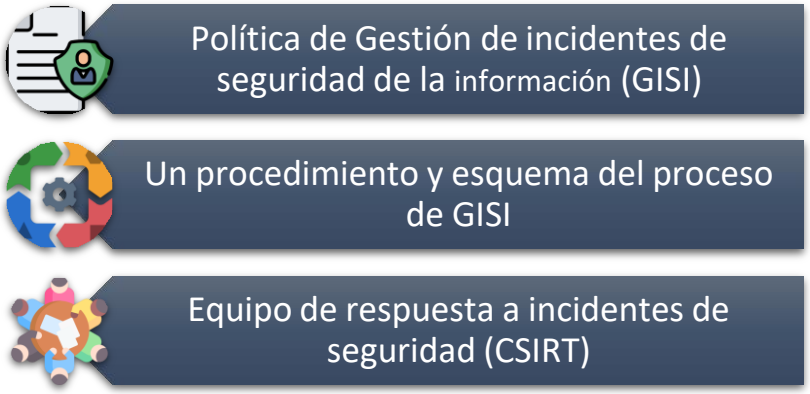
Figura 21. Fases gestión de incidentes

Fuente: elaboración propia.

Fase 1. Planeamiento y preparación

En esta fase se especifica la documentación para la adecuada gestión de las solicitudes e incidentes de seguridad de la información en la institución de educación superior, la norma define que se debe estructurar lo siguiente:

Figura 22. Planificación resolución de incidentes



Fuente: elaboración propia.

Política de Gestión de incidentes de seguridad de la información (GISI)

La política de GISI establece los requerimientos generales de la institución para la gestión de incidentes de seguridad de la información, con ella a borde se podrá prevenir y mitigar el impacto de los incidentes sobre los procesos y servicios de la institución.

La política establecida debe cumplir con los siguientes criterios:

ID	Nombre	Control	Directrices
1	Responsabilidades y procedimientos	Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Establecer las responsabilidades en la gestión de incidentes de seguridad digital. Definir el procedimiento de atención de incidentes de seguridad de la información. Dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados en la IES

			Realizar sensibilización a todos los colaboradores y terceros sobre incidentes de seguridad de la información.
2	Reporte de eventos de seguridad de la información	Informar sobre los eventos de seguridad de la información a través de los canales de gestión apropiados, tan pronto como sea posible	Reportar de forma inmediata de acuerdo con el procedimiento previsto los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.
3	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Evaluar los eventos de seguridad de la información y decidir si se van a clasificar	Evaluar cada evento o incidente de seguridad de la información presentado en la institución de educación superior, usando la escala de clasificación de eventos e incidentes de seguridad de la información con el fin de poder determinar clasificación y priorización. De acuerdo con el definido en el procedimiento previsto.

			Registrar los resultados de la evaluación y la decisión para referencia y verificación futuras (Lecciones aprendidas).
4	Respuesta a incidentes de seguridad de la información	Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	Dar respuesta a los incidentes de seguridad de la información que se presenten dentro de la institución de educación superior. La respuesta debe incluir lo siguiente: Recolectar evidencia lo más pronto posible después de que ocurra el incidente. Llevar a cabo análisis forense de seguridad de la información, según se requiera. Llevar el asunto a una instancia superior, según se requiera.

			Asegurarse de que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior. Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo. Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente. Escalar los incidentes a niveles superiores o control interno en caso de que sea requerido.
5	Aprendizaje obtenido de los incidentes de	Usar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la	Documentar todos los incidentes de seguridad de la información reportados en la IES.

	seguridad de la información	información para reducir la posibilidad o el impacto de incidentes futuros	Llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos en la IES. Por medio del aplicativo dispuesto para tal fin.
6	Recolección de evidencia	Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Tener en cuenta que los procedimientos para evidencia deben contener actividades tales como; identificación, recolección, adquisición y preservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos, por ejemplo, encendidos o apagados. Los procedimientos deben tener en cuenta: La cadena de custodia La seguridad de la evidencia La seguridad del personal Los roles y responsabilidades del personal involucrado La competencia del personal La documentación Las sesiones informativas.

Para el transporte de elementos, se debe llevar la cadena de custodia

El procedimiento debe definir como objetivo la implementación de los procesos para la correcta gestión de los incidentes de seguridad de la información, el alcance deberá estar limitado a los servicios derivados de los procesos que involucren software y hardware.

Para la implementación de este procedimiento la IES y como lo recomienda el modelo en su estructura inicial ya deberá contar con la fase 1 ejecutada, en donde se detalla mediante el marco de trabajo COBIT 2019 y el uso de los objetivos DSS02 y DSS03 que marcan los procesos correctos para la gestión de incidentes y la gestión de problemas.

En el **ANEXO 1** se detalla el formato que deberá usar la IES para el reporte de eventos de seguridad de la información.

En el **ANEXO 2** se detalla el formato que se deberá usar por la IES para el registro/bitácora de los eventos se seguridad de la información recibidos.

El adecuado establecimiento de un equipo de respuesta a incidentes de seguridad (CSIRT), en esta fase de determinan los requerimientos para establecer un equipo para el tratamiento de incidentes de seguridad de la información. Dentro de esos requerimientos se deben tener en cuenta lo siguiente, visión, misión, objetivos, alcance, servicios, roles, responsabilidades.

Fase 2. Detección e información

El propósito de esta fase es documentar toda la información relacionada con las vulnerabilidades, fallas, errores y/o problemas detectados en la fase anterior, con soluciones para mitigar las vulnerabilidades descubiertas, para lograr este objetivo se proponen dos herramientas, es importante especificar campos para administrar los eventos que ocurren. En esta fase de definen las actividades inherentes a la detección de eventos o anomalías que ocurran durante la ejecución de las actividades de los usuarios, tiene como responsabilidad el reporte de cualquier evento de seguridad que afecte negativamente la integridad, confidencialidad y/o disponibilidad de los elementos que competan a software y hardware de la institución.

Las actividades que se realizaran están contempladas en detalle a continuación:

- Recopilar información de los eventos de seguridad de la información para el debido registro a través de los medios definidos.
- Registro de los eventos de seguridad en la bitácora de eventos, incidentes y vulnerabilidades.
- Obtención de los datos sobre los eventos de seguridad de la información.

Las actividades mencionadas como apoyo, al grupo de trabajo cuando se presentan riesgos o amenazas durante el desarrollo de los procesos, les ayuda a analizar la situación, comparar el costo, el alcance del trabajo y el tiempo requerido para la solución de los mismos incidentes, que puede verse afectado; se definen según corresponda al incidente y se informan según sea necesario para realizar la gestión continua de los servicios de TI. Estos procesos están basados en el estándar COBIT 2019, como complemento, los cuales se deben implementar para cumplir con las actividades propuestas, teniendo en cuenta los objetivos de la empresa:

- Garantizar que los requisitos de todas las partes interesadas, incluidos los criterios de aceptación pertinentes, se consideren, capturen, prioricen y documenten de manera comprensible para todas

las partes interesadas, reconociendo que los requisitos pueden cambiar y volverse más detallados a medida que se desarrollan.

- Expresar las necesidades comerciales en términos de cómo se debe abordar la brecha entre las capacidades comerciales actuales y deseadas y cómo los usuarios interactuarán y utilizarán la solución.
- Especificar y priorizar los requisitos de información, funcionales y técnicos en función del diseño del cliente y los requisitos validados de las partes interesadas.
- Asegúrese de que los requisitos se alineen con las políticas y estándares comerciales, la arquitectura empresarial, los planes estratégicos y tácticos de I&T, los procesos comerciales y de TI internos y subcontratados, los requisitos de seguridad, los requisitos reglamentarios, la fuerza laboral de capacidades corporativas, la estructura organizacional, el caso comercial y la tecnología.
- Incorporar requisitos de control de la información en procesos comerciales, procesos automatizados y entornos de I&T para abordar los riesgos de la información y cumplir con leyes, reglamentos y contratos.
- Identificar las acciones requeridas para adquirir o desarrollar una solución basada en arquitectura empresarial.
- Considere el alcance, la fecha límite y/o las limitaciones presupuestarias.

Fase 3. Evaluación y decisión

Durante esta fase el responsable del proceso de gestión de incidentes, realiza la debida y correcta clasificación de los eventos o incidentes que se produzcan, para ello debe utilizar la política que se establezca en donde se detalle la categoría del incidente y la afectación o impacto

generado. Para realizar un buen trabajo en la implementación de esta etapa, de acuerdo a los lineamientos formulados en las etapas anteriores, se debe implementar correctamente la gestión de los siguientes procesos y subprocesos, enfocándonos en los lineamientos del estándar COBIT 2019, como complemento, hay una base para la buena práctica, de la siguiente manera:

- Definir e implementar métodos para permitir, restringir y/o revocar el acceso a las oficinas de la organización en función de las necesidades y roles dentro de la empresa.
- Definir estructuras y modelos para la clasificación de incidencias y solicitudes de servicio.
- Definir e implementar estándares y procedimientos para identificar y reportar problemas. Incluye categorización, categorización y priorización de temas.
- Identifique, documente y categorice las solicitudes de servicio y los incidentes, y priorícelos en función de la importancia comercial y los acuerdos de servicio.
- Investigar y diagnosticar problemas con la ayuda de expertos en la materia para evaluar y analizar su causa raíz.
- Seleccione el proceso apropiado para la solicitud y verifique que la solicitud de servicio cumpla con los criterios de solicitud definidos. Obtenga la aprobación (si es necesario) y cumpla con los requisitos.
- Identificar y documentar síntomas de incidentes, determinar posibles causas y asignar soluciones.
- Cree un registro de errores conocidos, documente las soluciones adecuadas e identifique las posibles soluciones.
- Mantener y ejecutar procedimientos operativos y tareas de manera confiable y consistente.
- Gestionar la operación de innovación y servicios técnicos subcontratados para mantener la seguridad de la información comercial y la confiabilidad en la prestación del servicio.
- Supervisar la infraestructura de I&T y los eventos relacionados.

- Mantener las medidas de protección frente a los factores ambientales. Instalar equipos y dispositivos especializados para monitorear y controlar el ambiente.
- Identificar e iniciar soluciones sostenibles a las causas fundamentales de los problemas. Si es necesario, envíe una solicitud de cambio para resolver los errores a través del proceso de gestión de cambios establecido.
- Verificar la resolución satisfactoria de incidentes y/o cumplir con las solicitudes de cierre de incidentes.
- Seguimiento, análisis y reporte de incidencias y solicitud de solicitudes de forma periódica.
- Asegurarse de que los afectados conozcan las medidas adoptadas y los planes establecidos para prevenir futuros accidentes.
- Implementar y mantener medidas preventivas, de detección y correctivas en toda la empresa para proteger los sistemas y la tecnología de la información del malware.
- Utilizar medidas de seguridad y procedimientos de gestión pertinentes para proteger la información a través de todos los métodos de conexión.
- Garantizar los derechos de acceso de todos los usuarios y coordinarlos para gestionar sus derechos de acceso en la empresa.
- Verifique las tendencias para informar la mejora continua.
- Documentar, aplicar y probar las soluciones finales o provisionales identificadas. Realice operaciones de recuperación para restaurar los servicios relacionados con I&T.

Fase 4. Respuesta

El equipo CSIRT durante esta fase define las actividades que debe realizar rápidamente para tratar el incidente, a continuación, se detallan las mínimas actividades que el equipo debería realizar.

- Tener en claro la respuesta inmediata para el incidente.
- Detallar y documentar las acciones de mitigación y controles según los resultados del evento.
- Avisar a las partes interesadas sobre el análisis de incidentes y posibles acciones para la contención y recuperación.
- En base al grado de afectación (sobre los activos) se tomarán las decisiones de escalamiento y pasar a la priorización del incidente, todo sin obviar las respuestas inmediatas.

Fase 5. Lecciones aprendidas

La ultima fase se ejecuta después de que el equipo de respuesta rápida determina con certeza que el incidente fue superado, este realiza un reporte final, en el cual se detallan las causas del incidente, las actividades realizadas y los resultados de la aplicación de las mismas.

Dentro del reporte que el equipo realiza deberá tener en cuenta si es necesario agregar cualesquiera de los siguientes enunciados:

- Realización de un análisis forense (si así lo considera el CSIRT).
- Evaluación de avances en la implementación de controles en los activos perjudicados.
- Reconocimiento y evaluación de los riesgos según el incidente presentado.
- Reconocimiento de las vulnerabilidades asociadas al activo y las lecciones aprendidas.
- Registrar los conocimientos o lecciones aprendidas de los ISI en la base de datos de conocimiento.
- Comunicación de los resultados las partes interesadas y dueños de procesos y activos afectados. La información compartida es confidencial según la clasificación de la política de seguridad.

4.2.8 Actuar – Cumplimiento del modelo

4.2.8.1 Administración del desempeño

Esta fase se define evaluando el desempeño del modelo producido en el proceso de TI, monitoreando cada actividad realizada brindando la gestión de la seguridad de la red, son muchas las tareas a evaluar, pero las más representativas que encontramos son:

Seguimiento y control de la cartera de proyectos.

- Gestión de la Continuidad del Servicio.
- Gestión de equipos de trabajo y proveedores.
- Gestión de la seguridad de la red.
- gestión de infraestructuras.
- Seguimiento del tratamiento del riesgo.

4.2.8.2 Mejora continua

Lo mejor es utilizar los niveles de madurez definidos en estos documentos, que están diseñados para evaluar la implementación y el desempeño de cada control definido para la gestión de la ciberseguridad dentro de una organización. Para ello, se recomienda seguir las siguientes instrucciones:

- Identificar y describir el estado actual de la ciberseguridad de la organización en términos de infraestructura, datos, procesos y programas.
- Describir los objetivos previstos de la ciberseguridad.
- Identificar y priorizar continuamente las oportunidades de mejora.
- Evaluar el progreso contra los objetivos establecidos.
- Comunicar los riesgos de ciberseguridad entre las partes interesadas internas y externas.

Estas actividades deben realizarse de manera regular y deben ir acompañadas del desarrollo de habilidades y competencias de los profesionales de TI, socialización de las estrategias implementadas, evaluación y refinamiento de los modelos de madurez propuestos, revisión de los estándares aplicables, planes de mejora, revisión de productos y servicios. y Evaluar. Servicios para la gestión de la ciberseguridad, así como de formación y certificación para particulares e instituciones.

4.3 Validación del modelo de gestión de ciberseguridad para resolver incidentes

Para validar la coherencia y la efectividad del modelo de gestión de ciberseguridad propuesto, como apoyo al cumplimiento de los componentes de seguridad y privacidad de la información en el marco de ciber delitos, se fundamentara en la validación por expertos. Siguiendo los criterios que han aplicado el método Delphi en sus investigaciones, donde establecen la secuencia metodológica a seguir, compuesta en tres fases fundamentales, como lo es la preparatoria, consulta y consenso. (Rodríguez & García, 2017)

Fase preparatoria:

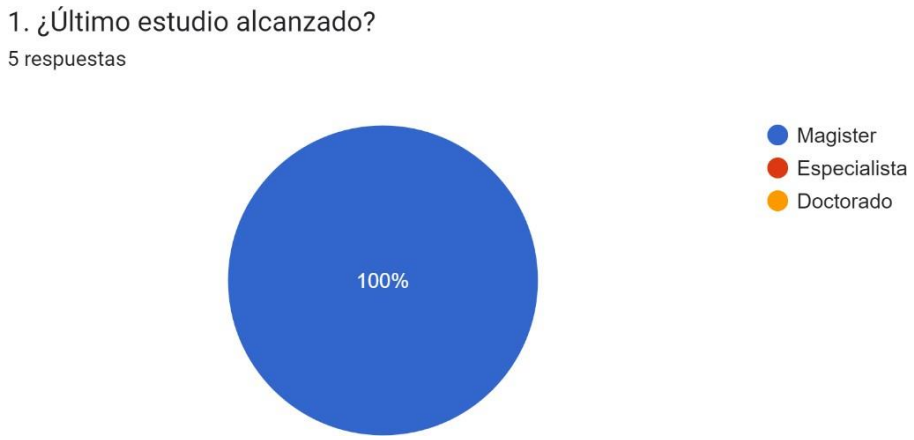
Selección de expertos: de acuerdo con el objetivo de la investigación, el método a desarrollar el Delphi, que en concordancia explica que la muestra se conforma por un grupo coordinador y un grupo expertos. (Blasco & López, 2010) El grupo coordinador se conformo a partir del director del proyecto a evaluar, Magister en gobierno en tecnologías de la información y la directora del programa de la Universidad.

Como criterio fundamental para realizar la selección del panel de expertos se seleccionó un grupo de profesionales con alguno de los siguientes perfiles:

- Experiencia en el área de implementación en procesos de MSPI en IES (Instituciones de educación superior)
- Docencia en TIC
- Estudios de maestría
- Experiencia profesional relacionada con las TIC

Información expertos

Figura 23. Estudios de expertos



Fuente: elaboración propia.

Figura 24. Cargos de expertos

Fuente: elaboración propia.

Figura 25. Años de experiencia laboral de expertos

Fuente: elaboración propia.

Del total de encuestados para la validación del modelo el 100% respondieron que su último titulo alcanzado es el de magister, destacándose el 80% de los mismos en el cargo de docentes dentro de la institución mientras que el 20% restante ocupa cargo administrativo. Asimismo, el 60% de los encuestados tiene alrededor de 2 a 4 años de experiencia en su cargo

mientras que el 20% restante resalta que esta entre los 1 y 2 años de experiencia, sumado al otro 20% que expresa que tiene ya de 4 a 6 años dentro de sus labores en la institución.

Elaboración del instrumento: se diseña un formulario que permite determinar la valoración del modelo propuesto. El cual para obtener una respuesta rápida y efectiva se decide realizar por medio del formulario de Google y enviar por correo electrónico.

Fase consulta: se realiza la primera versión del cuestionario y se sometió a valoración por parte del grupo de expertos, donde se realizan las acotaciones necesarias y se realiza la validación por parte de los seleccionados con la finalidad de obtener los criterios cuantitativos.

4.3.1 Análisis de resultados de validación de expertos

A continuación, se plantea la escala de Likert para poder obtener los resultados pertinentes de la validación de expertos como se muestra a continuación:

- MR: Muy relevante
- BR: bastante relevante
- R: relevante
- PR: Poco relevante
- NR: nada relevante

Pregunta	MR	BR	R	PR	NR
¿Considera relevante la aseveración de que la gestión de la ciberseguridad integra e institucionaliza las buenas prácticas para garantizar la seguridad y la privacidad de la información dentro de las IES (Instituciones de educación superior)?					

¿Considera que la adopción de un modelo de gestión de ciberseguridad para resolver incidentes, mejora la eficacia en los procesos dentro de las IES?
¿Comparte la idea de que las características particulares consideradas en el modelo de gestión de ciberseguridad; facilita a las IES cumplir con la implementación y gestión en los procesos de seguridad y privacidad de la información para mejorar la eficacia en su adopción?
¿Considera que el diseño del modelo de gestión de ciberseguridad para resolver incidentes en las IES, puede añadir valor y si se sigue e implementa facilita el cumplimiento de las buenas prácticas planteadas de acuerdo a los estándares escogidos?
¿Existe coherencia entre los elementos estructurales (Dominios, niveles, metas de TI) del modelo propuesto?
Existe claridad en el contenido de cada elemento del modelo
¿Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?

Fuente: elaboración propia.

Para lograr obtener los valores necesarios para la validación del modelo la estructura se base en el alfa de Cronbach, como se muestra a continuación:

Figura 26. Ecuación Alfa de cronbach

$$\infty = \frac{K}{K-1}\left[1 - \frac{\sum Vi}{Vt}\right]$$

K = número de profesionales expertos (5)

Vi = varianza que tienen los ítems

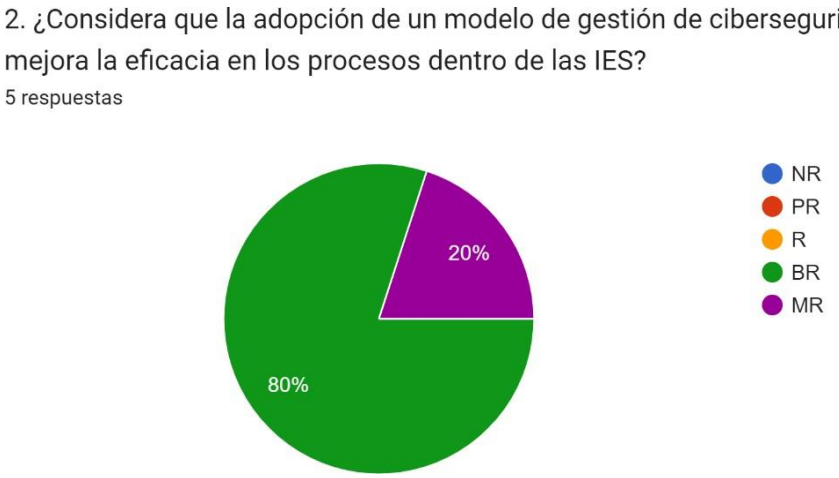
Vt = varianza que suman los ítems

∞ = Coeficiente de alfa de Cronbach

Figura 27. Respuesta 1 expertos

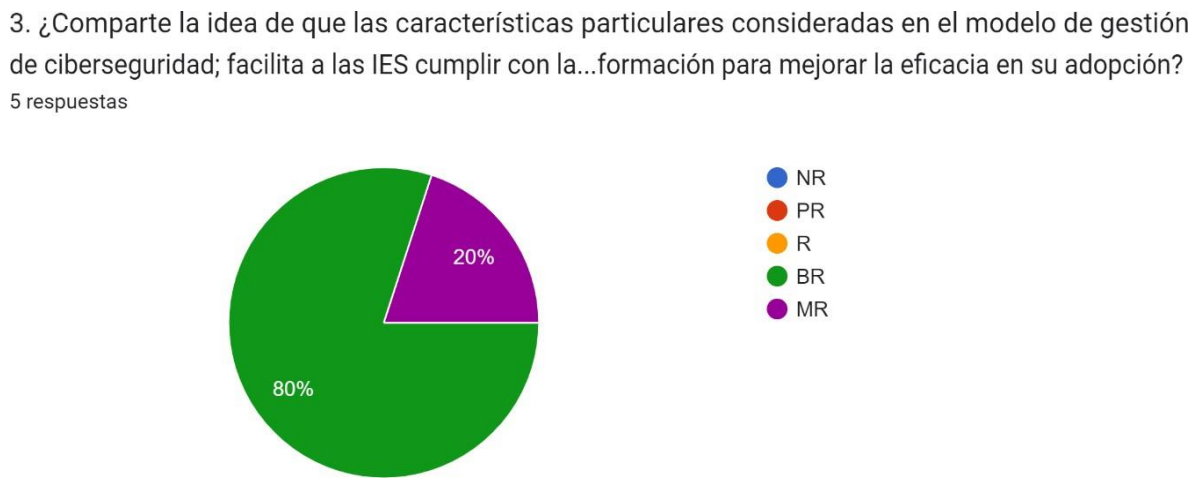
Fuente: elaboración propia.

Figura 28. Respuestas 2 expertos



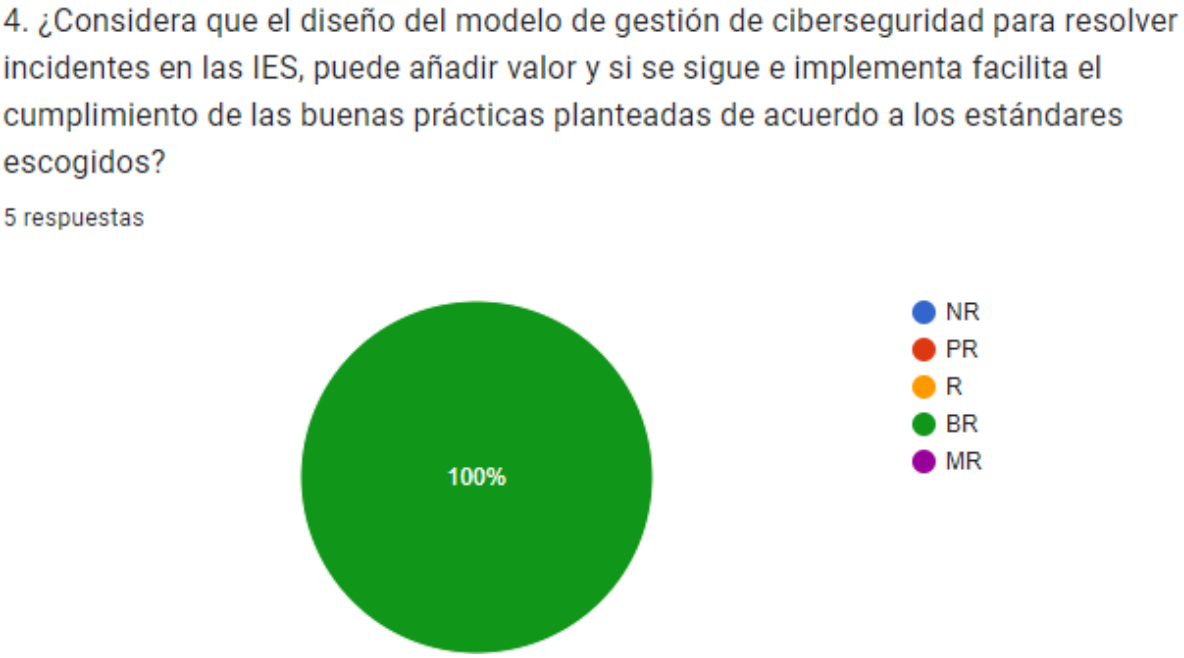
Fuente: elaboración propia.

Figura 29. Respuestas 3 expertos



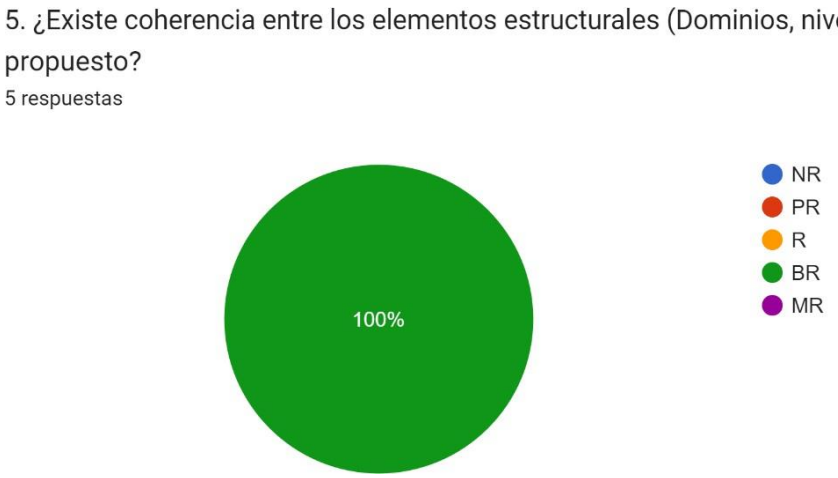
Fuente: elaboración propia.

Figura 30. Respuesta 4 expertos



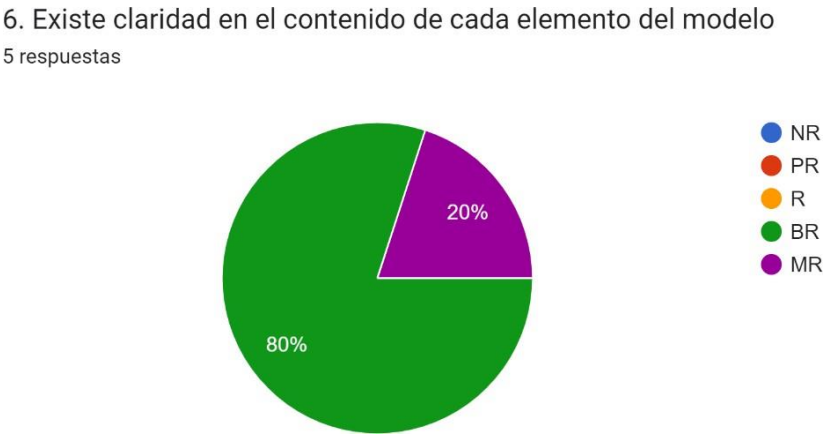
Fuente: elaboración propia.

Figura 31. Respuestas 5 expertos



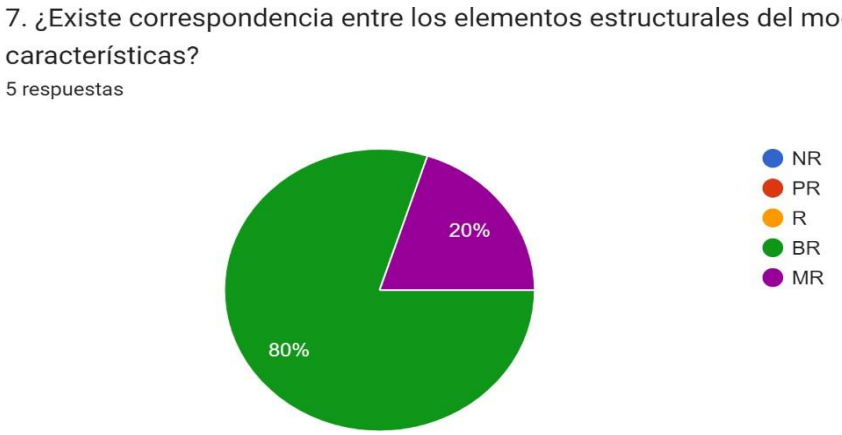
Fuente: elaboración propia.

Figura 32. Respuestas 6 expertos



Fuente: elaboración propia.

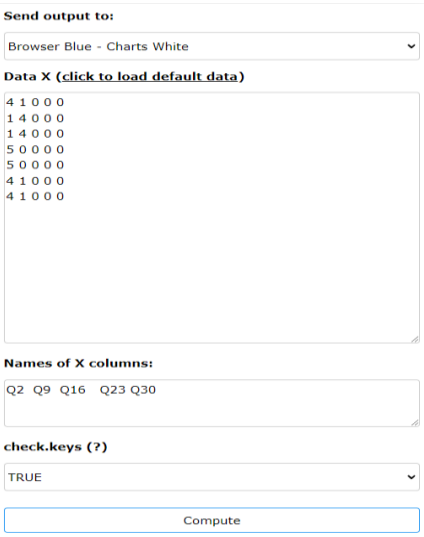
Figura 33. Respuestas 7 expertos



Fuente: elaboración propia.

Después de obtener los resultados de los expertos, procedemos a reemplazar cada respuesta en la ecuación impulsada por un software en línea llamado Cronbach Alpha, un software estadístico gratuito que se especializa en mostrar a los expertos los resultados obtenidos en las encuestas, en las que deben llenar la matriz, por lo que los puntos serán ser dado. A continuación, se muestra la obtención del puntaje para el modelo de propuesto.

Figura 34. Resultados encuestas



Fuente: tomado de http://www.wessa.net/rwasp_cronbach.wasp

Figura 35. Resultados validación

Cronbach Alpha and Related Statistics

Items	Cronbach Alpha	Std. Alpha	G6(smc)	Average R
All itmes	1	1	1	1
Q2 excluded	1	1	1	1
Q9 excluded	1	1	NA	NA
Q16 excluded	NA	NA	NA	NA
Q23 excluded	NA	NA	NA	NA
Q30 excluded	NA	NA	NA	NA

Fuente: tomado de http://www.wessa.net/rwasp_cronbach.wasp

4.3.2 Análisis de los resultados obtenidos

Con base en la opinión de expertos y herramientas validadas por Cronbach, los resultados obtenidos arrojaron resultados positivos, lo que indicó que todos los componentes del modelo fueron validados. Esto puede enfatizar que el modelo se puede usar para mejorar los procesos de ciberseguridad dentro de las IES (Instituciones de Educación Superior), al tiempo que enfatiza la adopción de estándares nuevos como lo son COBIT 2019, la norma ISO 27032 y la ISO 27035 que adoptan según sea necesario las actividades, metas y políticas, mostrando la adaptabilidad y la prominencia del modelo. Estos modelos son importantes para el posicionamiento y la innovación tecnológica que deben tener las IES, ya que brindan el posicionamiento necesario para orientar y/o gestionar el conocimiento desde una perspectiva holística y segura.

Conclusiones

Luego de culminado el desarrollo del trabajo de grado se puede considerar que se han logrado los objetivos propuestos presentados inicialmente, se ha cumplido con el propósito de la investigación, se ha realizado el diagnóstico con el fin de disminuir el riesgo de ciberataques. y garantizar el cumplimiento del proceso. La capacidad inicial para determinar el estado actual del riesgo presentado frente al nivel de riesgo definido por la organización permite a la alta dirección ver este riesgo cibernético, al que a menudo se le presta poca atención en la organización, su nombre comercial y mandato. proporcionando servicios técnicos, pero contribuye a sus objetivos de tecnología de la información.

A medida que se desarrollaron los objetivos propuestos, se realizó una caracterización para estructurar los riesgos que pudieran presentarse dentro de la institución, permitiendo establecer un nivel crítico para cada riesgo con la ayuda de un modelo de madurez, permitiendo ver el efecto del análisis que se había realizado. realizado, para cada riesgo emergente de acuerdo con los criterios definidos Se priorizan los riesgos y se identifican métodos para diseñar y mantener procesos adecuados de gestión de acceso a los recursos tecnológicos de la agencia.

Finalmente, se valida mediante validación de expertos el modelo de gestión de ciberseguridad que soporta la resolución de incidentes, ya que permite determinar si el modelo de gestión de ciberseguridad incorpora procesos óptimos en los que interactúa información que protege la información dentro de las instituciones educativas de educación superior. La implementación del modelo se basa en la creación de lineamientos de política basados en buenas prácticas, lo que redunda en la reducción de incidentes que puedan comprometer los servicios digitales de una institución.

Recomendaciones

- Se recomienda que el equipo de TI en cabeza por la alta gerencia de la Institución de educación superior que desee adoptar el modelo planteado tome las consideraciones indicadas en esta investigación en búsqueda de la sinergia de las buenas prácticas y estándares para la correcta protección de la información y demás procesos mencionados.

- Se recomienda que las instituciones de educación superior realicen una revisión de los riesgos y el correcto funcionamiento de sus procesos orientados a la gestión de incidentes de seguridad informática, en búsqueda de una mejora continua, así como la ejecución periódicamente de auditorias de mayor profundidad a través de las normas y estándares aquí planteados.

- Posiblemente en futuras investigaciones a este modelo le sean agregados elementos y estándares que faciliten agregar valor al mismo, por lo tanto se recomienda que otras instituciones adopten el modelo ya que cumplen con objetivos similares, lo anterior permitirá crear y validar nuevos análisis de datos que ayuden a un mayor crecimiento de las técnicas que dan frente a los diferentes incidentes, de igual manera de lo mencionado anteriormente se hace necesario una constante actualización del modelo.

Referencias

Barbosa Fernández, M. (2020). Modelo de ciberseguridad dirigido a entidades financieras, alineado a marcos de referencia de gestión y gobierno de TI. *Universidad Francisco de Paula Santander - Ocaña*, 1-120. Obtenido de http://repositorio.ufpso.edu.co/bitstream/123456789/2259/1/34237.pdf

Biddle, S. (21 de Diciembre de 2017). *Instituciones de educación superior: blanco de ciberataques en el mundo digital de hoy*. Obtenido de ebizLatam.com: http://www.ebizlatam.com/instituciones-educacion-superior-blanco-ciberataques-mundo-digital-hoy/

Congreso de la República. (2009). Ley 1273 de 2009. 1-15.

Congreso de la República. (2012). Ley 1581 de 2012. 1 - 12.

Congreso de la República. (2014). Ley 1712 de 2014. 1-13. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=56882

Congreso de la República. (2022). Decreto 338 de 2022. 1 - 10.

Díaz Ramírez, M., Coronado Becerra, W., & Gómez López , F. (2021). Diseño plan de respuesta a incidente de ciberseguridad para la infraestructura crítica cibernética del sector eléctrico Colombiano. *Universidad del Bosque*, 1-116. Obtenido de https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/7499/D%C3%ADaz_Ram%C3%ADrez_Milton_Fernando_2021.pdf?sequence=1&isAllowed=y

elEconomista. (01 de Octubre de 2022). *El 60% de las instituciones educativas han sufrido un ataque de ransomware*. Obtenido de elEconomista.es: https://www.eleconomista.es/ecoaula/noticias/11926865/09/22/El-60-de-las-instituciones-educativas-han-sufrido-un-ataque-de-ransomware.html

Gómez Prada, C., González Calderón, C., Landinez Duarte, I., & Espinosa Carrillo, J. (2019). Modelo de Ciberseguridad para la empresa Space Cargo (SPC) Colombia. *Fundación Universitaria Unipanamericana - Compensar*, 1-52. Obtenido de https://repositoriocrai.ucompensar.edu.co/bitstream/handle/compensar/2288/Modelo%20de%20Ciberseguridad%20para%20la%20empresa%20Spac_Grupo%20Investigacin%20I.pdf?sequence=1&isAllowed=y

Manjarres, S. (07 de Octubre de 2022). *Brechas de datos: la principal amenaza para las universidades*. Obtenido de WatchGuard: https://www.watchguard.com/es/wgrd-news/blog/brechas-de-datos-la-principal-amenaza-para-las-universidades

Molina Oviedo, A. (2020). Modelo de gobierno y gestión de riesgos TI para las Universidades públicas de Colombia: Caso de Estudio Universidad Popular del Cesar. *Fundación Universidad del Norte*, 1-115.

Palafox Pascual, L. (2019). NUTRIA: "Una metodología de Ciberseguridad para pymes en entornos industriales". *Universidad Internacional de la Rioja*, 1-116. Obtenido de https://reunir.unir.net/bitstream/handle/123456789/9422/Palafox%20Pascual%2C%20Lorena.pdf?sequence=1&isAllowed=y

Panche Abril, L., Gutierrez Rojas, V., & Ardila Jiménez , O. (2022). Metodología para la evaluación de madurez en gestión de incidentes de Ciberseguridad. *Pontificia Universidad Javeriana*, 1-80.

PORTAFOLIO. (31 de Agosto de 2022). *El 73% de las empresas en el mundo ha sufrido ciberataques*. Obtenido de PORTAFOLIO: https://www.portafolio.co/economia/finanzas/ciberseguridad-el-73-de-las-empresas-en-el-mundo-ha-sufrido-ciberataques-570387

Robayo Villarroel, H. (2022). Modelo de mejora del estado de la ciberseguridad en la gobernación de Tungurahua. *Pontificia Universidad Católica del Ecuador*, 1-130.

Rodríguez Castro, J. (2019). Modelo de gestión de riesgos de tecnologías de la información como apoyo en la continuidad del negocio en una empresa que brinda software como servicio. *Universidad Católica Santo Toribio de Mogrovejo*, 1-226. Obtenido de https://tesis.usat.edu.pe/bitstream/20.500.12423/2420/1/TM_Rodr%C3%ADguezCastroJorge.pdf

Santolaria Mairal, M. (2022). Desarrollo de una metodología para la gestión de incidentes de ciberseguridad en una organización. *Universitat Oberta de Catalunya*, 1-6. Obtenido de https://openaccess.uoc.edu/bitstream/10609/145994/7/osantolariaTFM0622memoria.pdf

Troya. (24 de Enero de 2023). *La necesidad de una educación en ciberseguridad actualizada para el nuevo mundo digitalizado*. Obtenido de Troya Noticias: https://troyanoticias.com/2023/01/24/la-necesidad-de-una-educacion-en-ciberseguridad-actualizada-para-el-nuevo-mundo-digitalizado/

Vargas Ramos, G. (2020). Modelo de gestión de incidentes informáticos para equipos de respuesta - CSIRT. *Universidad Mayor de San Andrés*, 1-4.

Verinzon. (07 de Marzo de 2022). *Demanda de expertos en ciberseguridad contnúa en aumento*. Obtenido de Carreras Universitarias de Colombia: https://carrerasuniversitarias.com.co/noticias/demanda-de-expertos-en-ciberseguridad-continua-en-aumento

Vilcarromero Zubaite, L., & Vilchez Linares, E. (2018). Propuesta de implementacion de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. *Universidad Peruana de Ciencias Aplicadas*, 1-107.

Apéndies

Apéndice A. Matriz de operacionalización de variable

Tabla 28. Matriz de operacionalización de variables

Propósito	Conceptualización	Dimensiones	Subdimensiones	Indicadores
Caracterizar los principales riesgos de ciberseguridad existentes para identificar modelos que puedan ayudar a minimizar los incidentes dentro de la empresa.	Gestión de Incidentes	Catalizador: Servicios, Infraestructura y Aplicaciones	Métricas para la consecución de Objetivos Métricas para la ejecución de buenas prácticas	Partes interesadas Objetivos o metas Ciclo de vida Buenas prácticas
		BAI02 Gestionar la definición de requisitos.	BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio. BAI02.02 Realizar un estudio de viabilidad y propones	Metas de TI Metas de proceso Métricas RACI Actividades

Gestión de riesgos de TI		soluciones alternativas. BAI02.03 Gestionar los requerimientos. BAI02.04 Obtener la aprobación de los requerimientos y soluciones.	
	MEA01 Supervisar, evaluar y valorar rendimiento y Conformidad	MEA01.02 Objetivos de seguimiento MEA01.04 Informes de desempeño MEA01.05 Acciones y asignaciones correctivas.	Metas de TI Metas de proceso Métricas RACI Actividades
	DSS	DSS01 Gestionar las operaciones	Metas de TI Metas de proceso Métricas

			DSS02 Gestionar las peticiones y los incidentes de servicio DSS03 Gestionar los problemas DSS04 Gestionar la continuidad DSS05 Gestionar los Servicios de seguridad DSS06 Gestionar los controles de los procesos del Negocio	RACI Actividades
Instituciones de educación superior	Universidades	Procesos		Actividades Resultados Indicadores

Fuentes: elaboración propia.

Apéndice B. Formato de reporte de incidentes

Tabla 29. Formato reporte de incidentes

REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	
FECHA Y HORA REPORTE DE INCIDENTE	
LUGAR DEL INCIDENTE	
DETALLES DE PERSONA QUE REPORTA/IDENTIFICA INCIDENTE	

DESCRIPCION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION:			
¿Qué Sucedió?:			
¿Cómo Sucedió?:			
¿Por qué Sucedió?:			
Consideraciones Iniciales sobre componente(s) / Activo(s) de información afectados?:			
¿Impactos adversos para la Entidad?:	Si:	No:	Cual:
¿Se identifica Vulnerabilidad alguna?:	Si:	No:	Cual:
¿Se identifica responsable del Incidente?:	Si:	No:	Cual:
ESTADO DEL INCIDENTE	Sucediendo____ Sucedió____ Sucede nuevamente ____		

CATEGORIA DEL INCIDENTE SE SEGURIDAD DE INFORMACION:				
¿Incidente de Seguridad de la Información Real?			**Incidente de Seg. ¿Información Sospechado?**	
Desastre natural:				
Terremoto			**Inundación**	
Descarga Electromagnética			**¿Otro? Especifique_____**	
Conflicto social:				
Disturbio			**Ataque Terrorista**	
Guerra			**¿Otro? Especifique:**	
Daño físico:				
Incendio			**Agua**	
Electrostática			**Ambiente Nefasto (Contaminación, polvo, corrosión)**	
Destrucción de Equipo			**Destrucción de Medios**	
Robo de Equipos			**Pérdida de Medios**	
Alteración de Equipo			**Alteración de Medios**	
¿Otro? Especifique_____ _____			**¿Otro? Especifique_____ _____**	
Falla en la infraestructura:				
Fallas en la Alimentación Eléctrica			**Falles en las Redes**	
Fallas en el Aire Acondicionado			**Fallas en el suministro de Agua**	
¿Otro? Especifique_____ _____			**¿Otro? Especifique_____ _____**	
Falla técnica:				
Falla en el Hardware			**Mal Funcionamiento del Software**	
Sobrecarga (saturación de capacidad de los sistemas)			**Violación de Mantenibilidad**	

¿Otro? Especifique_____			**¿Otro? Especifique_____**	
Malware:				
Gusano de Red			**Troyano**	
Botnet			**Ataques combinados**	
Página WEB con código malicioso incrustado			**Sitio de alojamiento con código malicioso**	
¿Otro? Especifique_____ _____			**¿Otro? Especifique_____ _____**	
Ataque técnico:				
Escaneo de Redes			**Aprovechamiento de Vulnerabilidades**	
Aprovechamiento de Puertas traseras			**Intentos de acceso**	
Interferencia			**Denegación de Servicio**	
¿Otro? Especifique_____			**¿Otro? Especifique_____**	
Violación de reglas:				
Uso no autorizado de recursos			**Violación a los Derechos de Autor**	
¿Otro? Especifique_____ _____			**¿Otro? Especifique_____ _____**	
Puesta en peligro de las funciones:				
Abuso de Derechos			**Falsificación de Derechos, denegación de acciones**	
Operaciones Incorrectas			**Violación de la Disponibilidad del Personal**	
¿Otro? Especifique_____ _____			**¿Otro? Especifique_____ _____**	
Puesta en peligro de la información:				

Interceptación			**Espionaje**	
Chuzada de Teléfonos			**Divulgación**	
Enmascaramiento			**Ingeniería Social**	
Phishing de Redes			**Robo de Datos**	
Pérdida de Datos			**Alteración de Datos**	
Error de Datos			**Análisis de Flujo de Datos**	
Detección de posición			**¿Otro?** **Especifique**_____	
Contenidos peligrosos:				
Contenido Ilegal			**Contenido que provoca pánico**	
Contenido Malicioso			**Contenido Abusivo**	
¿Otro? **Especifique**_____ _____			**¿Otro?** **Especifique**_____ _____	
DETALLE DE LA SOLUCION DEL INCIDENTE DE SEGURIDAD DE LA INFORMACION:				
Fecha y Hora de la investigación del incidente:				
Nombre(s) del(los) investigador(es) del incidente:				
Fecha y Hora de la Finalización del incidente				
Fecha y Hora de la Finalización del impacto				
Descripción de las acciones tomadas para resolver el incidente de SI:				
Descripción de las acciones planeadas para resolver el incidente de SI:				
Acciones pendientes para resolver el incidente de SI:				

Conclusiones:	
Lecciones aprendidas del incidente de SI:	
ELABORO	**REVISO**
Nombre:	**Nombre:**
Área:	**Área:**
Rol:	**Rol:**
APROBO	
Nombre:	**Área:**
Cargo:	**Fecha:**

Fuente: elaboración propia.

Apéndice C. Planilla de incidentes

Tabla 30. Planilla de incidentes

	A	B	C	D	E	F	G
1	PLANILLA DE REGISTRO DE EVENTOS / INCIDENTES						
2	**ID**	**DESCRIPCIÓN DEL EVENTO**	**TIPO**	**FECHA**	**HORA**	**DESCRIPCIÓN**	**ESTADO**
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							

Fuente: elaboración propia.