DISEÑO DE UN MODELO PARA LA GESTIÓN DE INCIDENTES EN CIBERSEGURIDAD BASADO EN LA NORMA ISO27002:2013 PARA LA EMPRESA PROYECTOS DE INVERSIÓN VIAL ANDINO S.A.S

GINA ALEJANDRA ARENIZ ARÉVALO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

DISEÑO DE UN MODELO PARA LA GESTIÓN DE INCIDENTES EN CIBERSEGURIDAD BASADO EN LA NORMA ISO27002:2013 PARA LA EMPRESA PROYECTOS DE INVERSIÓN VIAL ANDINO S.A.S

GINA ALEJANDRA ARENIZ ARÉVALO

Proyecto de Grado – Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

EDUARD MANTILLA TORRES
Asesor de trabajo de grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Villavicencio., Fecha sustentación

DEDICATORIA

Este trabajo se lo dedico primeramente a Dios que brinda día a día oportunidades de salir adelante, a mi hijo y a mis padres que con su amor y apoyo puedo lograr todo lo que me propongo.

AGRADECIMIENTOS

Agradezco a todas las personas que me colaboran día a día con aprendizajes, orientaciones y enseñanzas para mi carrera profesional, a los directivos y docentes de la Universidad nacional abierta y a distancia por su dedicación y compromiso con todos los que con mucho entusiasmo y esfuerzos logramos sacar un título académico adelante.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ATAQUE INFORMÁTICO: Es una técnica por el cual un sujeto, utilizando recursos tecnológicos, quiere tomar el control o inhabilitar cualquier tipo de sistema informático.

AMENAZA: Todo suceso o alteración capaz de atentar contra los activos de la información.

VULNERABILIDAD: Son todos los puntos que necesitan refuerzo dentro de la empresa, ya que están expuestos a que personal no autorizado tenga acceso y comprometa la rectitud de un proceso, que el recurso no se encuentre disponible o que se encuentre a disposición de terceros la información.

VULNERABILIDADES EN LOS SISTEMAS DE INFORMACIÓN: Es la consecuencia de errores en la puesta en marcha del sistema, también puede ser resultado de limitaciones en la infraestructura tecnológica.

CIBERSEGURIDAD: Conjunto de acciones preventivas el cual tienen como finalidad negar el acceso a personal no autorizado.

MALWARE: Tipo de código malicioso utilizado para infiltrarse dentro de un ordenador y dañar los activos de la información.

VIRUS: Es un malware el cual su función es perturbar todo el trabajo de los equipos de cómputo, sin el consentimiento de la persona encargada.

MODELO: Guía de buenas prácticas aplicables en una empresa, enfocada en las partes más importantes de sus procesos.

ACTIVO DE LA INFORMACIÓN: Todo tipo de información o activo dentro de la empresa que esté concerniente con el procedimiento de datos y que posea cuantía dentro de la empresa.

CONFIDENCIALIDAD: Garantiza la seguridad de la información o cualquier tipo de dato, que tengan almacenado dentro de la empresa.

DISPONIBILIDAD: Capacidad para lograr encontrar la información necesaria el cual sea requerida por un proceso, o bien en un intervalo de tiempo determinado.

AMENAZA: Es la posibilidad de dicho acontecimiento potencial o adverso puntual en innegable proceso en un intervalo de tiempo determinado.

ANÁLISIS DE RIESGO: Percibe toda la caracterización de los datos de la empresa, exponiendo las vulnerabilidades, riesgos y/o debilidades a las que se están expuestas.

ISO 27032:2012: En encarga de resguardar la privacidad, rectitud y que los recursos se encuentren disponibles en la nube.

ISO 27002:2013: modelo para el control en la privacidad de los datos, convirtiéndose en una guía de buenas prácticas a implementar.

RESUMEN

El desarrollo propuesto, presentará una estrategia para la gestión de incidentes de ciberseguridad basada en la norma ISO27002 para la empresa Proyectos de Inversiones Vial Andino S.A.S, luego de analizar y estudiar una posible vulnerabilidad y amenaza a la que es exhibida los servicios básicos tecnológicos de la organización, con el fin de brindar una serie de recomendaciones, prevenciones y acciones referente a ataques de cibernéticos que pueda presentarse en el desarrollo de su labor. Para lograr alcanzar los objetivos propuestos, primero realizará un análisis del inventario de activos, luego las amenazas a las que pueden estar expuestas estos equipos, se estudiaran los ataques cibernéticos que se presentan con más frecuencia, determinando que daños causan y cuáles son las posibles acciones a realizar después de que ocurra un incidente de ciberseguridad.

Así mismo se analizarán la norma ISO27002 para determinar cuáles podrían ser aplicables dentro del desarrollo del trabajo, luego se realizará un estudio para determinar el estado actual de ciberseguridad que presenta la organización, así como los recursos de infraestructura con los que cuenta, con esto se buscará orientar la metodología propuesta para que se adapte al modelo de negocio y a los recursos presentes. Una vez hecho el análisis y estudio del estado de ciberseguridad dentro de la organización se procederá a implementar el modelo de aseguramiento de ciberseguridad que sirva como apoyo dentro del proceso de gestión de seguridad.

Palabras claves: Ataques cibernéticos, políticas de ciberseguridad, riesgos inherentes, gestión del riesgo, incidentes informáticos.

ABSTRACT

The proposed development will present a strategy for the management of cybersecurity incidents based on the ISO27002 standard for the company Proyectos de Inversiones Vial Andino S.A.S, after analyzing and studying a possible vulnerability and threat to which the basic technological services of the company are exhibited. organization, in order to provide a series of recommendations, preventions and actions regarding cyber-attacks that may arise in the development of its work. In order to achieve the proposed objectives, it will first carry out an analysis of the inventory of assets, then the threats to which these computers may be exposed, the cyber-attacks that occur most frequently will be studied, determining what damage they cause and what are the possible actions. to perform after a cybersecurity incident occurs.

Likewise, the ISO27002 standard will be analyzed to determine which ones could be applicable within the development of the work, then a study will be carried out to determine the current state of cybersecurity presented by the organization, as well as the infrastructure resources it has, with this will seek to guide the proposed methodology so that it adapts to the business model and the resources present. Once the analysis and study of the state of cybersecurity within the organization has been carried out, the cybersecurity assurance model will be implemented to serve as support within the security management process.

Keywords: Cyber-attacks, cybersecurity policies, inherent risks, risk management, computer incidents.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Los avances tecnológicos han tenido un gran impacto, presentado durante el último año con el auge de la tecnología y los cambios a los que se ha tenido que someter toda la humanidad por el covid-19, ha generado que se adopten nuevos modelos de negocio como la adaptación de empleos remotos para mitigar la propagación de la enfermedad, presentando retos a los administradores del área de tecnologías de la información de las organizaciones para adaptarse de manera rápida y confiable a la nueva modalidad, sin que esta adaptación genere interrupciones en las operaciones del negocio, el objetivo es solucionar cualquier inconveniente de conectividad y disponibilidad de los recursos informáticos como por ejemplo, los empleados que se adaptan a trabajos remotos desde sus hogares, puedan contar con la información, dispositivos, aplicaciones, accesos a servicios y demás, quedando así expuestas muchas vulnerabilidades cibernéticas con las que antes no se contaban o no se tenían previstas, aumentando riesgos al no tener el mayor control de todos los dispositivos y puestos de trabajos, redes domésticas que se deberán configurar para dar acceso a las redes internas de la organización, accesos a servidores desde lugares remotos, exponiendo puertas de entradas y controles de acceso que puede permitir el ingreso de atacantes y software malicioso a los sistemas informáticos de la organización.

Hace poco tiempo, la organización Proyectos de Inversiones Vial Andino, se vio afectada por un ataque tipo ***ransonware*** el cual no pudo ser detectado y mitigado , el evento produjo perdidas de información significativas, ocasionalmente se detectan riesgos cibernéticos y ataques informáticos que pretenden acceder al sistema para ocasionar robos o daños de información, con el modelo presentado, se espera que dentro de la organización se implementen medidas de seguridad informáticas que sirvan de apoyo dentro del SGSI de la empresa. El Anexo A16 “gestión de incidentes de la seguridad de la información, según la norma ISO 27002”, el cual se viene desarrollando dentro de la organización durante el año 2021, con el fin de optimizar la ciberseguridad de toda la infraestructura informática.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo la implementación de un modelo para la gestión de incidentes de ciberseguridad permitiría a la empresa proyectos de inversión vial andino S.A.S, reducir las amenazas de los delitos informáticos?

2. JUSTIFICACIÓN

Cualquier organización que maneje tecnologías y sistemas de información, está expuesta a riesgos y ataques cibernéticos que puedan poner en jaque su buen funcionamiento, para proteger la información se deben poner en práctica reglas, normas, leyes, protocolos, políticas y demás que contribuyan a gestionar la ciberseguridad con el fin de proteger los sistemas e infraestructuras informacionales, optimizando estos recursos que aportan crecimiento y son base fundamental para el desarrollo de las estrategias organizacionales.

En la actualidad se ha visto un gran aumento en los ataques cibernéticos, a medida que fue avanzando la pandemia COVID-19, en el cual se hace importante realizar un proyecto que busque desarrollar un modelo para la orientación y guía sobre vulnerabilidades, riesgos y ataques cibernéticos a los que podría estar expuesta la organización Proyectos de Inversiones Vial Andino, y qué medidas de mitigación y prevención se pueden implementar, analizando la situación actual y los recursos informáticos con los que cuentan actualmente, para determinar así un modelo de aseguramiento cibernético que se adapte al modelo de negocio y contribuya al Área de Sistemas y telecomunicaciones con datos relevantes a tener en cuenta para robustecer la gestión de ciberseguridad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un modelo para la gestión de incidentes en ciberseguridad basado en la norma ISO 27002:2013 para la empresa proyectos de inversión vial andino S.A.S

3.2 OBJETIVOS ESPECÍFICOS

- Examinar el estado actual de los riesgos inherentes en la empresa proyectos de inversión andino S.A.S, teniendo en cuenta el dominio A16 de la norma ISO 27002:2013.

- Analizar los principales riesgos de ciberseguridad existentes para lograr determinar un modelo que contribuya a minimizar incidentes dentro de la empresa.

- Establecer un modelo para la gestión de incidentes que aporte a la organización fundamentos para el desarrollo del SGSI empresarial.

4. MARCO REFERENCIAL

4.1 MARCO CONTEXTUAL

4.1.1 Historia. Proyectos de Inversión Vial Andino S.A.S. es un consorcio constituido el 14 de marzo del 2016, el consorcio integrado por sociedades suscritas Episol y Epiandes es el consorcio seleccionado por la sociedad concesionaria vial andino SAS, para ejecutar las obligaciones de construcción previstas en contrato de concesión bajo el esquema de app N° 005 del 2015, celebrado ante la Agencia Nacional de Infraestructura ANI y la Sociedad Concesionaria Vial Andina S.A.S.

4.1.2 Misión. Proyectos de Inversión Vial Andino S.A.S., ejecutara el contrato de construcción cov-010-2016 del 18/03/2016 suscrito con Coviandina S.A.S, con el fin de proveer a nuestros clientes, usuarios y comunidad soluciones para garantizar obras duraderas, con criterios técnicos vigentes, altos estándares de calidad e innovación tecnológica, comprometidos con el medio ambiente en colaboración con la comunidad, trabajando con responsabilidad social y brindando a nuestros colaboradores un lugar de trabajo seguro y saludable en condiciones agradables, para su motivación y satisfacción laboral y personal.

4.1.3. Visión. Proyectos de Inversión Vial Andino S.A.S., en el año 2022 entregará la solución vial Chirajara – fundadores, cumpliendo con las especificaciones técnicas, tecnológicas, administrativas y económicas, habiendo generado un impacto positivo en lo social, ambiental, seguridad y salud en el trabajo a través de nuestros procesos, operación y mejoramiento continuo, superando las expectativas contractuales y de nuestros clientes.

4.2 MARCO CONCEPTUAL

4.2.1 Modelo de ciberseguridad. Dentro de los marcos, estándares, leyes y normativas nacionales e internacionales existentes, como: el Control Objectives for Information Systems and Related Tecnology (COBIT)1, el Marco de Ciberseguridad2 que propone un modelo de ciberseguridad; el Modelo de

[1] RITEGNO, Eduardo O. “COBIT2019”. {En línea}. 2018 {3 de junio del 2021} disponible en: {https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf}

[2] NATIONAL INSTITUTE OF ESTÁNDARES AND TECHNOLOGY (NITS). Marco de ciberseguridad. NIST. Nuevo en Framework. {En línea} 2018 {3 de junio del 2021} disponible en {https://www.nist.gov/cyberframework/new-framework}

Seguridad y Privacidad de la Información (MSPI)3 y la norma internacional ISO/IEC 270324, se trazan una cadena de pasos y representaciones a tener en cuenta cuando se requiera implementar un modelo de ciberseguridad, estos controles y lineamientos han sido estudiados y experimentados por organizaciones en el exterior como a nivel local, mostrando resultados favorables para la protección de los datos que se exponen en la red.

De cada uno de estos estándares, según el caso propuesto, se obtendrán las recomendaciones y controles aplicables al modelo de negocio y a la a los activos de la información dentro de la organización Proyectos de Inversión Vial Andino S.A.S.

4.2.2 Riesgos en la ciberseguridad. Describe las consecuencias futuras que se pueden generar a partir del funcionamiento de las actividades de los sistemas de información. “El cual tiene la posibilidad de que ocurra en el funcionamiento de una infraestructura tecnológica, cuando los activos de información son lo que más se valora dentro de la empresa, generando daño en un activo de la información"[5].

4.2.3 Vulnerabilidades en los sistemas de información. Es la debilidad que se presenta dentro de las empresas, afectando las estructuras físicas y/o activos de la información, el cual se refiere a los riesgos en los que se pueden ver expuestos los recursos tecnológicos afectando los procesos que se están realizando dentro de la organización. Todo esto lleva a que cada uno de los activos por lo menos podría tener una vulnerabilidad el cual pondría en riesgo a la empresa y podría ser aprovechada por una amenaza.[6]

4.2.4 Confidencialidad. Hace referencia al hecho de que la información sensible de la empresa esté disponible solo para el personal responsable y capacitado previamente para su manejo, teniendo consigo los permisos ya sean de gerencia o de los altos mandos sobre ella. Con el avance en el uso de las tecnologías, los

3 REPÚBLICA DE COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC Modelo de Seguridad y Privacidad de la Información MSPI. {En línea} 2013 {3 de junio del 2021} disponible en: {https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/}.

4 ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity. {En línea} 2012 {3 de junio del 2021} disponible en: {https://www.iso.org/standard/44375.html}.

5 RAMOS GALLARDO, Arelis Taimati, ARANGO HURTADO, Erika María y AMADOR TINOCO, Antonio. Riesgos en ciberseguridad y sus efectos sobre la transformación digital en la nueva normalidad, según las empresas operadoras de seguridad. Bogotá, D. C., 2020, 35p. Trabajo de grado (especialización en Administración de Empresas Virtual). Universidad EAN, Facultad de Administración, Finanzas y Ciencias Económicas.

6 *Ibíd.,* p. 11.

permisos para el manejo de información han innovado, el cual ya estos van establecidos desde el control parental de cada usuario y su respectiva cuenta para el manejo de información.[7]

4.2.5 Disponibilidad. Es la propiedad de ser accesible a un activo de la información y utilizable a demanda del personal responsable y autorizado de manipularlo en el momento que el considere que sea indispensable. Todas estas características aseguran que los usuarios sean (personas, procesos, etc), y el cual los que no tengan acceso, no logren obtener información sobre estos datos.[8]

4.2.6 Amenaza. Peligro potencial que se presentan en la infraestructura tecnológica y/o activos dentro de la empresa. Estos se hacen visibles al momento que se identifican vulnerabilidades sobre los activos de la empresa y sean usados para fundar deterioros dentro de la infraestructura tecnológica de la empresa.[9]

4.2.7 ISO/IEC 27002:2013. Trata de los controles para la seguridad que se deban implantar adentro de las empresas, es un modelo de destrezas el cual apoyan a minimizar amenazas, riesgos y/o debilidades en la información que manejan dentro de la empresa, cumpliendo con directrices de la norma mencionada como lo son: implementar de control para la privacidad en los datos, establecer modelos creado por la empresa misma que cumplan con los controles de las políticas de privacidad para los activos según el modelo.[10]

4.2.8 Ingeniería social. Aplicación de técnicas, que manejan los hackers para engañar a un usuario autorizado en sistemas de información de una compañía para

[7] SANTIAGO, Enrique Jesús y SÁNCHEZ ALLANDE, Jesús. Riesgos de ciberseguridad en las empresas. En: Revista de Ciencia, Tecnología y Medio Ambiente, (2017); p. 1-33.

[8] PALACIOS ORTEGA, Andrés. Diseño de un modelo de políticas de seguridad informática para superintendencia de industria y comercio de Bogotá. Bogotá, D. C., 2015. 87p. Trabajo de grado (pregrado en Ingeniería de Sistemas). Universidad Libre de Colombia, Facultad de Ingeniería.

[9] FAJARDO DÍAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano. Bogotá, D. C., 2017. 73p. Trabajo de grado (especialización en Seguridad de la Información). Institución Universitaria Politécnico Gran Colombiano, Facultad de Ingeniería y Ciencias Básicas.

[10] SALAZAR CHOEZ, Teodoro Kelvin. Análisis de la Norma ISO/IEC 27002:2013 para mejorar los controles de la seguridad de la información en la sala de cómputo # 14 de la carrera de Ingeniería en computación y redes. Jipijapa, Manabí Ecuador. 2018. 113p. Trabajo de grado (pregrado Ingeniería en Computación y Redes) Universidad Estatal del Sur de Manabí, Facultad de Ciencias Técnicas.

que este revele información sensible e importante creando un hueco de seguridad que pueda ser explotado.[11]

4.2.9 Políticas de la seguridad de la información. Aplicación Su primordial función es adoptar medidas que estén destinadas a preservar la confidencialidad, integridad y disponibilidad de los activos de la información de una empresa. Cada empresa puede estipular sus propias políticas las cuales deben ser aprobadas por la alta gerencia y socializadas con todos los trabajadores ya sean internos o externos de la empresa. En el cual estas políticas deben estar en constante actualización y ser reas por personal calificado para afrontar las necesidades de la organización.[12]

4.2.10 Delito informático. Suceso en el cual hace parte un sistema de cómputo como objeto en la ejecución de un hecho criminológico, en donde se vulnera la confidencialidad y la integridad de la información de los ciudadanos.[13]

4.3 MARCO TEÓRICO

Dentro de la seguridad informática es importante analizar y tener claro muchos de los conceptos teóricos que se presenta, permitiendo tener una visión más amplia y profunda para lograr solucionar cualquier inconveniente actual, entre los cuales puede ser un ***Ciberataque,*** donde, todo ataque dirigido a los (SI) Sistemas de Información que ofrecen servicios web, que pueden estar en riesgo y la información valiosa de la empresa quede expuesta, estos daños pueden ser en las bases de datos, en páginas web, servidores y dispositivos móviles con los que los usuarios interactúan, teniendo como objetivo primordial obtener datos personales para fines delictivos personales y financieros como robos en cuentas bancarias, estos ataques pueden ser mediante un ***Malware,*** lo que se conoce como cualquier tipo de programa o software creado con el fin de cometer un delito informático o realizar un daño al software o hardware.

Estos virus informáticos ingresan por las vulnerabilidades que se presentan en los SI y pueden esparcirse o multiplicarse si están codificados para tal fin, a estos tipos de malware se les conoce como ***gusanos o troyanos***, el daño que causan depende

[11] NOVOA GUTIÉRREZ, Edwin Alberto. Ingeniería Social como delito informático en las grandes empresas colombianas. Bello, Antioquia, 2018. 58p. Trabajo de grado (especialización en Seguridad Informática) Universidad Nacional Abierta y a Distancia UNAD, Facultad de Ingeniería y Ciencias Básicas.
[12] FAJARDO, *Op. cit.* p. 61.
[13] CANO, Jeimy. (2016). Fraude informático: viejos trucos, nuevos entornos. En: ACIS. No. 139 (jul, 2016).

de su estructura y fin con el que fueron creados; o también pueden ser ataques mediante ***Phishing***, el cual trata de suplantar la identidad, para lograr obtener credenciales (como números de tarjetas de crédito, información personal bancaria, o contraseñas de sus cuentas personales) para lograr utilizar los datos mediante el engaño, la persuasión o correos falsos que se direccionan para obtener datos de acceso.

Algunos de los ataques más comunes son los que se realizan mediante ***Ingeniería social***, que es toda la reunión de técnicas utilizadas para engañar a usuarios de algún sistema o personas y obtener los objetivos del ataque, dentro de esta técnica de ataque se incluyen las demás planteadas y muchas otras más como: *pretesting* (creación de escenarios), *baiting* (ataques por medio de dispositivos de almacenamiento). Otro ataque que también se presenta con mayor frecuencia y de los cuales muchas veces no se logra rescatar la información es el conocido como ***Ransomware***, es un malware de tipo troyano que imposibilita utilizar el dispositivo y la información del equipo encriptando los datos. Los atacantes utilizan la extorsión, hasta que los dueños del sistema paguen por el rescate y la descodificación de los mismos, muchos de estos programas se han logrado mitigar ya que existe en la web personas denominadas ***White hacker*** que se encargan de aportar sus conocimientos en seguridad e informática con el fin de contra-atacar todos los daños cibernéticos ocasionados por ataques y delitos informáticos.

Para contrarrestar todos estos ataques, es importante aplicar ***Ciberseguridad,*** acciones, estrategias, controles y demás que se utilizan e implementan dentro de los SI para disminuir las vulnerabilidades y riesgos cibernéticos y tener un plan de aseguramiento ante cualquier ciberataque, como por ejemplo, a través de la instalación de un Firewall (cortafuegos), el cual es un control de seguridad perimetral que se aplica dentro de la red LAN de un sistema informático, configurado para determinar que usuarios o dispositivos pueden o no tener credenciales para acceder a los datos internos, de esta manera se logra proteger la infraestructura de accesos no autorizados, bloqueo de páginas o aplicaciones donde se detecten algún tipo de ataque, alarmas sobre conexiones no autorizadas y control de tráficos de red; o aplicaciones de ***Controles de Acceso***, donde su principal función es administrar mediante dispositivos, software y administradores del servicio la entrada y salida de usuarios a sistemas e infraestructuras de las organizaciones, brindando accesos o restricciones según estipule la misma organización, algunos de los dispositivos utilizados son: lectores biométricos, lectores de tarjetas, lectores códigos QrR y de barra, contraseñas, sistemas de control de acceso mediante el móvil o IoT, entre otros.

Para lograr un proceso de gestión en ***seguridad informática,*** debe conocerse las particularidades de lo que se intenta resguardar, como es la infraestructura

tecnológica dentro de la empresa, los recursos tecnológicos, los documentos, el cual la empresa tiene información que puede ser crítica, valiosa y sensitiva, para lograr establecer los valores de cada activo el cual se vuelve indispensable para evitar futuros riesgos y vulnerabilidades dentro de la infraestructura tecnológica de la empresa.[14]

En cuanto a la ciberseguridad, se puede indicar que su objetivo principal es proteger los equipos organizacionales, los servidores, de situaciones en la que se toman medidas de prevención de riesgos cibernéticos propios del campo en el que se maneja e instaura un compuesto de modalidades de defensa, avance y resiliencia, primitivamente que se desconocen e insuficientemente utilizadas adentro de las políticas de la empresa. La ciberseguridad o también conocida como seguridad de tecnología de la información, está apoyada en los softwares y recursos tecnológicos que sirvan para salvaguardar la infraestructura tecnológica de los usuarios que incidan en realizar delitos informáticos; teniendo como objetivo prevenir y/o reducir los daños a todos los sistemas de información, activos o afectación física de los equipos de cómputo. [15]

Para lograr equilibrar la ***reducción de vulnerabilidad*** dentro de una empresa se establece una gestión correcta de las contraseñas, la administración de accesos privilegiados no se debe tomar a la ligera, por lo tanto, es necesario implementar medidas para proteger adecuadamente los equipos, la infraestructura tecnológica y datos confidenciales de los usuarios.

Es importante resaltar que las acciones del Cibercrimen afectan a la sociedad en general, no exclusivamente a las organizaciones legalmente constituidas. Una institución con un buen SGSI (Sistema de Gestión de Seguridad en la Información) puede notificar sobre los ataques informáticos, mostrando el cómo se mitigan los riesgos de los posibles ataques, disminuyendo las vulnerabilidades dentro de la empresa. Asimismo, es trascendental plantear una estrategia para la recuperación ante desastres y la continuidad del negocio en el cual sea el evento se dicte la

[14] ACOSTA, UBAQUE, Nubia Esperanza y LEÓN PATIÑO, Tania Kruskaya. Diseño del sistema de gestión de seguridad de la información (S.G.S.I) para el centro de datos de la personería de Bogotá D.C bajo las Normas NTC ISO IEC 27001:2013 y NTC ISO IEC 27002:2013. Bogotá, D. C., 2017, 219p. Trabajo de grado (especialización en Seguridad Informática). Universidad Nacional abierta y a Distancia – UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería.

[15] GÓMEZ ORJUELA, Fredy Humberto y VALENCIA VALENCIA, Héctor Fernando. Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa. Medellín, 2021, 246p. Trabajo de grado (magíster en Seguridad Informática). Instituto Tecnológico Metropolitano, Facultad de Ingeniería.

manera en la que las operaciones de la empresa vuelvan a tener su rumbo normal.[16]

La norma ISO 27002 es una recopilación de buenas prácticas para implementar en una empresa, el cual es un estándar que permite por medio de recomendaciones y el uso de buenas prácticas, disminuir los riesgos que presentan los activos de la compañía, de tal modo que al momento de generarse un episodio se minimiza el daño y se asegura la continuación de los procesos, con esto se consigue consolidar la protección de los SI de la compañía y disminuir de esta forma la amenazas y riesgos.[17]

El mundo hoy en día está expuesto a eventos en lo que van avanzando a un ritmo bastante rápido e incluso con una elevada cantidad de filtraciones de datos que exponen la seguridad a riesgos y amenazas cada año, debido a la enorme cuantía de información que se crea todos los días, en los sistemas informáticos y estos son el blanco de los ciber delincuentes, hackers, el cual son riesgos que se corren por el uso de las tecnologías y su constante evolución e innovación.[18]

El modelo de Seguridad Informática congrega métodos y políticas que se aplican para la protección de la información. El objetivo es la efectiva y eficiente prestación de servicios TI. En términos generales la Seguridad Informática, es la rama de la informática que tiene como fin la seguridad de las infraestructuras de cómputo y específicamente la seguridad de los datos. Para el desarrollarlo de esta ciencia se requiere de estándares, métodos, leyes y reglas, protocolos, y diversas herramientas que contribuyen a lograr minimizar los posibles riesgos a la infraestructura o a los datos.[19]

4.4 MARCO HISTÓRICO

El hackeo de los SI (Sistemas de información), en las empresas son fenómenos que han ido en ascenso, en el cual obtienen información privada de las empresas comprometiendo los datos privados en los activos, daños a la infraestructura, daños

[16] SALAZAR CHOEZ, *Op. cit.* p. 16.
[17] PARRA CALDERÓN, Jairo Andrés. Delitos informáticos y Marco Normativo en Colombia. Pitalito – Huila, 2019, 134p. Trabajo de grado (especialista en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas de Tecnología e Ingeniería.
[18] PEÑARANDA SUAREZ, José Luis. Diagnóstico de seguridad al sistema informático de gestión de contratos de prestación de servicios (CPS) de la Universidad del Rosario. Ocaña, 2017, 64p. Trabajo de grado (especialista en Auditoría de Sistemas). Universidad Francisco de Paula Santander, Facultad de Ingeniería de Sistemas.
[19] PEÑARANDA SUÁREZ, *Op. cit.,* p. 26.

a la información, generando perturbación en el quehacer diario de la empresa el cual puede llevarlos inclusive al fracaso. Según un reporte realizado por Symantec, que realizó un estudio entre 157 países, revelo que Colombia estuvo en la sexta nación de Latinoamérica con los mayores ataques en el 2017. Los delitos informáticos se convierten con el pasar del tiempo en una de las principales causas que afectan directamente a la seguridad de los activos de la información, fundamentalmente en los datos que circulan en la web.[20]
Por otro lado: "En Colombia los casos de cibercrimen han aumentado cerca del 28% cada año, de acuerdo con reportes del centro Cibernético Policial, donde afecta en gran parte la seguridad y privacidad de los usuarios."[21]

4.4.1 Antecedentes o estado actual. A continuación se muestran investigaciones recientes sobre incidentes informáticos a nivel internacional, nacional y local en donde se basan en gran parte de sus proyectos en aspectos que van asociados a la ciberseguridad y a la protección de las infraestructuras tecnológicas de las empresas, que mantienen una conexión continua al internet o servidores de la web; en estas investigaciones se logra identificar algunos factores importantes para tomar como referencia en la realización del proyecto, como se muestra a continuación:

***4.4.1.1 Nivel internacional*.** Según los autores Ladi Lizeth Vilcarromero Zubiate y Evit Vilchez Linares. Los cuales presentaron un proyecto de grado titulado "Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones". Para optar por el título de Magister en Dirección de Sistemas y Tecnologías de la Información de la Universidad Peruana de Ciencias Aplicadas en el año 2018. El cual explica que las amenazas de la ciberseguridad generan riesgos progresivamente dentro de los sistemas de información, vulnerando los activos de la información, la protección de datos personales entre otros factores. En este proyecto plantean una estrategia primordial para lograr suministrar en el departamento del SOC (Centro de Operaciones de Seguridad), un plan de ciberseguridad que logre establecer, monitorear, y optimizar los controles de ciberseguridad, basados en las normas ISO/IEC 27032 e ISO 31000:2009 para lograr así tener un SOC inicial y alcanzar una esencia competitiva en los negocios.[22]

---

[20] VALOYES MOSQUERA, Amancio. Ciberseguridad en Colombia. {En línea} 28 de agosto de 2019. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/6370

[21] GARCÍA JAY. Cibercrimen le cuesta a Colombia más de $190 mil millones de pesos al año. {En línea} 26 de junio del 2015, párr. 10 {Entrevistado por el diario El Tiempo} Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesosal-ano-380830

[22] VILCARROMERO ZUBIATE, Ladi Lizeth y VILCHEZ LINAREZ, Evit Vilchez. Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. Lima, 2018, 107p. Trabajo de grado

Por otro lado, el autor Jorge Martín Rodríguez Castro. El cual presento un proyecto de grado titulado “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”[23]. Para optar por el título de Magister en Ingeniería de Sistemas y Computación con mención en Dirección Estratégica de Tecnologías de Información de la Universitas Studiorum Sanctus Turibius de Mogrovejo, Perú en el año 2019. En el cual proponen un diagnóstico para saber el estado actual de la empresa y de cómo realizan los procesos para salva guardar los activos de la información, y a qué tipo de amenazas, vulnerabilidades y riesgos están expuestos. El proyecto de tesis se fundamenta en un método cuantitativo – experimental que permite recolectar información para crear un plan de gestión de riesgos de TI, donde se pretende estar a la vanguardia de los cambios e innovaciones que ayuden al perfeccionamiento continuo de la compañía, basándose en la ISO 31000:2018, ISO 27005:2018, COBIT 5 for Risk, Magerit v3.0 y ISO 22301:2012. Este proyecto de grado se relaciona con la investigación que se está realizando dado que proporciona datos significativos para implementar los mecanismos que apoyen un plan de gestión para mitigar los riesgos dentro de la empresa.

***4.4.1.2 Nivel Nacional*.** De acuerdo con Fredy Humberto Gómez Orjuela y Héctor Fernando Valencia Valencia. Que presentaron un trabajo de grado titulado “Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa[24]”. Con el fin de obtener el título de Magister en Seguridad Informática en el Instituto Tecnológico Metropolitano, de la ciudad de Medellín en el año 2021. En la investigación se estructura un plan para la gestión de incidentes de ciberseguridad, donde se parametrizan políticas relacionadas con la gestión de riesgos de tal forma que no existan interrupciones en la operatividad de la empresa. El trabajo de grado se apoya en estándares de ciberseguridad como lo son: NIST Cybersecurity Framework, Estándar NIST SP 800-61, MINTIC, INCIBE y la ISO/IEC 27035; donde sirven como base para diseñar y validar los procesos dentro de la empresa para la gestión de los incidentes de ciberseguridad, el cual envía respuestas corporativas de acuerdo a las políticas que están establecidas el cual

(maestría en Dirección de Sistemas y Tecnologías de la Información). Universidad Peruana de Ciencias Aplicadas, Escuela de Posgrado.

[23] RODRÍGUEZ CASTRO, Jorge Martín. 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. Chiclayo, Perú, 2019, 226p. Trabajo de grado (maestro en Ingeniería de Sistemas y Computación con mención en Dirección Estratégica de Tecnologías de Información). Universidad Católica Santo Toribio de Mogrovejo, Escuela de Posgrado.

[24] GÓMEZ ORJUELA, Fredy Humberto y VALENCIA VALENCIA, Héctor. Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa. Medellín, 2021, 246p. Tesis de grado (maestría en Seguridad Informática).

logra brindar una mejora en cada uno de los procesos que se ven afectados o vulnerados por ataques cibernéticos.

Por otro lado, Jorge Eliécer González Díaz y Víctor Alfonso Parrado Rodríguez. presentan un proyecto de grado titulado “Guía de gestión de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación – OTIC del Ministerio de Salud y Protección Social, tomando como base la norma ISO 27001:2013[25]”. Como requisito para obtener el título de Especialista en Seguridad Informática, de la Universidad Piloto de Colombia en la ciudad de Bogotá, en el año 2016. El trabajo de grado tiene como identificar diversos incidentes de seguridad de la información y proveer un documento que sirva como guía para obtener las contramedidas necesarias para hacer frente a los incidentes y/o eventos que afecten la seguridad de la información. Basado en la metodología de la norma ISO/IEC 27035:2011 donde se establecen procesos para la gestión de incidentes en seguridad de la información, de tal forma que se pueda preservar la confidencialidad, integridad y disponibilidad de toda la información de la empresa. Dicho proyecto se encuentra relacionado con este trabajo de investigación, ya que se pretende alcanzar un modelo para la gestión de incidentes dentro de una empresa y así mitigar posibles eventualidades que afecten la seguridad en los procesos que realicen en la organización.

***4.4.1.3 Local*.** De acuerdo con el autor Ramiro Andrés Delvasto Ramírez. El cual presento un proyecto de grado titulado “Modelo de gestión de incidentes de seguridad de la información para PYMES”[26]. Para alcanzar su título de Especialista en Seguridad Informática, de la Universidad Nacional Abierta y a Distancia (UNAD), Colombia en el año 2016. El cual tiene como objetivo principal establecer un modelo para la gestión de incidentes de seguridad de la información donde se busca que las diferentes dependencias de la empresa logren controlar un evento de ciberseguridad mediante la detección, reporte, contingencia y recuperación ante desastres pudiendo continuar con la productividad dentro de la organización. El trabajo se constituye en una monografía de compilación donde se lleva a cabo un análisis de distintas experiencias, basadas en la aplicación de la norma ISO/IEC 27035, el cual ayuda a realizar una clasificación de los incidentes de la seguridad de la información de la empresa, (el cual está sujeta a las políticas); esta depende

[25] GONZÁLEZ DÍAZ, Jorge Eliécer y PARRADO RODRÍGUEZ, Víctor Alfonso. Guía de gestión de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación – OTIC del Ministerio de Salud y Protección Social, tomando como base la norma ISO 27001:2013. Bogotá, D. C., 2016, 231p. Tesis de grado (especialización en Seguridad Informática), Universidad Piloto de Colombia, Facultad de Ingenierías.

[26] DELVASTO RAMÍREZ, Ramiro Andrés. Modelo de gestión de incidentes de seguridad de la información para Pymes. Bogotá, D. C., 2016, 64p. Tesis de Grado (especialización en Seguridad Informática), Universidad Nacional Abierta y a Distancia (UNAD), Escuela de Ciencias Básicas, Tecnología e Ingeniería.

de su infraestructura tecnológica, de sus riesgos y criticidad de cada uno de los activos de la información que existen dentro de la empresa.

4.5 MARCO NORMATIVO

4.5.1 NIST, marco de ciberseguridad. Este marco es una guía de buenas prácticas que se implementa dentro de las organizaciones que busca mantener su información protegida de los riesgos y amenazas del entorno web. Este marco es utilizado mayormente para la protección en ciberseguridad dentro de las infraestructuras críticas, sin embargo, es aplicable a cualquier compañía que desarrolle actividades con la información en entorno web. En la web oficial de NIST, se presenta el desarrollo del marco de gestión de ciberseguridad el cual consta de tres fases componentes principales: el núcleo, los niveles de implementación y los perfiles[27].

Núcleo: aquí se presentan las diferentes normativas, estándares y lineamientos que son aplicables dentro de la organización en toda su estructura, dentro de este se especifican cinco funciones, las cuales comprenden[28]:

- Identificación: Se trata de tener claridad sobre que dispositivos y software posee la compañía para determinar y crear estrategias de control de ciberseguridad involucrando al personal interno y externo, reconociendo los riesgos y amenazas que enfrenta el sistema informático, para lograr aplicar las medidas necesarias para mitigar estas vulnerabilidades. Esta función incluye: Gestión de activos, Entorno de negocios, Gobernanza, Evaluación de riesgos y Estrategia de gestión de riesgos.[29]
- Protección: realizan diferentes metodologías para salvaguardar los activos como controles de acceso, criptografías, el cual constan de capacitaciones, copias de seguridad entre otras, se busca mantener un alto índice de protección de los datos del sistema.

[27] ESTADOS UNIDOS. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. {En línea} disponible en: {https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf}

[28] ESTADOS UNIDOS. FEDERAL TRADE COMISSION. Ciberseguridad para pequeños negocios. Que es y cómo funciona el marco de ciberseguridad del NIST. {En línea} {3 de mayo de 2021} disponible en: {https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf}

[29] ESTADOS UNIDOS. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Op. cit. p. 30.

- Detección: Implementando técnicas y metodologías adecuadas se busca una detección temprana de posibles vulnerabilidades que permitan acceso a ataques cibernéticos que comprometen la información, el objetivo es buscar y analizar estas susceptibilidades del sistema antes que un posible atacante.

- Respuesta: Se debe tener un protocolo establecido para contrarrestar o prevenir amenazas y riesgos detectados, informar a los usuarios involucrados, documentar y presentar ante las directivas los sucesos de este tipo y actualizar el plan de protección.

- Recuperación: Mantener planes que permitan recuperar el sistema informático de una manera óptima restableciendo todos los procesos luego de presentarse algún tipo de ataque.

Niveles de implementación: El marco especifica que se debe clasificar los niveles de riesgos según el estado de protección o gestión de ciberseguridad de la organización, teniendo en cuenta los objetivos estratégicos, teniendo en cuenta e y la operación de la empresa, esta clasificación permite a los directivos tomar decisiones en relación a las prioridades que deben asumir para la gestión de dichos riesgos.

Los niveles de implementación se dividen en:[30]

- Nivel 1 o parcial, cuando dentro de la organización no se tiene un plan de gestión de riesgo bien definido o claro, sin que exista una colaboración efectiva dentro y fuera de la organización.

- Nivel 2 o de riesgo informado, la organización conoce los riesgos existentes de ciberseguridad, pero no se cuentan con políticas o lineamientos bien definidos para control de riesgos dentro y fuera de la organización.

- Nivel 3 o repetible, se conoce y se implementa gestión de seguridad para el correcto manejo de los riesgos cibernéticos, implementando métodos y técnicas que contribuyan a la protección del sistema, evaluando cada proceso.
- Nivel 4 o adaptable, las organizaciones mantienen en el funcionamiento del negocio una gestión de riesgos que está orientada a mejoras continuar a través de procesos, métodos, lineamientos, normas, estándares, entre otros, de tal manera que exista una constante protección contra riesgos de ciberseguridad.

[30] *Ibid*. p. 9-10.

Perfil del marco: a través de la implementación de la norma, los perfiles de marco contribuyen a dar una visión general en cuanto a cómo se encuentra la organización en relación a la gestión de riesgos asociados a la ciberseguridad, dentro de los perfiles se contempla el "Perfil Actual"[31] donde muestra lo que actualmente se ha logrado implementar en seguridad cibernética, y el "Perfil Objetivo"[32] donde se plantea lo que hace falta en temas de gestión de riesgos para alcanzar los objetivos propuestos de ciberseguridad, estos dos perfiles permiten que la organización posea una vista del estado actual vs el estado al que se desea llegar, con el fin de lograr implementar todo lo necesario para obtener un alto índice de seguridad en los SI.

4.5.2 Modelo de Seguridad y Privacidad de la Información (MSPI)[33]. Este modelo se implementa dentro de los SI de los entes gubernamentales y públicos de Colombia se lleva a cabo la identificación, evaluación y tratamiento de riesgos y vulnerabilidades el fin es logra una mejora continua con respecto a la seguridad. Así mismo se comprende una Gestión del Riesgo de Seguridad Digital (GRSD)[34] donde se determinan las políticas, roles , responsabilidades, contextos, impactos, y tratamiento de los riesgos, así mismo contempla la asignación de un responsable de seguridad digital con la capacidad de orientar, implementar, evaluar y monitorear la gestión de riesgos, donde su participación como encargado de seguridad, debe velar por la protección de los datos, y debe mantener informado a los directivos y altos mandos sobre todo los temas que estén relacionados con los riesgos y las vulnerabilidades que puedan suceder dentro de la empresa.

A través de la clasificación de activos (información, programas, redes, dispositivos, TI, páginas web, personas, instalaciones, entre otros) dentro de cada proceso, se logrará identificar si el organismo contempla que si se cumple el MSPI el cual le permitirá evaluar en qué grado de criticidad se encuentra según la seguridad de la información, donde el impacto que genere social, económico y ambiental supere los criterios establecidos dentro del modelo.

---

[31] *Ibíd.,* p. 11.
[32] *Ibíd.,* p. 11.
[33] REPÚBLICA DE COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. VICEMINISTERIO DE ECONOMÍA DIGITAL. Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD). {En línea} {2018}. Disponible en {https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+Públicas+-+Guía+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b}
[34] *Ibíd.* p. 10.

Se deberán identificar los riesgos, amenazas y vulnerabilidades según lo estipulado en la metodología, con el fin de que cada ente gubernamental y público brinde aportes individuales de personas involucradas o líderes de área y/o expertos en seguridad para luego valorar los riesgos a través de la utilización de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de controles en Entidades Públicas del DAFP[35]", así como se deberá identificar y evaluar las estrategias aplicables para el manejo de los riesgos basados en la norma ISO/IEC27001, donde también se incluye las acciones que deben tener para la mitigación de los riesgos una vez planteados los lineamientos se ejecutarán las acciones pertinentes para lograr mitigar cualquier ataque. El director de seguridad guía y orienta el plan de ejecución de cada uno de los responsables para realizar cada una de las tareas dentro de sus a ejecutar.

El modelo MSPI plantea una fase de monitoreo y evaluación donde cada ente gubernamental y público deberá realizar seguimiento a los planes y controles establecidos con el fin de controlar los riesgos disminuyendo las vulnerabilidades, contribuyendo a las mejores continuas y decisiones que toman los altos mandos en la organización. Dentro de la revisión se deberá realizar registros de incidentes para el análisis de fallos y perdidas de información, reportes de gestión del riesgo de seguridad, estos reportes incluyen: matrices de riesgo, listado de activos, reportes de criticidad e impactos, evolución de las debilidades, impactos económicos[36] el cual deben realizarse cada vez que ocurra un suceso, y se produzca un cambio importante en el sistema, o se incluya un nuevo proceso dentro de alguna dependencia de la empresa.

Dentro del plan se contempla la realización de auditorías internas y externas que permitan mantener un adecuado uso de los lineamientos, normas y controles de la implementación del SGSI con el fin de que todos los sistemas informáticos de los entes gubernamentales y públicos cumplan con lo que se estableció anteriormente.

4.5.3 Norma ISO/IEC 27032. Estándar de ciberseguridad, dentro de esta guía se plantean controles para la SI, en la infraestructura de red, y en las infraestructuras determinadas como críticas, con el objetivo de proporcionar a la organización que implemente esta norma la reducción de riesgos cibernéticos como ingeniería social, malware, *phishing, smishing, pretesting*, DDoS, entre algunos de los tantos ataques que se presentan en el entorno web.

La norma ISO 27032 nace como un complemento de la norma ISO 27001, el cual

[35] *Ibíd.,* p. 10.
[36] *Ibíd.,* p. 25.

tiene como propósito principal estipular dentro de la empresa buenas prácticas para lograr proteger los activos de la información, los que claramente son lo más importante que tiene una organización para poder ejecutar cada uno de los procesos dentro de ella. En el cual, las empresas actualmente no conocen como lograr implementar, adaptar o llegarse a certificar con estándares relacionados con la norma ISO 27001.[37]

Dentro de la norma se estipula que las partes interesadas como los que ofrecen los de productos web deben velar por la implementación de ciberseguridad mediante protocolos y políticas que minimicen vulnerabilidades y riesgos al momento de compartir la información, de gestionar los riesgos o incidentes y al responder ante un ataque.

La norma indica que, para implementar ciberseguridad, se debe aplicar seguridad dentro de la red interna LAN mediante el modelo OSI (Open Systems Interconnection Model) presentado en la norma ISO/IEC 7498-1[38] el cual estandariza la manera que deben funcionar las comunicaciones conectadas no privadas, ya que estos sistemas de protección se emplean en las diversas capas OSI que varían según su estructura y su forma de proteger según su diseño. (Véase Figura 1)

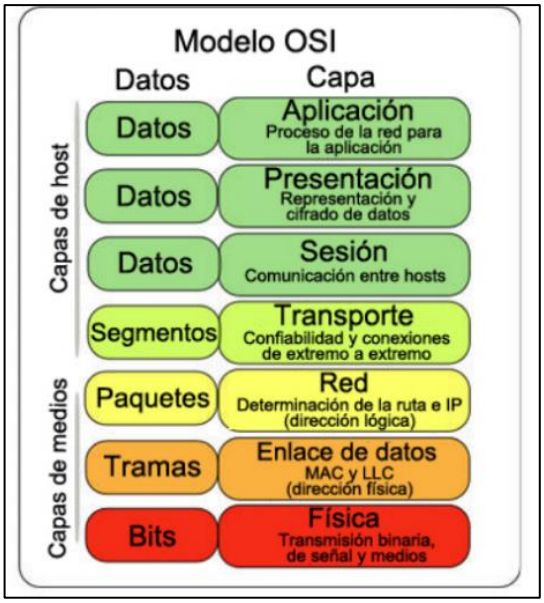
Determinando para cada una de las capas, una seguridad mediante controles, protocolos y políticas que proporcionen reducción de vulnerabilidades dentro de la infraestructura. La norma provee, “guías de hardening, listas de verificación, formatos, manuales de instalación”[39], entre otros, con el fin de adoptar un modelo de seguridad eficaz y confiable.

[37] GUZMÁN SOLANO. Sandra. Guía para la implementación de la Norma ISO 27032. Bogotá, D. C., 2019, 69p. Trabajo de grado (especialización en Seguridad de la Información), Universidad Católica de Colombia, Facultad de Ingeniería.

[38] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 7498-1. Information technology Open System Interconection. {On line} 2000 available in {https://www.iso.org/ics/35.100/x/}

[39] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity. {On line} 2012 available in: {https://www.iso.org/standard/44375.html}

Figura 1. Modelo OSI.



CORTÉS, Aníbal. Capítulo 6 Capa de Red, introducción a redes. CISCO. {En línea} {27 de mayo del 2021} disponible en: {http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter6_Capa%20de%20red.pdf}

4.5.4 COBIT. Presenta un marco para buenas prácticas a través del gobierno TI, se enfoca en la buena administración que se le debe dar a todos los recursos de tecnología de la información (información, aplicaciones o software, tecnologías, hardware, sistemas operativos, multimedios, redes, instalaciones físicas, recurso humano, entre otros) alineándolas e integrándolas con la necesidad del negocio, involucrando desde la gerencia para el apoyo y decisiones financieras de inversión, el personal técnico de TI, los auditores que evalúan el estado del sistema para aportar posibles mejoras, responsables de procesos o negocios, hasta los usuarios finales que interactúan día a día con el sistema. Proporciona 9 principios organizados por dos grupos".[40] Dentro de los cuales tenemos:

4.5.4.1 Principios de sistema de gobierno[41]*.*

- Valor para las partes interesadas: proporciona un factor clave a tener en cuenta a través del gobierno corporativo, teniendo en cuenta que se crean estrategias donde se tomen las mejores decisiones para lograr establecer un grupo amplio de partes interesadas donde estas se convierten en un activo importante para la

[40] RITEGNO. *Op. cit.,* p. 14
[41] *Ibíd.,* p. 14.

empresa, el cual pueden dar lugar a ventajas competitivas en TI (Tecnologías de la información), que mejor se adapten al modelo de negocio.

- Enfoque Holístico: Buscar la unificación de los datos y el enfoque tecnológico, dentro del gobierno corporativo, que se alinean para cumplimiento de objetivos a través de la buena gobernanza TI.

- Sistema de Gobierno Dinámico: proporciona el buen manejo de riesgos y recursos, se establezcan métodos que proporcionen la creación de valor.

- Separar Gobierno de Gestión: Buscar que la gestión y la gobernanza sean claramente identificadas por separado, determinando la función de cada una dentro de la compañía.

- El sistema de Gobierno debe estar ajustado a la necesidad empresarial: Se requiere diseñar de manera efectiva la participación del sistema de gobierno para que pueda solventar todas las necesidades de la organización y optimizar los recursos.

- Sistema de Gobierno extremo a extremo: Se debe abarcar todos los componentes organizacionales, gobernando el área TI que da soporte y control a las tecnologías de la información, y abarcar su gobierno a todo lo referente a TI, la información que es manipulada (generada, procesada, editada) en la empresa, y las diferentes tecnologías que se utilizan como canales para el procesamiento de la información.

4.5.4.1 Principios del marco de gobierno[42]*.*

- Basado en un modelo conceptual: Para lograr que las TI logren apoyar a la empresa en la automatización de los procesos, es indispensable tener claro los elementos que harán parte de ello y que características propias y comunes deben presentar.

- Abierto y Flexible: el marco que se implemente en lo referente al gobierno, debe permitir futuros cambios o inclusiones al sistema que se adapten perfectamente sin ocasionar ningún tipo de problemas, manteniendo en todo momento la integridad de los datos.

[42] *Ibíd.,* p.17.

- Alineado con los principales estándares: debe cumplir con los lineamientos que exigen los estándares implementados y las regulaciones de ley pertinentes.

Dentro de los objetivos del marco se identifican claramente los 5 objetivos del gobierno los cuales están directamente relacionados a la dirección, supervisión y valoraciones pertinentes para la toma de y cumplimiento de objetivos los cuales contemplan 35 objetivos que se deben contemplar dentro de los procesos de gestión (organización, implementación, soporte, valoración). Dentro del marco se estipula 11 factores de diseño que son determinantes a la hora de saber cuáles de los 40 objetivos se ajustan más al modelo de negocio, dentro de los cuales se busca examinar entre otras cosas como se encuentran determinadas las estrategias empresariales, riesgos, amenazas, las TI, el tamaño de la empresa entre otros.

Así mismo dentro del marco se especifican 7 componentes del sistema, los cuales en la versión del COBIT 5 se denominaban catalizadores, dentro de los cuales, citando directamente al marco, tenemos: “Procesos, Estructuras organizacionales, Principios políticas y procedimientos, Información, Cultura, ética y comportamiento, Personas, habilidades y competencias, Servicios, infraestructuras y aplicaciones.”[43] Dentro de COBIT se implementa un marco de modelo para la evaluación de la “Gestión de rendimiento COBIT”[44] que logra clasificar objetivos en niveles y entender cuáles de estos se adaptan al modelo de negocio.

4.6 MARCO LEGAL

La investigación se basa en razón de la elaboración de un modelo para la gestión de incidentes en ciberseguridad el cual sirva para robustecer cada área dentro de la empresa y ayude a la localización anticipada de las vulnerabilidades, riesgos y amenazas inherentes ante la ocurrencia de un delito informático dentro Proyectos de Inversión Vial Andino S.A.S El marco legal del siguiente trabajo de investigación se fundamenta en las siguientes políticas públicas.

[43] *Ibíd.,* p. 20.
[44] GONZÁLEZ, Pepe. COBIT 2019 — El nuevo modelo de gobierno empresarial para información y tecnología. {En línea} {3 de mayo del 2021} disponible en {https://ppglzr.medium.com/cobit-2019-el-nuevo-modelo-de-gobierno-empresarial-para-informaci%C3%B3n-y-tecnolog%C3%ADa-a7bf92b7288b}

4.6.1 Ley 1273 de 2009[45]. La cual se enfoca en la protección de la información y de los datos, el cual sirva para preservar integralmente los sistemas donde se utilicen recursos tecnológicos y se recolecte todo tipo de información, entre otras disposiciones. Por medio de la cual dicta disposiciones para lograr controlar los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos que tengan las empresas y los sistemas informáticos donde expone varios artículos el cual se deben cumplir:

- **Artículo 269A:** Acceso abusivo a un sistema informático.
- **Artículo 269B:** Obstaculización ilegitima de sistema informático o red de telecomunicación.
- **Artículo 269C:** Intercepción de datos informáticos.
- **Artículo 269D:** Daño informático.
- **Artículo 269E:** Uso de software malicioso.
- **Artículo 269F:** Violación de datos personales.
- **Artículo 269G:** Suplantación de sitios web para capturar datos personales.
- **Artículo 269H:** Circunstancias de agravación punitiva.

4.6.2 Ley 1581 de 2012. La presente ley tiene por objeto el cumplir con el derecho que tienen todos los ciudadanos de disponer los principios de conocer, actualizar y rectificar los datos personales registrados en cualquier base de datos o archivos de las empresas. Estos principios sobre la protección de los datos serán aplicables a todas las bases de datos, cuando estos datos vayan a ser suministrados a terceros se debe de manera previa, informar al titular y solicitar su autorización. En este caso los responsables y encargados de las bases de datos, archivos el cual quedan sujeto a las disposiciones contenidas en la presente ley.

4.6.3 Ley 1928 del 24 de julio de 2018. Se adopta el convenio sobre la ciberdelincuencia, el cual se enfoca en cooperar entre los estados y las empresas del sector privado enfocados en la lucha contra los delitos cibernéticos, así como la insuficiencia de brindar mayor seguridad a los intereses en el manejo de los recursos tecnológicos.[46] El convenio de la ciberdelincuencia es el único instrumento que permite combatir las amenazas a bienes jurídicos tutelados como la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas

[45] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. Protección de la información y de los datos. {En línea} {5 de mayo del 2021} disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[46] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1928 del 24 julio de 2018: convenio sobre la Ciberdelincuencia, {En línea} {5 de mayo del 2021} disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

informáticos, protegiendo en general los intereses vinculados al desarrollo de las tecnologías de la información.

4.6.4 Decreto Número 1573 de 12 de diciembre de 2014[47]**.** Contiene normas para Objeto, ámbito de diligencia, esclarecimientos, manuales y elementos según el Ministerio de las TIC. Que así mismo, la anotada Ley determino que es función del estado intervenir en el sector de las TIC con el fin de promover condiciones de seguridad del servicio al usuario final, incentivando acciones preventivas y de seguridad informática y de redes para el desarrollo de dicto sector.

4.6.5 Ley 23 de 1982. Sobre derechos de autor, el cual son reconocidos los titulares de los derechos reconocidos por ley, al realizar algún proyecto, en el cual la persona natural a jurídica que en virtud de contrato obtenga por su cuenta y riesgo, la producción de cierto tipo de proyecto que fue realizada por un autor o varios con las condiciones previstas en el artículo 20 de esta ley.[48, 49]

[47] REPÚBLICA DE COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC). Decreto Número 2573 de 2014. Diario Oficial No. 49.363 de 12 de diciembre de 2014

[48] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 23 de 1982. Sobre derechos de autor. Bogotá, D. C.: Diario Oficial No. 35.711 de 27 de febrero de 1981.

[49] PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto Nacional 1474 de 2002. Promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996). Bogotá, D. C.: Diario Oficial No. 44.496 del 24 de julio del 2002.

5. DISEÑO METODOLÓGICO

El trabajo de grado tiene en su metodología un enfoque cuantitativo, de acuerdo a, Rodríguez, Erazo y Narváez, los resultados obtenidos “deben ser estadísticamente representativas mediante la aplicación de un muestro representativo, de tal forma que, la información obtenida pueda sacar conclusiones estadísticas de la población en estudio”. Por otro lado, Valdiviezo, la investigación cuantitativa es aquella que: “Se encarga de la recopilación y análisis de información, se pone a prueba o comprueba mediante hipótesis, para lo cual utiliza un análisis estadístico basadas en valores numéricos, lo cual tiene como propósito explicar el fenómeno estudiado”.[50]

Las herramientas del método cuantitativo permitirán describir, la realidad de la empresa. Se empleará la investigación descriptiva para recabar la información cuantificable, con este tipo de investigación se espera encontrar la relación causal, no solamente describir o acercarse al problema de estudio, sino que intenta precisar las causas de este.[51]

- **Fase I – Diagnóstico:** en esta fase se aplica un instrumento de recolección de información, el cual se toma como población y muestra a la oficina encargada de sistemas y el gerente de la empresa Proyectos de Inversión Vial Andino S.A.S donde sus respuestas nos apoyaron a saber el estado actual y/o real en el que está la empresa y el cómo están capacitado el personal profesional dentro de ella.

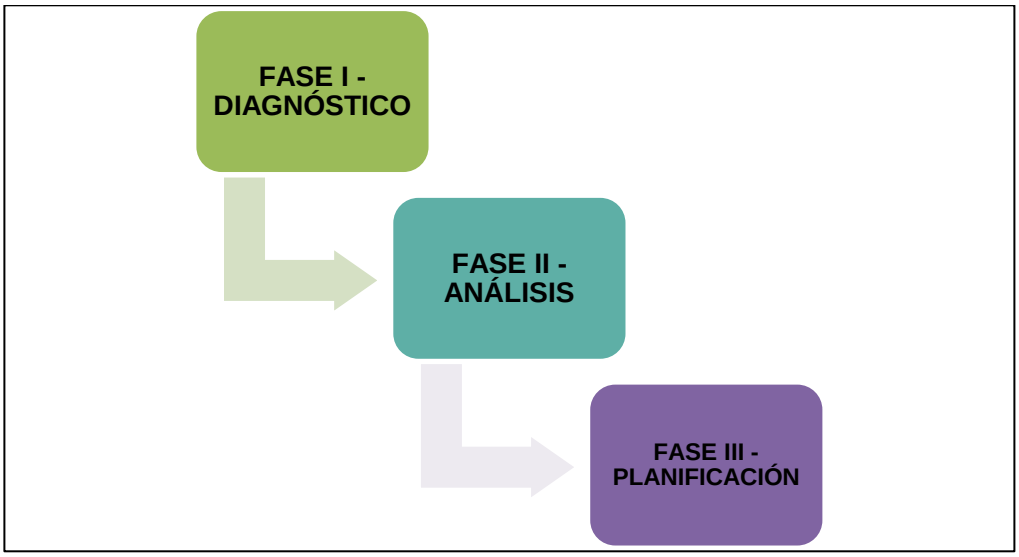
- **Fase II – Análisis** de los incidentes de ciberseguridad que se presentan dentro de la organización. Para la gestión de los mismos, se debe cumplir con la aplicación de la Fase I, la cual nos mostrará indicadores que logren determinar los niveles de riesgos, amenazas, entre otras debilidades que se presenten.

- **Fase III – Planificación:** una vez realizado el diagnóstico y el análisis, se necesita planificar unas bases sólidas de buenas prácticas, con el fin de lograr definir los roles y compromisos del personal encargado de la empresa Proyectos de inversión vial andino S.A.S, la planificación sirve de apoyo para orientar al grupo de trabajo en cuestión de que se presente una debilidad, riesgo o vulnerabilidades

[50] VALDIVIESO SUAREZ, Ximena Estefanía. Metodología de investigación cuantitativa en trabajos de graduación de la modalidad de titulación de la carrera de contabilidad y auditoría. Machala, 2019, 22p. Trabajo de grado (pregrado en Contabilidad y Auditoría) Universidad Técnica de Machala, Facultad de Ciencias Empresariales.
[51] *Ibíd.,* p. 8.

referentes a ataques cibernéticos que se realicen desde el exterior de la empresa o dentro de la misma. (Véase Figura 2)

Figura 2. Fases del proyecto.



Fuente: elaboración propia.

6. FASE I: EXAMINAR DEL ESTADO ACTUAL DE LA EMPRESA

6.1 SITUACIÓN REAL DE PROYECTOS DE INVERSIÓN VIAL ANDINO S.A.S

6.1.1 Componentes del instrumento. Considerando los lineamientos de la norma ISO 27002:2013 en el numeral A16, con el cual se diseña el guion de preguntas (Véase Anexo A), aplicados a la empresa Proyectos de Inversión Vial Andino S.A.S, que brinda servicios en el km76 +800 en la vía Bogotá – Villavicencio, campamento la flor.

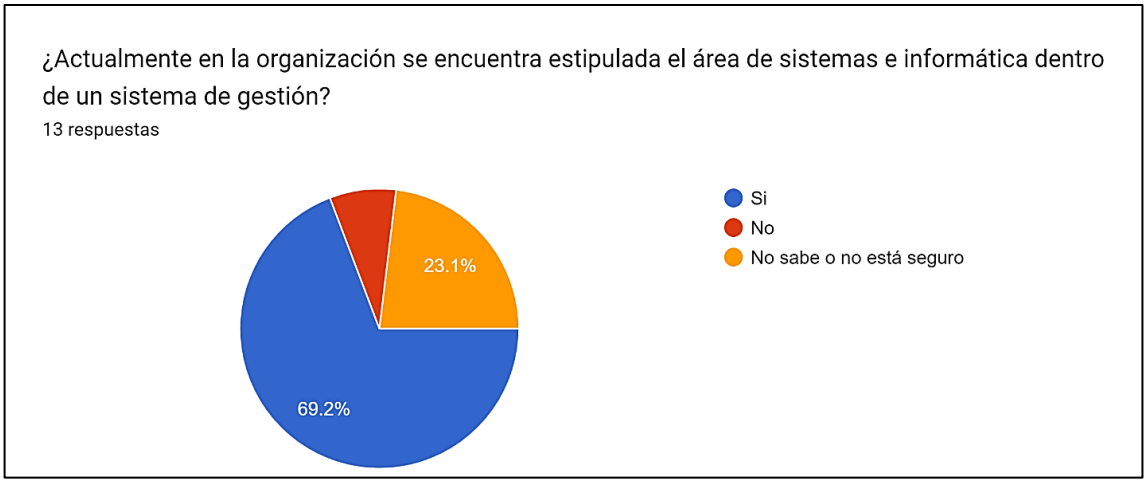
6.1.2 Aplicación del instrumento. Con el fin de analizar el estado actual de la empresa en cómo se está llevando a cabo la gestión de incidentes de ciberseguridad, se aplicó un instrumento al gerente y a 12 profesionales (5 técnicos informáticos, 3 administradores de redes, 1 gerente de tecnología, 2 ingenieros de sistemas y un ingeniero de telecomunicaciones) encargados del mantenimiento y funcionamiento de las tecnologías y sistemas de información, de la empresa, que dio como resultado un criterio negativo el cual muestra debilidades que se están presentando dentro de la organización, que se ven plasmadas en el instrumento (encuesta) mostrando resultados que se ven a continuación para lograr consolidar un modelo, el cual queda orientado a la creación de un plan de gestión para los incidentes en ciberseguridad.

Se toma como población la oficina de sistemas ya que son los encargados de manejar toda la infraestructura tecnológica dentro de la empresa y son los más capacitados para lograr realizar cada uno de los procesos dentro de su dependencia, realizar la encuesta al gerente es esencial ya que es el encargo de aprobar y contratar el personal idóneo para que cumplan con las responsabilidades dentro del Área de Sistemas. Con el instrumento aplicado se presentaron los siguientes resultados (encuesta), estipulando un nivel de madurez con capacidad de determinar los riesgos o como se realiza el manejo de los incidentes en ciberseguridad, para lograr tener las capacidades de resolver uno de los interrogantes de la indagación la cual se formuló para el trabajo de investigación. Por motivos de la pandemia Covid-19, se realizó una encuesta conformada por 13 preguntas claves, por medio de la herramienta de formulario de Google y su distribución se manejó a través de correo electrónico al personal escogido de muestra en la empresa.

Como se puede observar en la Figura 3, el 69.2% de los profesionales del Área de Sistemas de la empresa tienen conocimiento que la dependencia está contemplada dentro de un sistema de gestión, sin embargo, el 30,8% de los entrevistados dicen

que no o desconocen la formación del Área de Sistemas dentro del sistema de gestión de la organización. (Véase Figura 3)

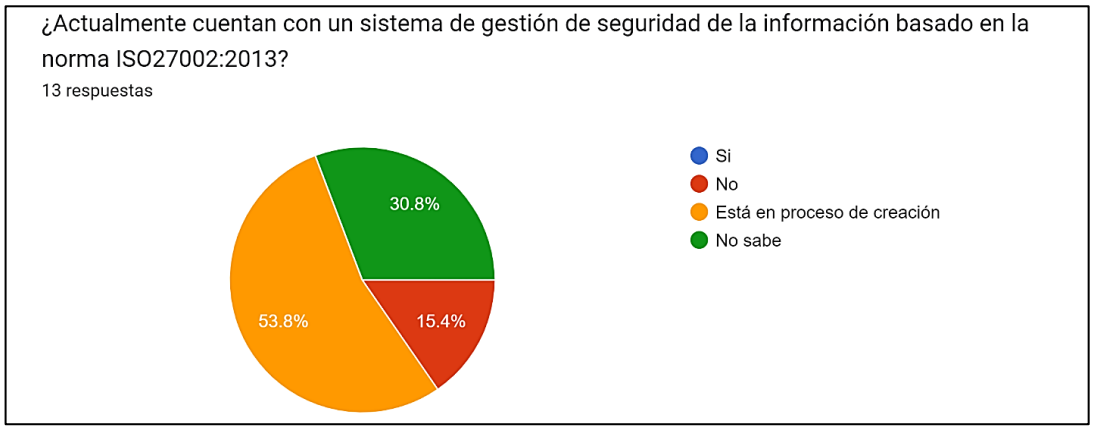
Figura 3. Pregunta 1: Área de Sistemas e Informática está estipulada dentro de un sistema de gestión.



Fuente: elaboración propia.

En la Figura 4, se evidencia que no existe dentro de la organización un sistema de gestión de la seguridad de la información (SGSI) totalmente establecido, ya que solo el 53.8% de los encuestados tienen conocimiento que se encuentran en proceso de implementación del SGSI, el 30.8% no sabe si existe y el 15.4% está seguro de que no existe dentro de la organización. (Véase Figura 4)

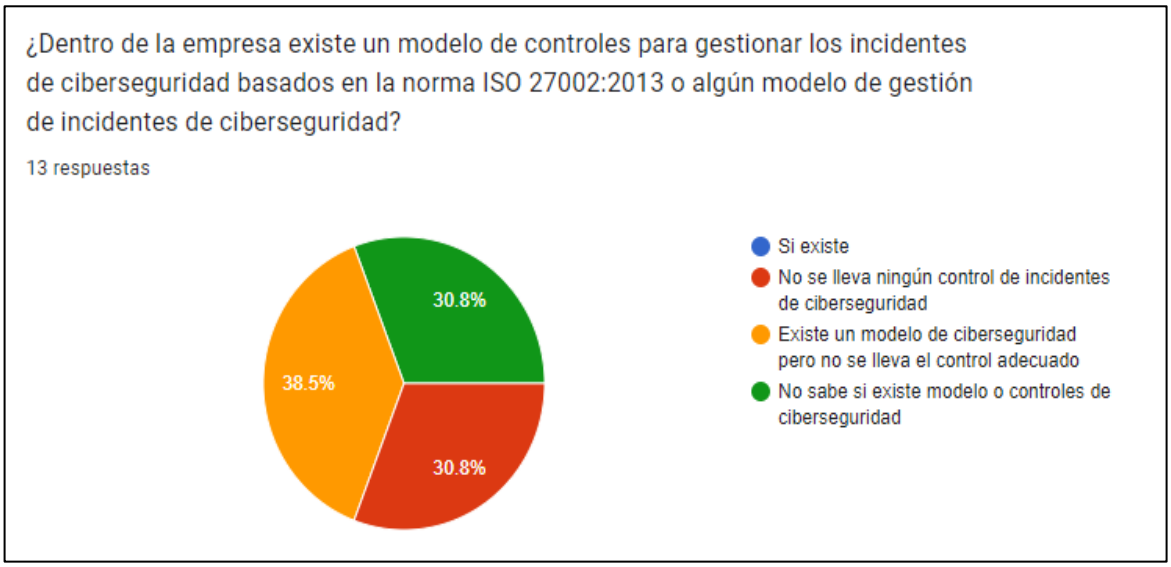
Figura 4. Pregunta 2: SGSI basado en la Norma ISO27002:2013



Fuente: elaboración propia.

De esta pregunta se puede deducir que, aunque dentro de la organización exista un procedimiento para la gestión de incidentes, queda claro que no está estipulado dentro de la norma ISO27002:2013 y que los encargados del Área de Sistemas no siguen un adecuado modelo de gestión de incidentes. Ya que el 61.4% de los empleados encuestados no llevan el control y desconocen si existe un modelo de control de gestión de incidentes. (Véase Figura 5)

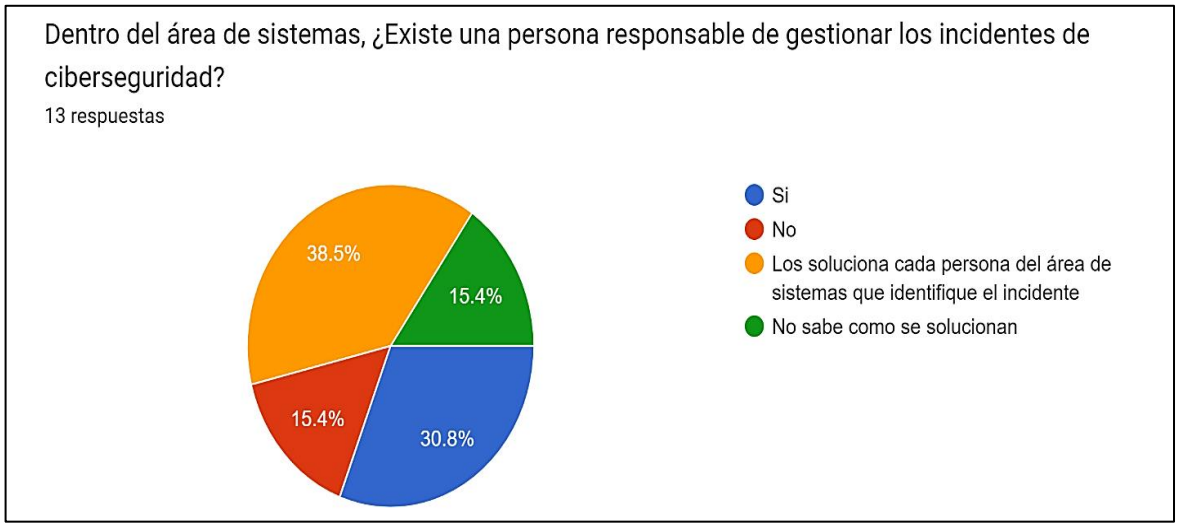
Figura 5. Pregunta 3: Existe un modelo de controles para gestionar los incidentes de ciberseguridad basados en la Norma ISO 27002:2013



Fuente: elaboración propia.

En esta Figura 6 se evidencia que, a pesar de que en la organización está contemplada el Área de Sistemas, los empleados del área no tiene claro si existe o no una persona encargada de gestionar los incidentes de ciberseguridad como un jefe de seguridad de la información, aunque el 30.8% tiene claro que hay una persona encargada de esta función, el 38.5% de estos respondió que cuando se presentan incidentes de ciberseguridad cada uno lo soluciona a su manera y criterio, el 15%.4 no sabe cómo se solucionan los diferentes incidentes de ciberseguridad y el 15.4% dice que no existe una persona encargada del tema. (Véase Figura 6)

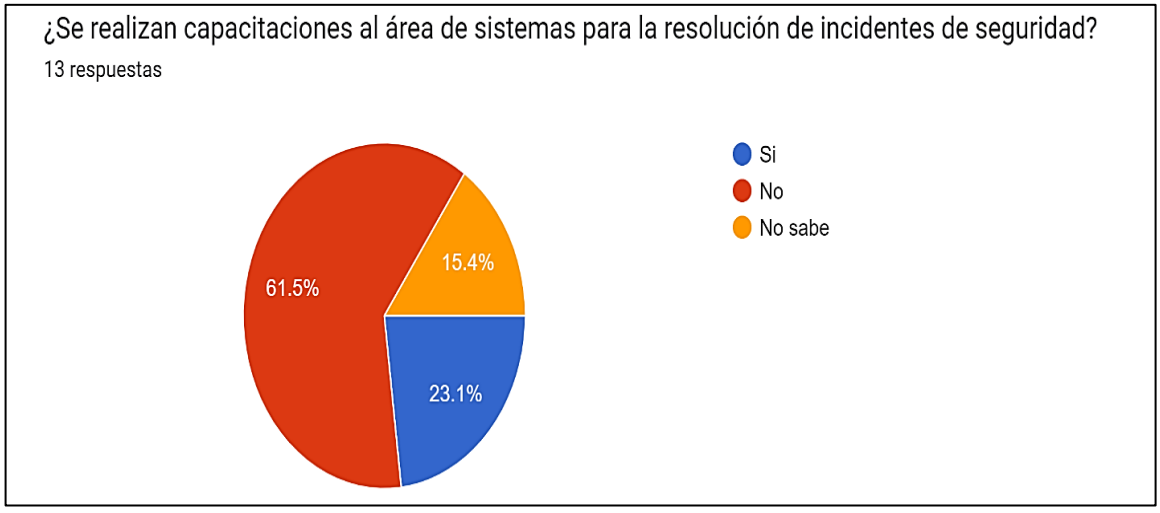
Figura 6. Pregunta 4: Hay una persona responsable de la gestión de accidentes por ciberseguridad.



Fuente: elaboración propia.

Según la Figura 7 de esta pregunta 5, los empleados del Área de Sistemas de la empresa no están recibiendo una capacitación adecuada en cuanto a ciberseguridad, ya que solo el 23.1% de los encuestados aseguran haber recibido algún tipo de orientación sobre temas de seguridad. (Ver Figura 7)

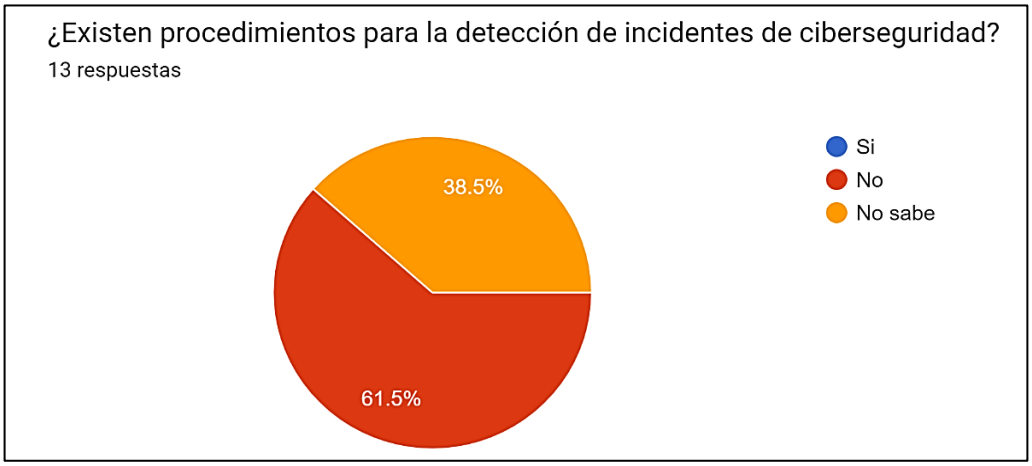
Figura 7. Pregunta 5: Capacitaciones en el Área de Sistemas para resolución de incidentes de seguridad.



Fuente: elaboración propia.

La Figura 8, muestra que el 61.5% de los encuestados asegura que en la organización no existen procedimientos para la detección de incidentes de inseguridad, mientras que el 38.5% no sabe si existen o no. Esto deja claro la falencia del área para el manejo de incidentes de seguridad. (Véase Figura 8)

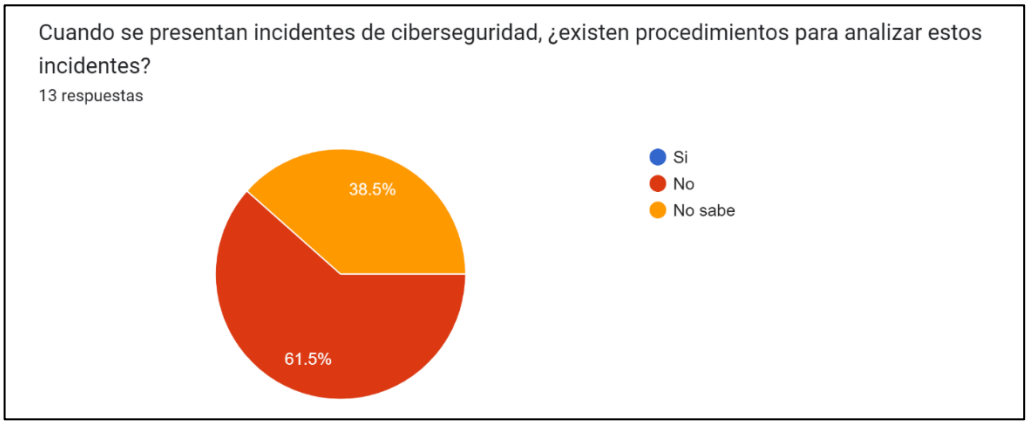
Figura 8. Pregunta 6: Existencia de procedimientos para la detección de incidentes de ciberseguridad.



Fuente: elaboración propia.

De acuerdo con la Figura 9, el 61.5% responde que no existen procedimientos para el análisis sobre los incidentes de ciberseguridad, frente a un 38.5% que no sabe si existen o no estos procesos, esto concuerda con la pregunta 6 donde también afirman que no existen procesos para la detección de estos incidentes. (Véase Figura 9)

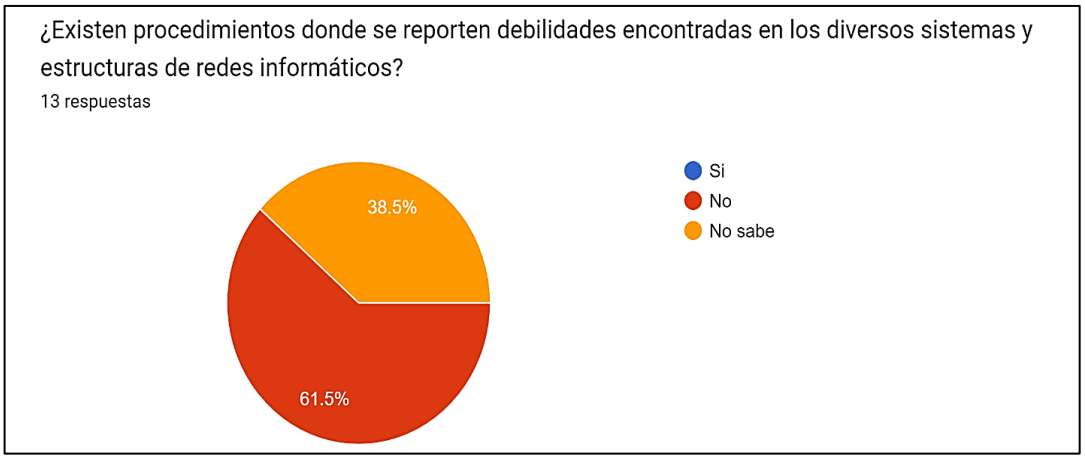
Figura 9. Pregunta 7: Existen procedimientos para analizar incidentes de ciberseguridad.



Fuente: elaboración propia.

El 61.5% de los profesionales que respondieron la encuesta, afirman que no se hace un acompañamiento de las debilidades que se encuentran dentro de la empresa, para lograr disminuir los riesgos, mientras el 38.5% no sabe si se deben reportar o debilidades encontradas en los diversos sistemas informáticos. (Véase Figura 10)

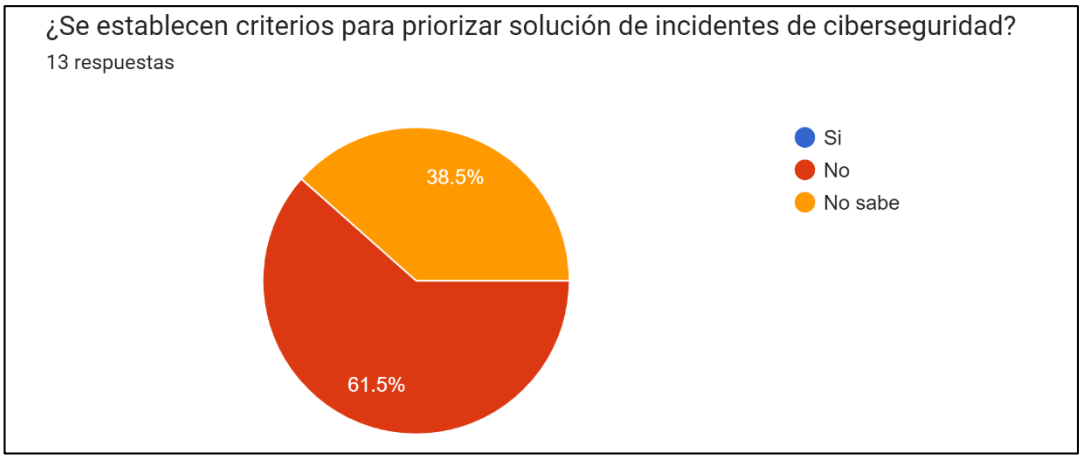
Figura 10. Pregunta 8. Procedimientos que reportan las debilidades de los diversos sistemas y estructuras de redes informáticos.



Fuente: elaboración propia.

Según la Figura 11, los encuestados afirman que dentro de la organización no se están siguiendo criterios de priorización de incidentes de ciberseguridad ya que mientras el 61.5% afirma que no existen, el 38.5% desconoce la existencia de dichos criterios. (Véase Figura 11)

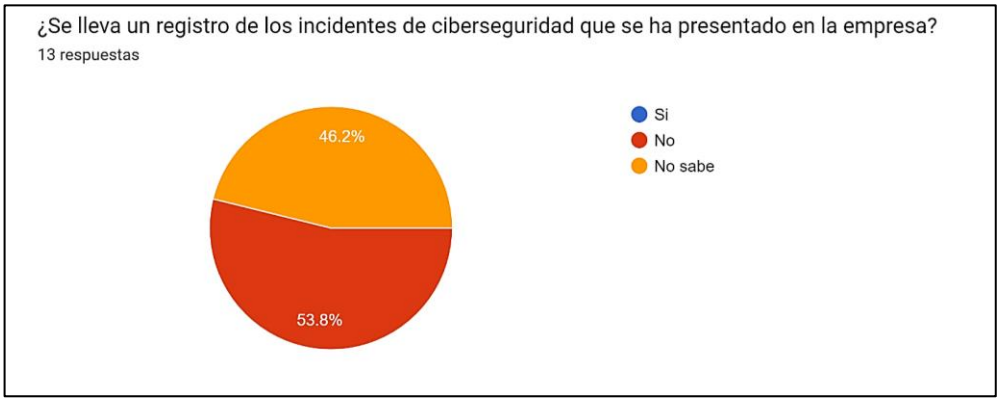
Figura 11. Pregunta 9: Criterios para priorizar solución de incidentes de ciberseguridad.



Fuente: elaboración propia.

En la Figura 12 se observa que el 53.8% de los profesionales afirman no llevar un reporte de los incidentes de ciberseguridad que se presentan, frente a un 46.2% que afirman que desconocen si se lleva dicho registro, esto deja claro que dentro de la organización no se está llevando el debido control y registro de los incidentes de ciberseguridad que se puedan presentar. (Véase Figura 12)

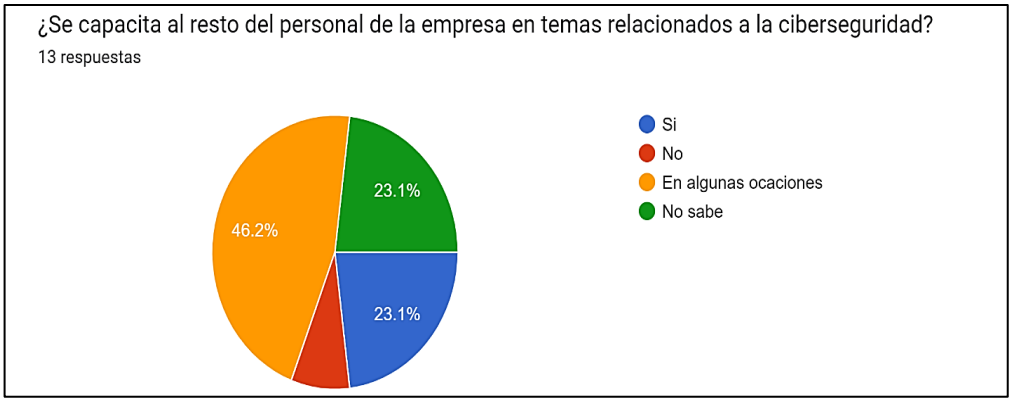
Figura 12. Pregunta 10: Registro de los incidentes de ciberseguridad que se han presentado en la empresa.



Fuente: elaboración propia.

Tan solo el 23.1% de los profesionales del Área de Sistemas de la organización, afirman capacitar al personal de la empresa en temas de ciberseguridad, la mayoría de ellos realizan estas capacitaciones esporádicamente ya que el 46.2% de los encuestados responde que en algunas ocasiones se realizan este ejercicio, mientras que el 30.7% asegura que no se realizan o no saben si se realizan dichas capacitaciones. (Véase Figura 13)

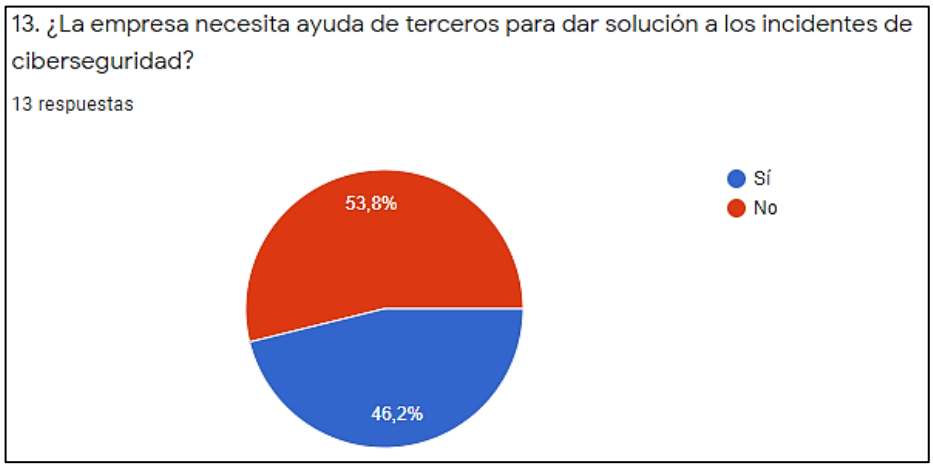
Figura 13. Pregunta 11: Capacitación al resto de personal de la empresa en temas de ciberseguridad.



Fuente: elaboración propia.

El 53.8% afirma que la empresa no busca ayuda para lograr solucionar los incidentes de ciberseguridad, frente al 46.2% que dice que se apoya en terceros para solucionar todo tipo de incidente cibernético que se presente dentro de la organización. (Véase Figura 14)

Figura 14. Pregunta 12: Ayuda a la empresa de terceros para solucionar incidentes de ciberseguridad.



Fuente: elaboración propia.

6.1.3 Análisis de resultados. De los resultados obtenidos mediante la encuesta como se muestra es las figuras anteriores, la encuesta aplicada al gerente y profesionales de sistemas de la empresa Proyectos de Inversión Vial Andino S.A.S, estuvo conformada por 12 preguntas en la que se buscó se puede deducir que esta área actualmente no posee un modelo para la gestión de incidentes de ciberseguridad, cabe resaltar que dentro de la empresa está en proceso de elaboración e implementación el sistema de gestión de seguridad de la información, tal como lo expresan los encuestados en la pregunta número tres, sin embargo analizando las respuestas del personal del área, es notorio la falta de implementación de este en temas de incidentes de ciberseguridad, ya que no está claro o definido una persona encargada de la gestión de los incidentes de ciberseguridad, no poseen actualmente procesos de detección y análisis de incidentes, no se lleva el control de debilidades encontradas en los diversos sistemas de información, no existe un procedimiento para priorizar incidentes de ciberseguridad, es muy poca la capacitación que se hace al personal del Área de Sistemas y al resto del personal de la organización sobre ciberseguridad.

Esto es una debilidad preocupante que afecta la seguridad de los sistemas de información, dejando una brecha grande al momento de abarca cada uno de los incidentes en ciberseguridad que se presenten referente a los delitos informáticos

en cada uno de los activos de la información; como lo son la perdida y sustracción de información afectando la integridad y disponibilidad de la misma, alteración en la confidencialidad de la información, afectación en la seguridad en los equipos físicos, entre otras, dejando al Área de Sistemas sin la posibilidad de abarcar el soporte a todos los servicios de tecnología de la información (TI) necesarios para el adecuado control de la infraestructura tecnológica de la organización.

Por otra parte, los encargados del Área de Sistemas manifiestan que no tienen un formato para informar acerca de los riesgos, vulnerabilidades, debilidades que se presentan dentro de la ejecución de los procesos trayendo como consecuencia la no medición en el nivel de riesgo que estos causan al momento de que se presente una vulnerabilidad ya que al no contar con un modelo que gestione cualquier suceso y ayude a reducir los riesgos y/o vulnerabilidades que se puedan presentar de ciberseguridad, pueden tener más posibilidades de que a futuro se generen nuevos ataques al momento de realizar algún proceso sistemático dentro de la empresa.

7. FASE II – PRINCIPALES RIESGOS INHERENTES

7.1 IDENTIFICACIÓN DE LA ORGANIZACIÓN

En el Anexo B se encuentra el organigrama general de la organización Proyectos de Inversión Vial Andino, donde se identifica cada uno de los cargos del personal interno de la organización. (Véase Anexo B)

7.2 INVENTARIO DE LA EMPRESA

Para lograr identificar los principales riesgos y vulnerabilidades que tiene la empresa, primero se debe realizar un inventario para lograr saber los activos informáticos con qué cuentan, su clasificación, y su tipo para que se le pueda dar su importancia en cada uno de los procesos en los cuales apoyan.

Cabe resaltar que cada uno de los activos de la información de la empresa, son fundamentales para la ejecución de los procesos dentro y fuera de ella, por ese motivo se establece un nivel de criticidad para darle importancia a cada uno de ellos en cuanto a la protección y el nivel de seguridad que debe tener dentro del área de trabajo de cada uno de los responsables.

Tabla 1. Nivel de criticidad

Criticidad	Puntuacón	Especificación
ALTA	DE 8 A 15	Dos o todas las propiedades altas
MEDIA	DE 5 A 3	Al menos una propiedad alta o las tres medias
BAJA	MENOR QUE 3	Todas las propiedades bajas

De acuerdo con el impacto que tenga cada uno de los sucesos que se presentan se clasifican con los siguientes niveles: Criticidad Alta, Criticidad Media, Criticidad Baja.

Fuente: elaboración propia.

Tabla 2. Inventario Hardware y Software

Id	Proceso	Nombre del activo	Tipo	Clasificación			Criticidad	
				Confidencialidad	Integridad	Disponibilidad		
001	Todos los procesos	Servidor Work Manager / SO Windows server R8 2002	Hardware	5	5	4	10	Alta
002	Todos los procesos	Servidores NAS / SO Windows server R8 2002	Hardware	5	5	3	10	Alta
003	Almacén, Contabilidad, Compras, Costos y Presupuesto, Construcción	Software SAP / Subcontratado por Claro/ Servidor en la nube	Software	5	5	5	10	Alta
004	Todos los procesos	Antivirus	Software	5	5	5	10	Alta
005	Departamento Técnico	Equipos LAN	Hardware	5	5	5	10	Alta
006	Departamento Técnico	Equipos WAN	Hardware	5	5	5	10	Alta
007	Departamento Técnico	VPN / 30 licencias	Software	5	5	5	10	Alta
008	Departamento Técnico	Firewall Fortinet	Software	5	5	5	10	Alta
009	Departamento Técnico	Gestor de correo electrónico / contratado Outlook 365	Software	5	5	5	10	Alta
010	Departamento Técnico	sistema de alimentación ininterrumpida	Hardware	1	5	5	6	Media

011	Departamento Técnico	Equipos de Cómputo (250 equipos entre portátiles y de escritorio / SO Windows 10 licenciado)	Hardware	5	5	5	10	Alta
012	Departamento Técnico	Red Seguridad perimetral / cámaras de seguridad y lector de huellas para accesos.	Hardware	4	4	3	8	Alta
013	Talento Humano	Software gestión de recursos humanos	Software	4	4	4	8	Alta
014	Talento Humano	Personal	Recurso Humano	4	4	4	8	Alta
015	Servicios	Software propio	Otros	4	4	5	8	Media
016	Servicios	Paquete office	Software	4	5	4	9	Media

Fuente: elaboración propia

Proyectos de inversión vial andino S.A.S, cuenta con una variedad de softwar, equipos de cómputo y activos de la información, para los procesos de contabilidad, recursos humanos, costos y presupuestos de obra, construcción, maquinaria y equipos, almacén, área socio ambiental, jurídica, y sistemas, donde se elaboran diversos informes de movimientos financieros, económicos y operacionales que son propios de la gestión de obras civiles.

7.3 NIVELES DE RIESGOS DE LA EMPRESA

Después de realizar la compilación del inventario de todos los equipos informáticos que existen en la empresa, se determina cuál de estos activos al no funcionar correctamente pueden afectar el rendimiento de las actividades que se están ejecutando dentro de la organización, con el fin de obtener el nivel del riesgo

mediante la relevancia que tiene cada uno de los activos, y a su vez que tanto cada activo dependa de otros si no se salva guarda la información recolectada.

También se relacionan las principales amenazas que afectan el riesgo en la empresa ya que no está exenta de que pueda suceder alguna catástrofe como lo son (desastres naturales, incendios, tormentas, entre otros), se debe recopilar esa información y medir cual es el índice en el que puede afectar directa o indirectamente los procesos o actividades que se realizan por parte de la empresa.

En primer lugar, se determina para cada uno de los activos, cuáles son las actividades que realizan dentro de la empresa, y se determina que peligro puede presentarse en cada uno de estos activos (suceso), para poder determinar si cada suceso presenta un nivel de riesgo alto o bajo, se debe clasificar según el impacto que generé dentro de la organización que este suceso ocurra y la probabilidad que exista de que este suceso ocurra dentro de la infraestructura tecnológica de la organización, para asignar valores a estos criterios de toman como base tablas de valores número tres y cuatro basadas en la Norma ISO 73:2009.

Para determinar los niveles del riesgo: se estructura de acuerdo con lo estipulado por la norma ISO 73:2009, donde para cada suceso se obtiene un valor que se obtiene del impacto que tenga por la probabilidad de que exista el suceso o el evento previamente estipulados, y según la tabla número 5 el valor obtenido determinará el nivel del riesgo de cada uno.

Tabla 3. Valores de Impacto

Categoría	Nivel
Catástrofe	9-10
Alto	7-8
Medio	5-6
Bajo	3-4
Relevante	1-2

Fuente. Basados en la norma ISO 73:2009

Tabla 4. Niveles de Probabilidad

Probabilidad	Nivel
Constante	5
Moderada	4
Ocasional	3
Posible	2
improbable	1

Fuente. Basados en la norma ISO 73:2009

Tabla 5. Valores de rango

Nivel	Rango Valor del nivel
Critico	50
Alto	30-49
Medio	10-36
Bajo	0-10

Fuente. Elaboración propia.

7.4 IDENTIFICACIÓN DE RIESGOS

En el Anexo B, se presenta la matriz de riesgos asociada a la identificación de vulnerabilidades (véase Anexo B), resumido en:

Tabla 6. Riesgo R1.

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
INFRAESTRUCTURA	R1	Fuga de datos por acceso sin credenciales.	MAYOR	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 7. Riesgo R2

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
SERVIDORES NAS	R2	Sustracción de información por acceso no autorizado a bases de datos por la práctica inoportuna del beneficiario y contraseña de ingresos a bases de datos.	CATASTRÓFICO	MODERADO	**ALTO**

Fuente: elaboración propia.

Tabla 8. Riesgo R3.

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
SERVIDORES NAS	R3	Sustracción de información por el manejo inoportuno de privilegios y usuarios en bases de datos	CATASTRÓFICO	MODERADO	**ALTO**

Fuente: elaboración propia.

Tabla 9. Riesgo R4

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
SERVIDORES NAS	R4	Perdida de datos por ataques del exterior	CATASTRÓFICO	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 10. Riesgo R5

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
SERVIDORES NAS	R5	Pérdidas económicas por fallas en servidores donde se almacenan las bases de datos	CRÍTICO	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 11. Riesgo R6

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
SERVIDORES NAS	R6	Causa de fuerza mayor	MAYOR	CONSTANTE	**ALTO**

Fuente: elaboración propia.

Tabla 12. Riesgo R7

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
GESTOR DE CORREO ELECTRÓNICO	R7	Ataques cibernéticos ocasionados por correos electrónicos	MAYOR	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 13. Riesgo R8.

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
PAQUETE OFIOMÁTICO	R8	Mal uso de las herramientas ofimáticas	MENOR	POSIBLE	**BAJO**

Fuente: elaboración propia.

Tabla 14. Riesgo R9

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
SOFTWARE SAP	R9	Privilegios y accesos no autorizados, ataques informáticos	MAYOR	CONSTANTE	**ALTO**

Fuente: elaboración propia.

Tabla 15. Riesgo R10.

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
Recursos tecnológicos	R10	Malas conexiones en la infraestructura tecnológica	MAYOR	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 16. Riesgo R11

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
SERVIDOR WORK MANAGER	R11	Acceso no autorizado	CATASTRÓFICO	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 17. Riesgo R12

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
ANTIVIRUS	R12	No protección contra códigos maliciosos	MAYOR	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 18. Riesgo R13

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
Seguridad de Red	R13	Limitación del proceso	MAYOR	OCASIONAL	**MEDIO**

Fuente: elaboración propia.

Tabla 19. Riesgo R14

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
EQUIPOS LAN	R14	Robo y eliminación de datos.	MAYOR	OCASIONAL	**MEDIO**

Fuente: elaboración propia.

Tabla 20. Riesgo R15

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
EQUIPOS WAN	R15	Perturbación del proceso.	MAYOR	OCASIONAL	**MEDIO**

Fuente: elaboración propia.

Tabla 21. Riesgo R16

Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
RECURSOS HUMANOS	R16	Ingeniería social	MAYOR	POSIBLE	**MEDIO**

Fuente: elaboración propia.

Tabla 22. Riesgo R17

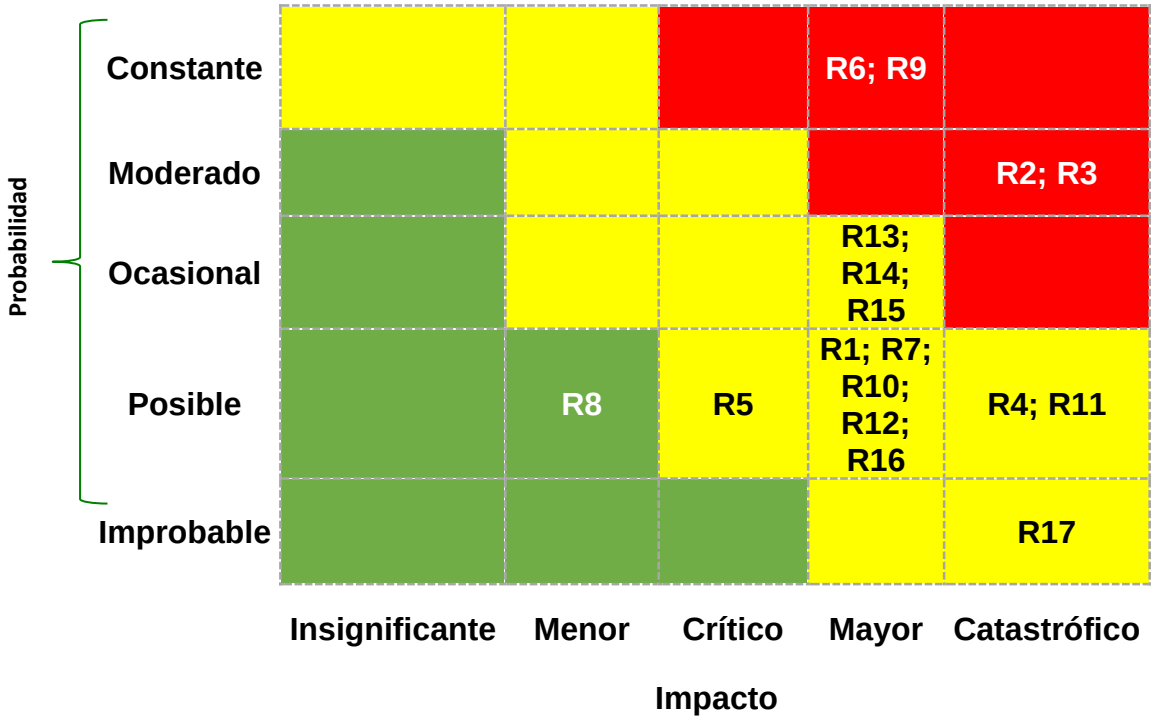
Servicio	#	Suceso	IMPACTO	OCURRENCIA	NIVEL
EVENTOS NATURALES	R17	Perdida de equipos y daños en las instalaciones por eventos naturales	CATASTRÓFICO	IMPROBABLE	**MEDIO**

Fuente: elaboración propia.

7.5 MATRIZ DE RIESGOS

En la Figura 15 se presenta el mapa donde se deja ver en qué escala se encuentra cada uno de los riesgos identificados, con el fin de determinar las acciones a seguir para disminuir al máximo el nivel en el que se encuentra cada uno y así alcanzar un alto grado de madurez en seguridad informática. (Ver Figura 15)

Figura 15. Mapa de Riesgo.



Fuente. Elaboración propia.

8. FASE III: MODELO PARA LA GESTIÓN DE INCIDENTES QUE APORTE A LA ORGANIZACIÓN BASES PARA INCLUIR DENTRO DEL SGSI.

8.1 NIVEL DE CONFIDENCIALIDAD

Se plantea una estructura para ser empleada dentro de la empresa, la cual establezca el nivel de seguridad adecuado para preservar los activos informacionales de la empresa y el cómo debe ser su clasificación dándole una prioridad y un nivel de criticidad al documento. Por eso se sugiere los siguientes criterios para clasificar la información:

Tabla 23. Clasificación de documentos

Nivel de Confidencia	Nivel de Integridad	Nivel de Disponibilidad
Reservado	Alto	Bajo
Clasificado	Medio	Medio
Pública	Bajo	Alto

Fuente: elaboración propia.

Tabla 24. Clasificación de los niveles para la información

Alto	Toda información que tenga en su nivel de integridad y su nivel de disponibilidad Alto.
Medio	Toda información que tenga en un nivel alto y en su nivel de disponibilidad medio.
Bajo	Toda información que el nivel de integridad sea bajo no necesitará de permisos y será pública.

Fuente: elaboración propia.

Con lo anteriormente expuesto es de suma importancia comenzar a implementar esta clasificación de la información para darle un uso adecuado y avanzar en la disminución de perdida de información. Sin embargo, lo más importante es mejorar los procesos en la administración de los incidentes que se puedan presentar para tener una mejor organización con los activos de la información y lograr determinar responsabilidades al momento de delegar funciones para cada uno de los procesos.

8.2 PROCESO DE GESTIÓN DE INCIDENTES

Para tener claridad en relación con la gestión de incidentes se debe establecer una estructura y unos principios que apoyen a la resolución de cualquier evento o amenaza que suceda el cual ocasione que un proceso o servicio que se preste falle o se detenga. Esta estructura brindará un adecuado manejo a estos riesgos de una manera rápida y eficiente dentro de lo posible para que sigan con normalidad los servicios y/o procesos que se realicen en la empresa.

En este apartado se incluirá una guía o serie de pasos de buenas prácticas, el cual servirán de apoyo a los profesionales encargados de poner en marcha las respuestas y enfrentar la mayoría de incidentes de ciberseguridad que se presenten. El personal encargado debe encargarse de realizar los siguientes procesos:

- Realizar un análisis periódico de los riesgos que se han presentado mínimo una vez por año.
- Planear auditorias basadas en la ISO 27002:2013, que muestre el estado actual en el que se encuentran los controles sobre los activos de la información.
- Realizar simulacros sobre la seguridad de la empresa, mínimo una vez cada seis meses.
- Realizar controles sobre los activos de la información y las plataformas tecnológicas.
- Capacitación a los empleados periódicamente sobre seguridad de la información.
- Dentro del grupo de profesionales en el Área de Sistemas debe existir un oficial o gerente de seguridad informática, encargado de gestionar de manera adecuada la implementación de todo el sistema de gestión de seguridad de la información incluyendo el modelo para la gestión de incidentes en ciberseguridad planteado.

8.3 CLASIFICACIÓN EVENTOS DE CIBERSEGURIDAD

Se deben clasificar los eventos que se están presentando donde se esté poniendo en riesgo algún proceso informacional de la empresa, esta clasificación de los eventos permitiría preservar la operación de la organización y mitigar las amenazas que puedan afectar los activos de información. (Véase Tabla 25)

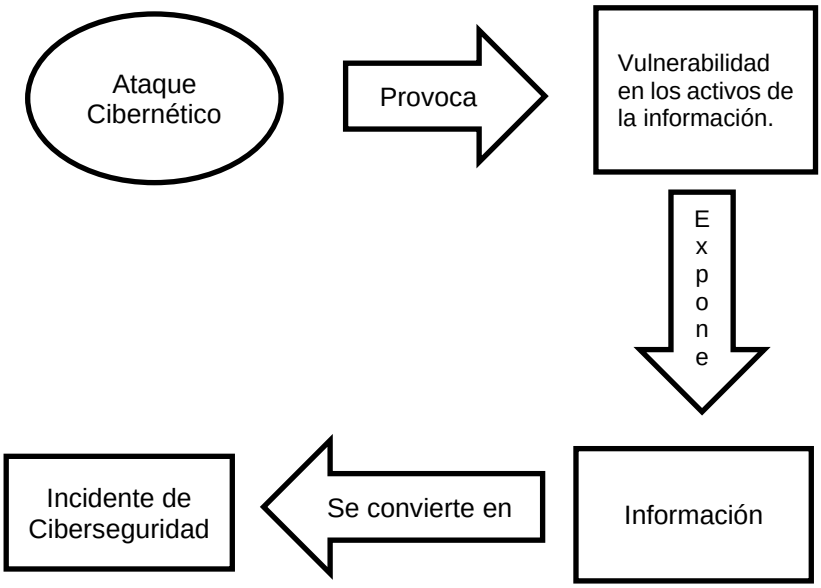
Tabla 25. Incidente Ciberseguridad

NOTA: Un incidente de Ciberseguridad o en la seguridad de la información a pesar de que conlleve a una vulneración de la confidencialidad, integridad o

disponibilidad, puede verse como un aprendizaje que ayude a fortificar la seguridad física e interna de la empresa. Aunque lo importante es prevenir que estos incidentes sucedan, ya que debemos velar por el buen funcionamiento de la organización y porque la información siempre este salvaguardada.

Fuente: elaboración propia.

Figura 16. Estructura incidente.



Fuente: elaboración propia. Basada en ISO 27001:2013 Inciso A16.

8.4 CARACTERIZACIÓN DE INCIDENTES DE CIBERSEGURIDAD

Como se explicó inicialmente se debe tener claro cuáles son los activos de la información con los que cuenta la empresa, la valoración que tiene cada uno de estos activos y las amenazas que se pueden presentar, este análisis permite establecer el tipo de vulnerabilidades, eventos o incidentes que pueda afectar la información valiosa de la empresa.

En la Tabla 26, se estipulan una serie de posibles amenazas, riesgos u otro tipo de evento de ciberseguridad que pueda alterar el correcto funcionamiento en los procesos o servicios dentro de la empresa:

Tabla 26. Identificaciones posibles incidentes.

No.	Incidente
1.	Manipulación malintencionada de los activos de la información.
2.	Alteración de la configuración en los equipos de cómputo.
3.	Suplantación de usuario.
4.	Alteración de privilegios de usuario final.
5.	Acceso no autorizado a los equipos de cómputo.
6.	Insertar software malicioso o dañino (virus, gusanos, malware, troyanos)
7.	Acceso no autorizado a las oficinas.
8.	Alteración intencional de documentos o información.
9.	Eliminar información.
10.	Sustracción y robo activos de información
11.	Ataques de denegación en los servicios (Dos y DDoS).
12.	Explotación de una debilidad en un sistema.
13.	Ataque Rasomware dentro de los equipos de cómputo.
14.	Alteración en las contraseñas de los usuarios.
15.	Recepción de correos electrónicos no deseados.
16.	Alteración en las redes LAN o WAN. (Modificación de IP)

Fuente: elaboración propia.

Es importante identificar los incidentes de seguridad informática a los que está expuesta la empresa, ya que esto nos permite tener claro las vulnerabilidades y riesgo que corre el sistema informático implementado, con el fin de fortalecer estas debilidades y lograr proteger al sistema y a la información que se maneja. Podemos clasificar de cierta forma los riesgos que están sucediendo y generar un reporte de tal manera que sirva como base para poder resolver estos incidentes, y a futuro poder generar una investigación el cual permita a la empresa tomar decisiones, medidas y precauciones para que no vuelva a suceder ninguno de estos sucesos, y a su vez, el personal del Área de Sistemas se encuentre capacitado para enfrentarse a este tipo de situaciones.

8.5 GESTIÓN DE REPORTE DE INCIDENTES

El oficial de seguridad de la información deberá hacer conocer y/o capacitar al personal de la empresa para lograr rellenar de manera adecuada en el formato de reportes de incidentes el riesgo que se ha presentado, lo que permite tener un historial que pueda servir de investigación a futuro para aumentar la seguridad, mitigar el impacto que ha generado o contrarrestar en el menor tiempo posible la solución del mismo, el formato que se propone a continuación deberá ser enviado por el personal que lo diligencie al oficial de seguridad para su posterior análisis y

toma de decisiones sobre la mejor solución que se va realizar de acuerdo al riesgo presentado:

Tabla 27. Formulario reporte de incidentes

Formulario Reporte de Incidentes Proyectos de inversión vial andino S.A.S					
Nombres y Apellidos:			Oficina:		
Cargo:			E-mail:		
Celular:	Teléfono Oficina:		Extensión:		
Tipo de Contrato:	Termino Fijo:	Término Indefinido:	Contratista:		
Información sobre el incidente					
Fecha:			Hora:		
1.	Manipulación malintencionada de los activos de la información.		10.	Sustracción de información por medio de phishing.	
2.	Alteración de la configuración en los equipos de cómputo.		11.	Robo de activos de la información.	
3.	Suplantación de usuario.		12.	Ataques de denegación en los servicios (Dos y DDoS).	
4.	Alteración de privilegios de usuario final.		13.	Explotación de una debilidad en un sistema.	
5.	Acceso no autorizado a los de equipos de cómputo.		14.	Ataque de Rasomware dentro de los equipos de cómputo.	
6.	Insertar software malicioso o dañino (virus, gusanos, malware, troyanos)		15.	Alteración en las contraseñas de los usuarios.	
7.	Acceso no autorizado a las oficinas.		16.	Recepción de correos electrónicos no deseados.	
8.	Alteración intencional de documentos o información.		17.	Alteración en las redes LAN o WAN. (Modificación de IP)	
9.	Eliminar información.				
18.	Otro (describa):				
DESCRIPCIÓN:					
FIRMA:			CÉDULA:		

Fuente: elaboración propia.

Tabla 28. Formulario Reporte de Riesgos

Formulario Reporte de Riesgos Proyectos de inversión vial andino S.A.S	
Nombres y Apellidos:	Oficina:
Cargo:	E-mail:

Celular:		Teléfono Oficina:		Extensión:	
Tipo de Contrato:		Termino Fijo:	Término Indefinido:	Contratista:	
Información sobre el riesgo					
Fecha:			Hora:		
1.	Extracción o inyección de datos.		10.	Pérdida de la continuidad de las operaciones de los procesos.	
2.	Inyección o modificación de archivos maliciosos para actuar sobre los activos de la información.		11.	Daños a la reputación de la empresa mediante la exposición de información confidencial.	
3.	Capacidad limitada de almacenamiento en los equipos de cómputos.		12.	Daños a la seguridad informática implementada de la empresa como daños a firewall, a dispositivos de vigilancia, a Backus de información, entre otros.	
4.	Alteración de privilegios de usuario final.		13.	Costos financieros o sanciones debido a incumplimiento de normas o leyes de seguridad informática.	
5.	Firmware malicioso.		14.	Indisponibilidad de servicios de la empresa, como falta de suministro de internet, de respaldos energéticos a servidores, entre otros.	
6.	Phishing		15.	Fraude o robo de identidad.	
7.	Daños o pérdida de activos tecnológicos de procesamiento o almacenamiento de la organización.		16.	Pérdida de información confidencial.	
8.	Daños o pérdida de sistemas de información de la organización.		17.	Manipulación o alteración de información sensible.	
9.	Pérdida de la propiedad intelectual.				
18.	Otro (describa):				
DESCRIPCIÓN:					
FIRMA:			CEDULA:		

Fuente: elaboración propia.

8.6 CLASIFICACIÓN DE ATAQUES DE CIBERSEGURIDAD

Al momento de que se recibe el reporte por parte del responsable del Área de Sistemas que lo realizó, el oficial de seguridad quien recibe este reporte debe clasificar el incidente o riesgo de tal manera, que se pueda priorizar la manera en responder cada uno de esos sucesos de una forma rápida y efectiva dentro de cada proceso de la empresa, a continuación, se muestra el criterio de evaluación atendiendo lo estipulado en la guía de gestión de incidentes del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), de acuerdo con todas la infraestructura tecnológica, los riesgos inminentes y la criticidad que tiene cada uno de los activos en cada uno de los incidentes:

Tabla 29. Clasificación ataques

Clasificación de ataques	
Nombre	Descripción
Acceso no autorizado a los equipos de computo	Toda persona que intente suplantar la identidad del personal de la empresa, intente abusar de los privilegios de acceso a los equipos informáticos que se le ha dado, interceptación de la información que se reúna dentro de la empresa.
Modificación en los activos de la información	Toda persona que intente implantar código malicioso que ponga en riesgo la integridad y el servicio dentro de la empresa, manipulando las configuraciones y/o destruyendo información.
Que impidan la realización de los procesos	Toda persona que altere el acceso a los servicios del personal, cause deficiencias en la empresa, y de manera mal intencionada vulnere las aplicaciones que se utilizan dentro de la empresa.
Multipropósito	Sucesos de varios incidentes el cual se involucren de una u otra manera para que no se logre el correcto funcionamiento de la empresa, ya sea realizando ingeniería social, difusión de softwares maliciosos como lo son los virus, gusanos, etc., incendios, daños por desastres naturales.

Fuente: elaboración propia.

8.6.1 Impacto de los eventos. Cada evento que se presenta tiene un impacto dentro de la empresa el cual se estipula un rango para cada uno de los niveles como se exponen en la Tabla 30.

Tabla 30. Rango en el impacto de los eventos.

Nivel	Rango	Incidente
Muy Alta	5	Todo evento catastrófico que afecte directamente los activos de la información de la empresa. Debe ser atendido de inmediato.
Alta	4	Todo evento que altere o vulnere la imagen y el nombre de la empresa, involucrándolos en temas legales. Debe ser atendido de inmediato.
Media	3	Todo ataque moderado o intento de hackeo en los equipos de cómputo de la empresa.
Baja	2	Incidentes que afecten de manera insignificante y que no retrasen la realización de los procesos.
Muy Baja	1	Estos incidentes deben ser monitoreados con el fin de que no aumente su rango y se logren controlar y reforzar para que no vuelvan a suceder.

Fuente: elaboración propia.

8.6.2 Asignación incidentes vs impacto

Tabla 31. Asignación Incidentes vs Impacto.

No.	Incidente	Clasificación	Rango
1.	Manipulación malintencionada de los activos de la información.	Modificación en los activos de la información	Muy alta
2.	Alteración de la configuración en los equipos de cómputo.	Acceso denegado	Media
3.	Suplantación de usuario.	Acceso denegado	Media
4.	Alteración de privilegios de usuario final.	Acceso denegado	Alta
5.	Uso no autorizo de equipos de cómputo.	Acceso denegado	Alta
6.	Insertar software malicioso o dañino (virus, gusanos, malware, troyanos)	Modificación en los activos de la información	Media

7.	Acceso no autorizado a las oficinas.	Acceso denegado	Muy alta
8.	Alteración intencional de documentos o información.	Modificación en los activos de la información	Muy alta
9.	Eliminar información.	Modificación en los activos de la información	Muy alta
10.	Sustracción de información por medio de phishing.	Que impidan la realización de los procesos	Muy alta
11.	Robo de activos de la información.	Que impidan la realización de los procesos	Muy alta
12.	Ataques de denegación en los servicios (Dos y DDoS).	Que impidan la realización de los procesos	Baja
13.	Explotación de una debilidad en un sistema.	Acceso denegado	Muy baja
14.	Implementación de Rasomware dentro de los equipos de cómputo.	Que impidan la realización de los procesos	Media
15.	Alteración en las contraseñas de los usuarios.	Acceso denegado	Alta
16.	Recepción de correos electrónicos no deseados.	Multipropósito	Media
17.	Equipos de cómputo sin protección antivirus.	Que impidan la realización de los procesos	Muy baja
18.	Alteración en las redes LAN o WAN.	Multipropósito	Media

Fuente: elaboración propia.

8.7 FORMATO DE REPORTE DE VERIFICACIÓN DE INCIDENTES

Tabla 32. Reporte de Verificación

REPORTE DE PRUEBAS Y RESULTADOS				
EMPRESA	**ÁREA AUDITADA**	**FECHA**		
Objetivo:				
PRUEBA No. X				
ÁREA AUDITAR:				
Prueba:				
Objetivo:				
Técnica:				
Tipo de Prueba:	Cumplimiento Sustantiva Doble Finalidad			
Procedimiento a Emplear:				
Recursos:				
RESULTADOS DE LA PRUEBA				
Hallazgos				
Causa				
Situación de Riesgo que genera				
Recomendaciones de Auditoria				
Fecha				
Elaborado por				
Revisado por				

Fuente: elaboración propia.

8.8 LISTA DE CHEQUEO DE INCIDENTES

Tabla 33. Chequeo de incidentes.

LISTA DE CHEQUEO				
EMPRESA/ÁREA		**RESPONSABLE**	**FECHA**	
Objetivo:				
No	**Preguntas**	**Cumple**	**No Cumple**	**Observación**
	A. Acceso físico			
1	¿Existen mecanismos de identificación al personal que ingresa a la empresa?			
2	¿Existe señales que alerten sobre las áreas sensibles y su localización como lo son los Sistemas de CCTV (Circuitos cerrados de cámaras de vigilancia)?			
3	¿Existen controles de acceso a la infraestructura física de la empresa, por medio de registro en sistemas de información?			

	B. Inventario Hardware			
5 **6** **7** **8**	¿Existe un formato de inventario donde se especifique el hardware utilizado en la organización? ¿Cuenta el inventario con codificación de activos para los dispositivos y/o periféricos? ¿Existe un mecanismo mediante personal autorizado y formatos establecidos que permitan controlar la salida de dispositivos del área donde son asignados? ¿Se lleva el control de activos hardware faltantes?			
	C. Plan de Emergencia activos de la información			
11 12 13	¿Existe un plan de Emergencia que ayude a la solución de ataques cibernéticos? ¿Están contempladas las normas de acción en manuales o procedimientos ante situaciones de ataques cibernéticos? ¿En la empresa se realizan Backups (Copias de seguridad), como metodo de prevención en caso de que suceda algún ataque a los sistemas de la información?			

14	¿Se realizan capacitaciones para la generación de contraseñas seguras dentro de la empresa?			
	D. Circuitos Eléctricos			
16	¿Existe revisión periódica por parte de un trabajador o contratista de las instalaciones eléctricas?			
17	¿Los circuitos eléctricos están certificados y cumplen con algún tipo de estándar?			
18	¿Se han presentados fallos eléctricos como cortos circuitos dentro de la organización?			
19	¿Se tienen debidamente ubicados y señalados los extintores dentro de las instalaciones de la empresa?			
20	¿Los diferentes interruptores y conectores de energía cumplen en su instalación con estándares de seguridad?			

Fuente: elaboración propia.

9. CONCLUSIONES

Al realizar un examen del estado actual de los riesgos inherentes en el que se encuentra la empresa Proyectos de Inversión Andino S.A.S, teniendo en cuenta el dominio A16 de la norma ISO 27002:2013. Mediante el cual, a través de una encuesta se logró conseguir información sobre las debilidades tales como que el personal no está capacitado y los profesionales no cuentan con las destrezas adecuadas para identificar ataques de ciberseguridad y/o lograr gestionar respuestas de manera rápida y efectiva, afectando así la manera en el que se despliegan los procesos dentro de la empresa y los activos de la información.

Luego de realizar el examen y con la intención de lograr hallar las debilidades, las amenazas y riesgos, se realiza un análisis de los principales riesgos de ciberseguridad existentes para lograr determinar un modelo que contribuya a minimizar los riesgos dentro de la empresa, tomando elementos pertinentes en cada una de las fases propuestas, el cual sirve para lograr la construcción de una guía de buenas prácticas y establecer los mecanismos para la gestión de los reportes de incidentes y riesgos dentro de la empresa.

Teniendo en cuenta los tipos de incidentes y riesgos de seguridad para los activos de la información que se identificaron para la empresa Proyectos de Inversión Andino S.A.S, se recomienda utilizar los recursos (Formato de reportes de incidentes, Formato de reportes de Riesgos y Lista de chequeo), por este motivo el proceso debe ser escalable a medida que se van fortaleciendo las debilidades encontradas, en el cual se diseña en la Fase III de este proyecto, un modelo como guía para la prevención, atención y dar respuesta de manera eficiente a las vulnerabilidades y riesgos de ataques de ciberseguridad que se presenten en la empresa.

10. RECOMENDACIONES

- Los resultados obtenidos con este trabajo de especialización sirven de fundamento para la implementación un modelo para la gestión de incidentes en ciberseguridad basado en la norma ISO27002:2013, dentro de cualquier empresa que desee tomarlo como base, el cual servirá de apoyo para la optimización de la prestación de los servicios de TI.

- El modelo de gestión de incidentes propuesto debe ser aplicado por un profesional que esté capacitado o certificado en la Norma, el cual tenga experiencia en cuanto a ciberseguridad, seguridad informática o temas afines con la protección de datos.

- Este proyecto de investigación puede formar parte de investigaciones futuras, además de servir como referente para el mercado local o colombiano, donde puedan apoyarse para lograr estructurar un esquema sólido y funcional para resolver incidentes de ciberseguridad.

BIBLIOGRAFÍA

ACOSTA, UBAQUE, Nubia Esperanza y LEÓN PATIÑO, Tania Kruskaya. Diseño del sistema de gestión de seguridad de la información (S.G.S.I) para el centro de datos de la personería de Bogotá D. C bajo las Normas NTC ISO IEC 27001:2013 y NTC ISO IEC 27002:2013. Bogotá, D. C., 2017, 219p. Trabajo de grado (especialización en Seguridad Informática). Universidad Nacional abierta y a Distancia – UNAD, Escuela de Ciencias Básicas, Tecnología e Ingeniería.

CANO, Jeimy. (2016). Fraude informático: viejos trucos, nuevos entornos. En: ACIS. No. 139 (jul, 2016).

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. Protección de la información y de los datos. {En línea} {5 de mayo del 2021} disponible en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

_____. Ley 1928 del 24 julio de 2018: convenio sobre la Ciberdelincuencia, {En línea} {5 de mayo del 2021} disponible en: http://es.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

_____. Ley 23 de 1982. Sobre derechos de autor. Bogotá, D. C.: Diario Oficial No. 35.711 de 27 de febrero de 1981.

DELVASTO RAMÍREZ, Ramiro Andrés. Modelo de gestión de incidentes de seguridad de la información para Pymes. Bogotá, D. C., 2016, 64p. Tesis de Grado (especialización en Seguridad Informática), Universidad Nacional Abierta y a Distancia (UNAD), Escuela de Ciencias Básicas, Tecnología e Ingeniería.

ESTADOS UNIDOS. FEDERAL TRADE COMISSION. Ciberseguridad para pequeños negocios. Que es y cómo funciona el marco de ciberseguridad del NIST. {En línea} {3 de mayo de 2021} disponible en: {https://www.ftc.gov/es/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework-es.pdf}

ESTADOS UNIDOS. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Marco para la mejora de la seguridad cibernética en infraestructuras críticas. 2018. {En línea} disponible en: {https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf}

FAJARDO DÍAZ, Carmen Elizabeth. Análisis de los riesgos de seguridad de la información de un aplicativo de gestión documental líder en el mercado colombiano. Bogotá, D. C., 2017. 73p. Trabajo de grado (especialización en Seguridad de la Información). Institución Universitaria Politécnico Gran Colombiano, Facultad de Ingeniería y Ciencias Básicas.

GARCÍA JAY. Cibercrimen le cuesta a Colombia más de $190 mil millones de pesos al año. {En línea} 26 de junio del 2015, párr. 10 {Entrevistado por el diario El Tiempo} Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/cibercrimen-le-cuesta-a-colombia-190-000-millones-de-pesosal-ano-380830

GÓMEZ ORJUELA, Fredy Humberto y VALENCIA VALENCIA, Héctor Fernando. Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa. Medellín, 2021, 246p. Trabajo de grado (magíster en Seguridad Informática). Instituto Tecnológico Metropolitano, Facultad de Ingeniería.

GONZÁLEZ DÍAZ, Jorge Eliécer y PARRADO RODRÍGUEZ, Víctor Alfonso. Guía de gestión de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación – OTIC del Ministerio de Salud y Protección Social, tomando como base la norma ISO 27001:2013. Bogotá, D. C., 2016, 231p. Tesis de grado (especialización en Seguridad Informática), Universidad Piloto de Colombia, Facultad de Ingenierías.

GONZÁLEZ, Pepe. COBIT 2019 — El nuevo modelo de gobierno empresarial para información y tecnología. {En línea} {3 de mayo del 2021} disponible en {https://ppglzr.medium.com/cobit-2019-el-nuevo-modelo-de-gobierno-empresarial-para-informaci%C3%B3n-y-tecnolog%C3%ADa-a7bf92b7288b}

GUZMÁN FLÓREZ, Camilo Alfonso y ANGARITA PINZÓN, Cristián Andrés. Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá. Bogotá, D. C., 2017, 79p. Trabajo de grado (Especialización en seguridad de la información). Universidad Católica de Colombia, Facultad de Ingeniería.

GUZMÁN SOLANO. Sandra. Guía para la implementación de la Norma ISO 27032. Bogotá, D. C., 2019, 69p. Trabajo de grado (especialización en Seguridad de la Información), Universidad Católica de Colombia, Facultad de Ingeniería.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity. {On line} 2012 available in: {https://www.iso.org/standard/44375.html}

_____. ISO/IEC 7498-1. Information technology Open System Interconection. {On line} 2000 available in {https://www.iso.org/ics/35.100/x/}

SANTIAGO, Enrique Jesús y SÁNCHEZ ALLANDE, Jesús. Riesgos de ciberseguridad en las empresas. En: Revista de Ciencia, Tecnología y Medio Ambiente, (2017); p. 1-33.

NATIONAL INSTITUTE OF ESTÁNDARES AND TECHNOLOGY (NITS). Marco de ciberseguridad. NIST. Nuevo en Framework. {En línea} 2018 {3 de junio del 2021} disponible en {https://www.nist.gov/cyberframework/new-framework}

NOVOA GUTIÉRREZ, Edwin Alberto. Ingeniería Social como delito informático en las grandes empresas colombianas. Bello, Antioquia, 2018. 58p. Trabajo de grado (especialización en Seguridad Informática) Universidad Nacional Abierta y a Distancia UNAD, Facultad de Ingeniería y Ciencias Básicas.

NIÑO WILCHES, Yamith Andrés Fernando. Importancia de la implementacion del concepto de ciberseguridad organizacional en las organizaciones tipo PYMES. Bogotá, D. C., 2015, 143p. Trabajo de grado (maestría en gestión de organizaciones). Universidad Militar Granada, Facultad de Ciencias Económicas.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity. {En línea} 2012 {3 de junio del 2021} disponible en: {https://www.iso.org/standard/44375.html}.

PALACIOS ORTEGA, Andrés. Diseño de un modelo de políticas de seguridad informática para superintendencia de industria y comercio de Bogotá. Bogotá, D. C., 2015. 87p. Trabajo de grado (pregrado en Ingeniería de Sistemas). Universidad Libre de Colombia, Facultad de Ingeniería.

PARRA CALDERÓN, Jairo Andrés. Delitos informáticos y Marco Normativo en Colombia. Pitalito – Huila, 2019, 134p. Trabajo de grado (especialista en Seguridad Informática). Universidad Nacional Abierta y a Distancia UNAD, Escuela de Ciencias Básicas de Tecnología e Ingeniería.

PEÑARANDA SUAREZ, José Luis. Diagnóstico de seguridad al sistema informático de gestión de contratos de prestación de servicios (CPS) de la Universidad del Rosario. Ocaña, 2017, 64p. Trabajo de grado (especialista en Auditoría de Sistemas). Universidad Francisco de Paula Santander, Facultad de Ingeniería de Sistemas.

PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto Nacional 1474 de 2002. Promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20)

de diciembre de mil novecientos noventa y seis (1996). Bogotá, D. C.: Diario Oficial No. 44.496 del 24 de julio del 2002.

RAMOS GALLARDO, Arelis Taimati, ARANGO HURTADO, Erika María y AMADOR TINOCO, Antonio. Riesgos en ciberseguridad y sus efectos sobre la transformación digital en la nueva normalidad, según las empresas operadoras de seguridad. Bogotá, D. C., 2020, 35p. Trabajo de grado (especialización en Administración de Empresas Virtual). Universidad EAN, Facultad de Administración, Finanzas y Ciencias Económicas.

REPÚBLICA DE COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC). Modelo de Seguridad y Privacidad de la Información MSPI. {En línea} 2013 {3 de junio del 2021} disponible en: {https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/}.

_____. Decreto Número 2573 de 2014. Diario Oficial No. 49.363 de 12 de diciembre de 2014

REPÚBLICA DE COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. VICEMINISTERIO DE ECONOMÍA DIGITAL. Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD). {En línea} {2018}. Disponible en {https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+Públicas+-+Guía+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b}

RITEGNO, Eduardo O. “COBIT2019”. {En línea}. 2018 {3 de junio del 2021} disponible en: {https://iaia.org.ar/wp-content/uploads/2019/07/COBIT2019-IAIA.pdf}

RODRÍGUEZ CASTRO, Jorge Martín. 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. Chiclayo, Perú, 2019, 226p. Trabajo de grado (maestro en Ingeniería de Sistemas y Computación con mención en Dirección Estratégica de Tecnologías de Información). Universidad Católica Santo Toribio de Mogrovejo, Escuela de Posgrado.

SALAZAR CHOEZ, Teodoro Kelvin. Análisis de la Norma ISO/IEC 27002:2013 para mejorar los controles de la seguridad de la información en la sala de cómputo # 14 de la carrera de Ingeniería en computación y redes. Jipijapa, Manabí Ecuador. 2018. 113p. Trabajo de grado (pregrado Ingeniería en Computación y Redes) Universidad Estatal del Sur de Manabí, Facultad de Ciencias Técnicas.

VALDIVIESO SUAREZ, Ximena Estefanía. Metodología de investigación cuantitativa en trabajos de graduación de la modalidad de titulación de la carrera de

contabilidad y auditoría. Machala, 2019, 22p. Trabajo de grado (pregrado en Contabilidad y Auditoría) Universidad Técnica de Machala, Facultad de Ciencias Empresariales.

VALOYES MOSQUERA, Amancio. Ciberseguridad en Colombia. {En línea} 28 de agosto de 2019. Disponible en http://repository.unipiloto.edu.co/handle/20.500.12277/6370

VILCARROMERO ZUBIATE, Ladi Lizeth y VILCHEZ LINAREZ, Evit Vilchez. Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. Lima, 2018, 107p. Trabajo de grado (maestría en Dirección de Sistemas y Tecnologías de la Información). Universidad Peruana de Ciencias Aplicadas, Escuela de Posgrado.

ANEXOS

Anexo A. Acuerdo de confidencialidad

V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE PROYECTOS DE INVERSIÓN VIAL ANDINO S.A.S Y GINA ALEJANDRA ARENIZ AREVALO

Por la **parte reveladora**
Nombre: **PROYECTOS DE INVERSIÓN VIAL ANDINO S.A.S**
Dirección: Km 76 + 800 vía Bogotá – Villavicencio.
Teléfono: (1) 7569668
E-mail: atencionalusuario@coviandina.com

Por la parte **receptora de la información**
Nombre: **GINA ALEJANDRA ARENIZ AREVALO**
Dirección: Diagonal 6 Sur no 40-110
Teléfono: 3108806204
E-mail: ginalejandrareniz@gmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la Proyectos De Inversión Vial Andino S.A.S, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto aplicado con el título: Modelo De Aseguramiento En Ciberseguridad Para La Empresa Proyectos De Inversión Vial Andino S.A.S

2. Que la información de propiedad de Proyectos De Inversión Vial Andino S.A.S ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en

consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación Modelo De Aseguramiento En Ciberseguridad Para La Empresa Proyectos De Inversión Vial Andino S.A.S, Gina Alejandra Areniz Arévalo que, para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de Proyectos De Inversión Vial Andino S.A.S.

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al Proyectos De Inversión Vial Andino S.A.S, así como también a no utilizar dicha

información en beneficio propio ni de terceros, sólo con fines estadisticos y de mejoramiento de la Proyectos De Inversión Vial Andino S.A.S.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

   modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto Modelo De

Aseguramiento En Ciberseguridad Para La Empresa Proyectos De Inversión Vial Andino S.A.S lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionaran las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la

relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma Proyectos De Inversión Vial Andino S.A.S, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de Proyectos De Inversión Vial Andino S.A.S.

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: activos informáticos, infraestructura tecnológica, procesos de seguridad, sistemas de gestión de seguridad.

10. La información capturada por la **parte receptora** se observará como modelo aplicable, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad todo el persona Proyectos De Inversión Vial Andino S.A.S no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de Proyectos De Inversión Vial Andino S.A.S, ni violentará la ley de delitos informáticos colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante Gina Alejandra Areniz Arévalo se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa Proyectos De Inversión Vial Andino S.A.S para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la emresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La parte receptora queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora**, esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los

cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes Gina Alejandra Areniz Arévalo - Proyectos De Inversión Vial Andino S.A.S se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las clausulas del presente acuerdo de confidencialidad por parte de Gina Alejandra Areniz Arévalo.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Villavicencio, Meta a los 4 días del mes de junio de 2021.

Como Parte Receptora:

Gina Alejandra Areniz Arévalo
Estudiante UNAD.
C.C. No. 1091664682 de Ocaña.

Por la parte reveladora:

Camilo Ernesto Álvarez
Proyectos De Inversión Vial Andino
C.C. No. 79943474 de Bogotá.

Anexo B. Autorización.

V0.1

Villavicencio, 04 de junio de 2021

Ingeniero:
CAMILO ERNESTO ALVAREZ
Gerente Administrativo
Proyectos de inversión Vial Andino S.A.S

Asunto: Autorización para la ejecución del proyecto titulado: Modelo De Aseguramiento En Ciberseguridad Para La Empresa Proyectos De Inversión Vial Andino S.A.S.

Cordial saludo estimado ingeniero,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a nombre de la empresa, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: Modelo De Aseguramiento En Ciberseguridad Para La Empresa Proyectos De Inversión Vial Andino S.A.S, el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "Presentar un modelo de aseguramiento en ciberseguridad a la organización caso de estudio Proyectos de Inversión Vial Andino S.A.S"; al mismo tiempo será apoyado por los objetivos específicos: " 1.Estudiar los ataques y

vulnerabilidades cibernéticas que se presentan dentro de las empresas de construcción en Colombia.
2.Determinar las normas, leyes, guías, procedimientos y políticas nacionales e internacionales para la protección y prevención de ciberseguridad.
3.Identificar los ataques cibernéticos que se han presentado dentro de la organización caso de estudio.
4.Analizar las posibles vulnerabilidades de ciberseguridad que se pueden estar presentando dentro de la organización.
5.Plantear un modelo de ciberseguridad que se adapte al modelo de negocio y contribuya a minimizar vulnerabilidades presentes." para obtener como resultado un alto impacto en la seguridad de la empresa nombre de la empresa.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

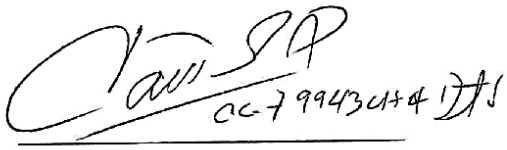
- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por Proyectos de Inversión Vial Andino S.A.S.
- La empresa Proyectos de Inversión Vial Andino S.A.S deberá establecer qué tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El dcumento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Villavicencio, Meta., a los 4 días del mes de junio de 2021.

Cordialmente,

Gina Alejandra Areniz Arévalo
Estudiante UNAD.



Camilo Ernesto Álvarez
Gerente Administrativo

Anexo C. Encuesta para el diagnóstico del estado actual de la Empresa

1. ¿Actualmente la empresa cuenta con la División de Área de Sistemas?

SI
NO

2. ¿La empresa cuenta con un modelo de controles para gestionar los incidentes de ciberseguridad basados en la norma ISO 27002:2013?

SI
NO

3. ¿La empresa cuenta con un responsable para gestionar los incidentes de ciberseguridad?

SI
NO

4. ¿Cuándo se presenta un incidente se reporta el evento al responsable del área?

SI
NO

5. ¿Existen procedimientos para la detección de incidentes de ciberseguridad?

SI
NO

6. ¿Existen procedimientos para el análisis de incidentes de ciberseguridad en la empresa?

SI
NO

7. ¿Existen procedimientos de elaboración de reportes para los incidentes en ciberseguridad que se presentan dentro de la empresa?

SI
NO

8. ¿El reporte de incidentes se acompaña con las posibles debilidades encontradas en los sistemas de la empresa?

SI
NO

9. ¿En la empresa se capacita el personal para la resolución de incidentes en ciberseguridad?

SI
NO

10. ¿Se advierte a los usuarios que el tratar de vulnerar los sistemas es considerado un mal uso para la compañía?

SI
NO

11. ¿Se establecen criterios de priorización de incidentes de ciberseguridad en la empresa?

SI
NO

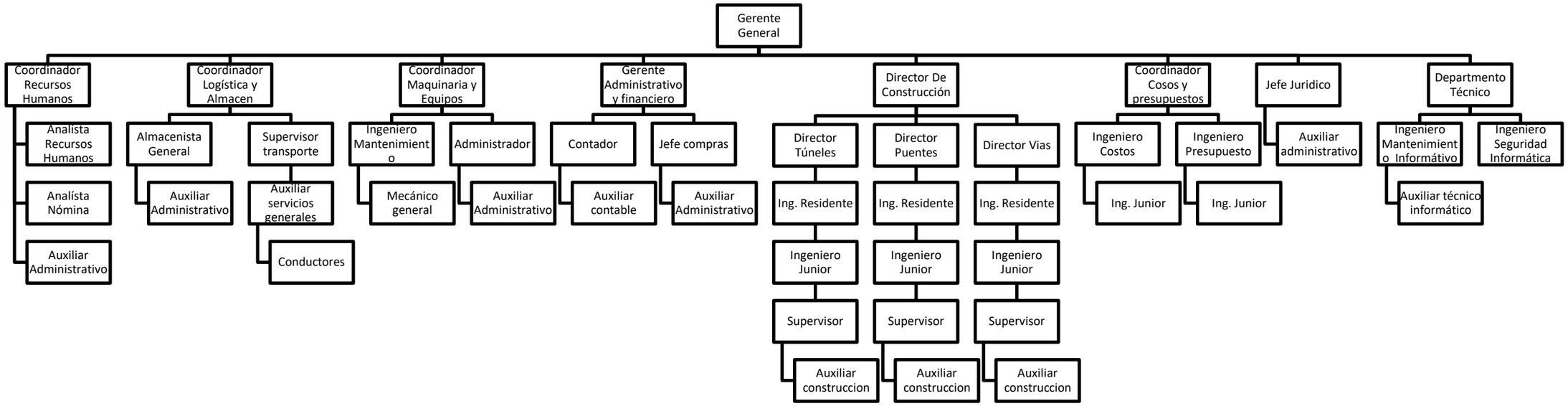
12. ¿Se lleva un registro de los incidentes que se han presentado dentro de la empresa?

SI
NO

13. ¿La empresa necesita ayuda de terceros para dar solución a los incidentes de ciberseguridad?

SI
NO

Anexo D. Organigrama Proyectos de Inversión Vial Andino



Fuente. Elaboración propia.

Anexo E. Matriz de Riesgos

									IMPACTO				MAGNITUD DEL IMPACTO								NIVEL DE RIESGO INHERENTE		
No.	**Nombre del proceso**	**Nombre del riesgo**	**Causa que origina**	**Evento de Riesgo**	**Consecuencia para la compañía**	**Factor (Asociado a la Causa)**	**Categoría (Asociado al Riesgo)**	**Tipo de Impacto (Asociado a la Consecuencia)**	**Vida Humana (Daño a personas)**	**Legal y Penal**	**Reputacional**	**Pérdida Económica**	**%**	**GRADO IMPACTO TEÓRICO**	**IMPACTO**	**GRADO IMPACTO AJUSTADO**	**GRADO IMPACTO FINAL**	**IMPACTO FINAL**	**PROBABILIDAD DE OCURRENCIA**	**NIVEL DE RIESGO INHERENTE**	**NIVEL DE RIESGO INHERENTE**	**Área Responsable del Riesgo**
R1	INFRAESTRUCTURA	Fuga de información por accesos no autorizados a zonas restringidas	Falta de controles de accesos	Intrusión de personal no autorizado a las instalaciones	Fugas de información	Recurso Humano y tecnológicos	Ejecución y administración de procesos	Seguridad Información	NO	SI	NO	NO	**45 %**	**5**	**CRÍTICO**	**8**	**8**	**MAYOR**	**POSIBLE**	**16**	**MEDIO**	Departamento técnico
R2	SERVIDORES NAS	Fuga de información por accesos no autorizados a bases de datos por el uso inadecuado de usuario y contraseña de ingresos a bases de datos.	Falta de controles de accesos, cifrado de contraseñas de acceso, fuga de información, usuarios comunes.	Intrusión a bases de datos, filtración, robo o alteración de información.	Fugas de información o alteración de información	Recurso Humano	Fraude interno	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**10**	**10**	**CATASTRÓFICO**	**MODERADO**	**40**	**ALTO**	Departamento técnico
R3	SERVIDORES NAS	Fuga o confiablidad de informació	Uso inadecuado de usuarios	Accesos no autorizados a aplicaciones y	Fugas de información o alteración	Tecnología	Fraude interno	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**10**	**10**	**CATASTRÓFICO**	**MODERADO**	**40**	**ALTO**	Departamento técnico

		n por el uso inadecuado de privilegios y usuarios en bases de datos	privilegiados o generación de usuarios genéricos.	bases de datos	de información																
R4	SERVIDORES NAS	Perdidas de información por ataques externos a las bases de datos	Ataques externos por hackers	Perdida de información, robo de información, secuestros de información	Perdida de información	Situaciones Externas	Fallas tecnológicas	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**10**	**10**	**CATASTRÓFICO**	**POSIBLE**	**20**	**MEDIO**	Todos los Procesos / Departamento Técnico
R5	SERVIDORES NAS	Pérdidas económicas por fallas en servidores donde se almacenan las bases de datos	Fallas tecnológicas	Pérdida de disponibilidad de la información	Pérdida económica	Tecnología	Fallas tecnológicas	Pérdida Económica	NO	NO	SI	SI	**45 %**	**5**	**CRÍTICO**	**5**	**5**	**CRÍTICO**	**POSIBLE**	**10**	**MEDIO**	Departamento técnico
R6	SERVIDORES NAS	Causa de fuerza mayor	terremoto, rayo, inundación o incendio.	desastre natural, quemado de algún componente electrónico	Perdida de hardware	Tecnología	Fallas tecnológicas	Pérdida Económica e Información	NO	NO	SI	SI	**45 %**	**5**	**CRÍTICO**	**8**	**8**	**MAYOR**	**CONSTANTE**	**40**	**ALTO**	Departamento Técnico
R7	GESTOR DE CORREO ELECTRÓNICO	Ataques cibernéticos ocasionados por correos electrónicos	Phising, Spam, Malware, Ingeniería social	Fuga de información, daños a software y/o dispositivos, ataques cibernéticos	Perdida de información, Perdida económica	Tecnología, Recurso Humano	Recurso Humano y tecnológicos	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**8**	**8**	**MAYOR**	**POSIBLE**	**16**	**MEDIO**	Departamento técnico, Recurso Humanos
R8	PAQUETE OFIOMÁTICO	Mal uso de las herramientas ofimáticas	Duplicidad de información, uso inadecuado de las herramientas.	Usuarios mal capacitados	Alteración y perdida de la información	Recurso Humanos	Recurso Humanos	Seguridad Información	NO	NO	NO	SI	**20 %**	**2**	**INSIGNIFICANTE**	**3**	**3**	**MENOR**	**POSIBLE**	**6**	**BAJO**	Recurso Humano / Departamento Técnico
R9	SOFTWARE SAP	Privilegios y accesos no autorizados, ataques informáticos	No identificación de roles a los usuarios, fugas de contraseñas, ataques externos o internos	Falta de controles de acceso en los softwares, falta de capacitación al personal, mal desarrollo de software.	Perdida de información, Perdida económica	Tecnología, Recurso Humano	Recurso Humano y tecnológicos	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**8**	**8**	**MAYOR**	**CONSTANTE**	**40**	**ALTO**	Departamento técnico, Recurso Humanos, almacén, contabilidad, costos y presupuesto,

																				construcción
R10	EQUIPOS DE COMPUTO	Riesgos del equipamiento informático	Pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	Mala manipulación del usuario, hurto por parte de un tercero	Perdida de información y de activos físicos	Recurso Humano y tecnológicos	Recurso Humano y tecnológicos	Pérdida Económica	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**6**	**7**	**MAYOR**	**POSIBLE**	**14**	**MEDIO**	Departamento técnico
R11	SERVIDOR WORK MANAGER	Gestión de acceso de usuarios	Falta de control de acceso a la red de usuarios no autorizado.	Ataques de denegación de servicios	Robo de información, fallos técnicos a la infraestructura tecnológica	Recurso Humano y tecnológicos	Ejecución y administración de procesos	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**9**	**9**	**CATASTRÓFICO**	**POSIBLE**	**18**	**MEDIO**	Todos los Procesos / Departamento Técnico
R12	ANTIVIRUS	No protección contra códigos maliciosos	Ataques cibernéticos externo/interno	Falta de controles de detección, de prevención de ataques informáticos	Perdida de información o data	Recurso Humano y tecnológicos	Ejecución y administración de procesos	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**8**	**8**	**MAYOR**	**POSIBLE**	**16**	**MEDIO**	Departamento técnico
R13	FIREWALL	Interrupción del servicio	Denegación de servicio, malware	Ejecución de Malware, ataques informáticos, ingeniería social.	Fugas de información, afectación económica	Recurso Humano y tecnológicos	Fallas tecnológicas	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**8**	**8**	**MAYOR**	**OCASIONAL**	**24**	**MEDIO**	Departamento técnico
R14	EQUIPOS LAN	Pérdida y hurto de datos e información.	Malware, ingeniería social.	Ejecución de Malware, ataques informáticos, ingeniería social.	Fugas de información, afectación económica	Recurso Humano y tecnológicos	Fallas tecnológicas	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**8**	**8**	**MAYOR**	**OCASIONAL**	**24**	**MEDIO**	Departamento técnico
R15	EQUIPOS WAN	Interrupción del servicio	Denegación de servicio, malware	Ejecución de Malware, ataques informáticos, ingeniería social.	Fugas de información, afectación económica	Recurso Humano y tecnológicos	Fallas tecnológicas	Seguridad Información	NO	SI	SI	SI	**70 %**	**7**	**MAYOR**	**8**	**8**	**MAYOR**	**OCASIONAL**	**24**	**MEDIO**	Departamento técnico
R16	RECURSOS HUMANOS	Ingeniería social	Falta de capacitación a los usuarios del sistema	Falta de resguardo de contraseñas, mal uso de buenas	Perdidas de información, intrusiones,	Recurso humano	Fraude interno	Seguridad Información	NO	SI	NO	SI	**45 %**	**5**	**CRÍTICO**	**8**	**8**	**MAYOR**	**POSIBLE**	**16**	**MEDIO**	Departamento Técnico, Recursos Humanos

				prácticas tecnológicas.	convertirse en punto de ataque																	
R17	DESASTRES NATURALES	Perdida de dispositivos e infraestructura por desastres naturales	Incendios, inundaciones, terremotos, y demás desastres naturales	Daños en la infraestructura tecnológica y física de organización	Pérdida económica, perdida de información.	Situaciones Externas	Daños a activos físicos	Pérdida Económica e Información	SI	SI	NO	SI	**75 %**	**8**	**MAYOR**	**10**	**10**	**CATASTRÓFICO**	**IMPROBABLE**	**10**	**MEDIO**	Alta gerencia, departamento técnico

Fuente. Elaboración propia.