IMPLEMENTACIÓN DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN - PESI - PARA LA CORPORACIÓN DE ALTA TECNOLOGÍA PARA LA DEFENSA “CODALTEC”

SARA MERCEDES PINEDA TÉLLEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CEAD ACACIAS
VILLAVICENCIO META
JULIO 2019

IMPLEMENTACIÓN DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN - PESI - PARA LA CORPORACIÓN DE ALTA TECNOLOGÍA PARA LA DEFENSA “CODALTEC”.

SARA MERCEDES PINEDA TÉLLEZ

Proyecto de grado para optar al título de
Especialista en Seguridad Informática

MsC. KATERINE MÁRCELES VILLALBA
Directora del Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
CEAD ACACIAS
VILLAVICENCIO META
JULIO 2019

Nota de aceptación:

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y A Distancia UNAD, para optar al título de Especialista en Seguridad Informática.

_____

Jurado

_____

Jurado

DEDICATORIA

Dedicado a Nuestro Creador, quien nos ha permitido ser sus hijos, dándonos la oportunidad de elegir nuestros caminos.

A mis hijas y familia quienes han sido un apoyo incondicional en el impulso y apoyo al logro de mis proyectos.

AGRADECIMIENTOS

La autora expresa sus agradecimientos a:

A los directivos Coronel Diego Andrés Hernández Mosquera, Mayor Luis Enrique Ariza Vargas y empleados de la Corporación de Alta Tecnología para la Defensa "**CODALTEC**", por abrir sus puertas para el desarrollo del presente estudio, brindándome su apoyo y orientación profesional, para el logro de los objetivos trazados.

A la Universidad Nacional Abierta y a Distancia UNAD y a la escuela de ciencias básicas, tecnología e ingeniería y su grupo de docentes, quienes me brindaron la oportunidad, la formación y los conocimientos para concluir con la especialización de Seguridad Informática.

A los ingenieros Katerine Márceles Villalba directora del proyecto y Christian Angulo Rivera director del curso, asesores del presente estudio, pues gracias a su experiencia y conocimientos profesionales tuvieron a bien señalar el camino propicio para llevar a buen término el presente estudio.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

ACTIVO DE INFORMACIÓN: Aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida[1].

AMENAZA: Es la causa potencial de un daño a un activo de información, es todo aquella acción o elemento capaz de atentar contra la seguridad de la información[2].

ANTIVIRUS: Software encargado de detectar, bloquear y eliminar virus informáticos o código malicioso[3].

ATAQUE: Es la acción de interrumpir o dañar un activo de información con el objetivo de causar problemas de confiabilidad, disponibilidad e integridad. O cuando se materializa una amenaza de seguridad[4].

ANÁLISIS DE RIESGOS: Utilizar de la información disponible, para identificar peligros y estimar los riesgos. Causa: Razón por la cual el riesgo sucede[5].

CONTROLES: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información[6].

DISPONIBILIDAD: Propiedad que determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas[7].

CÓDIGO MALICIOSO: Software diseñado para ejecutar acciones maliciosas (como provocar daños al software de la computadora, robar información almacenada en un sistema informático, aprovechar recursos informáticos para efectuar otras acciones perjudiciales para el usuario) y que incluye programas como virus, gusanos, troyanos, spyware, entre otros. Pueden utilizar como vía de diseminación, el correo electrónico, sitios de internet, redes, dispositivos móviles, dispositivos removibles (por ejemplo, pen-drives) [8].

---

[1] FINDETER. Plan de tratamiento de riesgos de seguridad y privacidad de la información. Findeter. Bogotá, 2018.
[2] Ibíd.
[3] LOZANO OLAVE, Marisol. Diseño de un Plan Estratégico de Seguridad de Información (PESI) para una compañía del sector asegurador. Tesis de especialista. Institución Universitaria Politécnico Grancolombiano. Bogotá, 2017.
[4] Ibíd.
[5] FINDETER, op. cit.
[6] Ibíd.
[7] Ibíd.
[8] LOZANO OLAVE, op. cit.

DATOS PERSONALES: Según lo exige la legislación y la reglamentación, cuando sea aplicable. (Ley 1273 de 2009, ley 1581 de 2012 y el Registro Nacional de Bases de Datos, en la Súper Intendencia de Industria y Comercio SIC, adicionando las políticas de tratamiento de la información).

DISEÑO DE RED SEGURA: Definición de un esquema de red aplicando medidas de seguridad informática, que una vez implementadas minimizan los riesgos de una intrusión[9].

DEFENSA EN PROFUNDIDAD: Identificar los controles necesarios para proteger la información[10].

DMZ: Una DMZ o una zona desmilitarizada, es un segmento de red específico, en el cual se ubican servicios específicos de red que son públicos a redes poco seguras como Internet[11].

ESTÁNDAR DE SEGURIDAD: Conjunto de normas o modelos diseñados con la finalidad de brindar soluciones sistemáticas a un área del conocimiento específico[12].

FIREWALL: Un firewall o también llamados corta fuego, es un software o hardware que restringe el acceso a sitios web o una red sin autorización de acceso[13].

GESTIÓN DE RIESGOS: La gestión de riesgos es el pilar fundamental de la seguridad de la información[14].

IMPACTO: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo[15].

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información[16].

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos[17].

---

[9] TOAPANTA, Moisés. Seguridad de redes. Universidad Politécnica Salesiana. Guayaquil, 2014.
[10] LOZANO OLAVE, op. cit.
[11] Ibíd.
[12] Ibíd.
[13] Ibíd.
[14] Ibíd.
[15] Ibíd.
[16] Ibíd.
[17] Ibíd.

INCIDENTE DE SEGURIDAD: Un incidente de seguridad es cualquier acción que atente contra la confiabilidad, disponibilidad e integridad de la información[18].

INGENIERÍA SOCIAL: Es la secuencia de acciones que tienen como finalidad la obtención de información, el fraude o el acceso no autorizado a sistemas informáticos, y que ha implicado en algún momento la manipulación psicológica de personas[19].

INTRUSOS: Es una persona que intenta acceder a un sistema informático sin autorización, a través de técnicas y/o métodos informáticos que se lo permitan. ISO: (International Organizatión for Standardization). Organización internacional de estándares[20].

MEJORES PRÁCTICAS: Las buenas prácticas de seguridad de la información son un instrumento que permiten desarrollar de manera consciente las estrategias en la compañía. Metodología: Es un conjunto de reglas o métodos organizados de forma sistémica con el objetivo de lograr el cumplimiento de una norma o un estándar[21].

PHISHING: Suplantación de identidad de una página o sitio Web[22].

PLAN DE CONTINGENCIA: Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas[23].

PROPIETARIO DEL RIESGO SOBRE EL ACTIVO: Persona responsable de gestionar el riesgo[24].

PROBABILIDAD DE OCURRENCIA: Posibilidad de que se presente una situación o evento específico[25].

PSE: Proveedor de servicios electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet[26].

---

[18] Ibíd.
[19] Ibíd.
[20] Ibíd.
[21] Ibíd.
[22] Ibíd.
[23] Ibíd.
[24] Ibíd.
[25] Ibíd.
[26] Ibíd.

RESPONSABLES DEL ACTIVO: Personas responsables del activo de información[27].

RIESGO: Grado de exposición de un activo que permite la materialización de una amenaza[28].

RIESGOS: Es la posibilidad de que una amenaza aproveche una vulnerabilidad y dañe un activo de información. Departamento de seguridad[29].

RIESGO INHERENTE: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control[30].

RIESGO RESIDUAL: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo[31].

RED DE DATOS: Es aquella infraestructura o red de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos[32].

RED PRIVADA VIRTUAL VPN: Sistema de telecomunicación consistente en una red de datos restringida a un grupo cerrado de usuarios, que se construye empleando en parte o totalmente los recursos de una red de acceso público, es decir, es una extensión de la red privada de una organización usando una red de carácter público[33].

REPUDIO: Denegación, por una de las entidades implicadas en una comunicación, de haber participado en la totalidad o en parte de dicha comunicación[34].

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014) [35].

SGSI: Siglas del Sistema de Gestión de Seguridad de la Información. Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar,

---

[27] Ibíd.
[28] Ibíd.
[29] Ibíd.
[30] Ibíd.
[31] Ibíd.
[32] Ibíd.
[33] Ibíd.
[34] Ibíd.
[35] Ibíd.

mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001:2013[36].

SEGURIDAD LÓGICA: Conjunto de medidas de seguridad y herramientas informáticas de control de acceso a los sistemas informáticos[37].

SEGURIDAD FÍSICA: Controles externos al ordenador, que tratan de protegerlo contra amenazas de naturaleza física como incendios, inundaciones, entre otros[38].

TELETRABAJO: El teletrabajo es un nuevo sistema de organización del trabajo en que la persona trabajadora desarrolla una parte importante de su trabajo fuera de la empresa y por medios telemáticos[39].

VISIBILIDAD: Tener la capacidad de conocer que sucede en el entorno tecnológico de la compañía, para así anticiparse a situaciones que puedan afectarla[40].

VULNERABILIDAD: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada[41].

VULNERABILIDAD DE SEGURIDAD: Es un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema[42].

WI-FI (WIRELESS FIDELITY O FIDELIDAD SIN CABLES): Es una red de ordenadores sin utilización de cables equivalente a la tecnología inalámbrica 802.11 para comunicación a distancia[43].

WI-PHISHING: Wi-phishing, sustracción de datos personales a través de falsas redes públicas de acceso[44].

---

[36] Ibíd.
[37] Ibíd.
[38] Ibíd.
[39] Ibíd.
[40] Ibíd.
[41] Ibíd.
[42] Ibíd.
[43] Ibíd.
[44] Ibíd.

RESUMEN

La Corporación de Alta Tecnología para la Defensa "**CODALTEC**", en su propósito de liderar el desarrollo de las capacidades tecnológicas del Sector Defensa, ha centralizado sus esfuerzos enfocándolos a la ciencia, tecnología e innovación, generando paralelamente una tecnología dual creando sus propias soluciones de desarrollo de sistemas, modelado de sistemas de información, sensores y simuladores para la fuerza pública, disminuyendo la brecha tecnológica del país en la industria del Sector Defensa, a través del desarrollo tecnológico, por medio de la apropiación y generación del conocimiento integrándolas a las Universidades, a los sectores productivos público, privado y del Estado. Proceso en el que se ha caracterizado por su calidad, esfuerzo y tiempo para planear estas estrategias.

La propuesta de trabajo de grado como Especialista en Seguridad Informática consistió en diseñar el Plan Estratégico de Seguridad de la Información "PESI", para la Corporación de Alta Tecnología para la Defensa "**CODALTEC",** destinado al área de Seguridad de la Información para que de esa manera se pueda llegar a cumplir con el objetivo propuesto, que es proteger los activos de información de la Corporación.

Se alinea el PESI a los objetivos estratégicos de "**CODALTEC**", la gestión de riesgos, la optimización de recursos, la entrega de valor y la integración del aseguramiento de los procesos de la seguridad de la información, con el objeto de permitir a "**CODALTEC**", cumplir con la expectativa planeada en la implementación de la seguridad de la información, como son los requerimientos de seguridad de los activos de información, hardware, software y comunicaciones, aplicando los atributos de "disponibilidad, integridad y confiabilidad de la información".

El PESI brindará un gran apoyo al área de seguridad de la información de "**CODALTEC**" al generar actividades de mejora continua, perfeccionando la gestión de los procesos de las áreas de infraestructura, gestión de la configuración, base de datos y arquitectura; que garanticen proteger, asegurar y minimizar el daño que pueda sufrir "**CODALTEC**", debido a una situación adversa que ocurra sobre sus activos de información, teniendo en cuenta la gestión de riesgos de seguridad de la Información, la optimización de recursos, entrega de valor, medición del desempeño de seguridad de la información por medio de los indicadores y la integración del aseguramiento del proceso de acuerdo al PESI.

Palabras Claves: Riesgo informático, Plan Estratégico de Seguridad de la información, NTC-ISO-IEC 27001:2013, Metodología Magerit.

ABSTRACT

This project carried out the design of a Strategic Plan for Information Security "PESI" for the High Technology Corporation for Defense "CODALTEC", firstly the level of computer security, the infrastructure of hardware, software, communications and security was evaluated with which counts the information of "CODALTEC", where it was incorporated in this process to the directives, heads, leaders and the suitable personnel and connoisseur of the areas of Infrastructure, Management of the configuration, architecture, databases, office PMO, office of OGA asset management, Human Resources, information security and development, personnel with a management profile, experience and leadership in the development of information security activities.

The PESI was focused in the first place to carry out a study of the current situation regarding the fulfillment of the control objectives and the requirements of the NTC-ISO-IEC 27001: 2013; then identify the critical assets for the organization, based on the performance of a risk analysis, detecting the threats that may affect each asset. From this point on, the project had as a reference this previous analysis with the final objective of executing the appropriate plans aimed at improving the levels of information security in "CODALTEC", so that the dimensions of security are covered.

In order to guarantee the improvement of information security in "CODALTEC", based on an analysis of the security of the initial information, a series of projects was defined to help achieve that optimum state of security desired. This is an applied project, where it was necessary to carry out a research process, study and an analysis of good IT security practices; for the fulfillment of the specific objectives set out in this work.

This work of degree sought to enrich the knowledge acquired and the use of the computer resources of "CODALTEC" to obtain a greater knowledge of the security of the information and in addition to this the acquired experience that will have a high impact in the vision of new strategies to design, generating a greater facility to face the presence of adversities that may arise against the security of information.

Therefore, in pursuit of continuous improvement, "CODALTEC" and its directives are presented with the design of a Strategic Information Security Plan "PESI" that includes information security projects that support the area of Information Security, managing their physical and logical needs, in order to expand and grow properly in the fulfillment of their activities. So that they make the decision of its approval.

Keywords: IT risk, Strategic Information Security Plan, NTC-ISO-IEC 27001: 2013, Magerit methodology.

INTRODUCCIÓN

Este proyecto realizó el diseño de un Plan estratégico de Seguridad de la Información “PESI” para la Corporación de Alta Tecnología para la Defensa “**CODALTEC**”, primeramente se evaluó el nivel de seguridad informática, la infraestructura de hardware, software, comunicaciones y la seguridad con que cuenta la información de “**CODALTEC**”, donde se incorporó en este proceso a las directivas, jefes, líderes y el personal idóneo y conocedor de las áreas de Infraestructura, Gestión de la configuración, arquitectura, bases de datos, oficina PMO, oficina de gestión de activos OGA, Recursos Humanos, seguridad de la información y desarrollo, personal que posee perfil de gestión, experiencia y liderazgo en el desarrollo de las actividades referentes de la seguridad de la información.

El PESI estuvo enfocado en primer lugar a realizar un estudio de la situación actual frente al cumplimiento de los objetivos de control y los requerimientos de la NTC-ISO-IEC 27001:2013; seguidamente en identificar los activos críticos para la organización, a partir de la realización de un análisis de riesgos detectando las amenazas que pueden afectar a cada activo. A partir de este punto el proyecto tuvo como referencia este análisis previo con el objetivo final de ejecutar los planes adecuados orientados a mejorar los niveles de seguridad de la información en “**CODALTEC**”, de forma que las dimensiones de la seguridad estén cubiertas.

Con el objeto de garantizar la mejora de la seguridad de la información en **“CODALTEC”**, a partir de un análisis de la seguridad de la información inicial, se definió una serie de proyectos que ayudan a conseguir ese estado óptimo de seguridad deseado. Este es un proyecto aplicado, donde fue necesario realizar un proceso de investigación, estudió y un análisis de buenas prácticas de seguridad informática; para el cumplimiento de los objetivos específicos planteados en este trabajo.

Este trabajo de grado buscó enriquecer el conocimiento adquirido y el aprovechamiento de los recursos informáticos de “**CODALTEC**” para obtener un mayor conocimiento de la seguridad de la información y además de ello la experiencia adquirida que tendrá un alto impacto en la visión de nuevas estrategias a diseñar, generando una mayor facilidad para afrontar la presencia de adversidades que se puedan presentar contra la seguridad de la información.

Por lo anterior en búsqueda de la mejora continua, se presenta a “**CODALTEC**” y sus directivas el diseño de un Plan estratégico de Seguridad de la Información “PESI” en el que se incluyan los proyectos de seguridad de la información que apoyen el área de Seguridad de la Información, gestionando sus necesidades físicas y lógicas, con el objeto de ampliar y crecer adecuadamente en el cumplimiento de sus actividades. Para que tomen la decisión de su aprobación.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Diseñar un Plan Estratégico de Seguridad de la Información “PESI”, alineado con los objetivos estratégicos y conforme con los lineamientos de la Dirección de la Corporación de Alta Tecnología para la Defensa “**CODALTEC**” generando políticas y proyectos de seguridad de la información para el periodo 2018-2022; que garanticen la protección de la información de la empresa.

1.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar la situación actual de la seguridad de la información en “**CODALTEC**”.

- Diseñar el procedimiento para la identificación de riesgos de las operaciones y la seguridad de la información de “**CODALTEC**”.

- Analizar las necesidades e iniciativas para el Plan Estratégico de Seguridad de la Información.

- Generar una planeación para formular el portafolio de proyectos de seguridad de la información.

- Formular los indicadores de seguridad de la Información en concordancia con lo elaborado.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCIÓN DEL PROBLEMA

La Corporación de Alta Tecnología para la Defensa "**CODALTEC**" en su propósito de liderar el desarrollo de las capacidades tecnológicas del Sector Defensa y con el pleno conocimiento de que las tecnologías de la información ya están al alcance de todos y es posible tener conectividad desde cualquier lugar y acceder desde cualquier dispositivo a aplicaciones corporativas; además muchos de los procesos de entidades públicas como privadas se han tecnificado y automatizado; actividades necesarias pero que lo hacen propenso a la materialización de incidentes relacionados con la seguridad de la información.

"**CODALTEC**" es una joven empresa que fue creada en diciembre de 2012 y ha ido creciendo poco a poco, sus procesos se han venido manejando de acuerdo a las necesidades del día a día, lo que ocasiona que la entidad y sus sistemas de información sean vulnerables a errores técnicos y humanos y a una sucesión de amenazas que afecten los activos críticos de información a diferentes delitos cibernéticos e informáticos, llegando a cristalizarse como un riesgo potencial inminente para sus activos, y para la eficaz gestión de la empresa. Además "**CODALTEC**" en los últimos años ha tenido una gran expansión en el desarrollo de sus actividades lo que ha creado la necesidad de que sus procesos se realicen fundamentados en una norma o estándar de calidad nacional e internacional que los acredite en materia de controles de seguridad de la información.

Analizando lo anterior se evidencia que el manejo de la información en la actualidad no cuenta con una adecuada protección lo que la hace limitada e insuficiente generando riesgos altos para este activo que es de gran importancia y que es necesario proteger desde su origen hasta su destino final, al igual que a los procesos y sistemas que hacen uso de la misma. Es necesario cubrir estas limitaciones actuales que presenta la entidad para permanecer en el mercado competitivamente, en el que se haga un uso eficiente de los recursos, de procesos estructurados y funcionarios especializados. Es deber de la organización garantizar la confidencialidad, integridad y disponibilidad de la información, hecho que obliga a "**CODALTEC**" a tomar las medidas para la adopción de buenas prácticas, como las descritas en el estándar de seguridad NTC-ISO-IEC 27001:2013.

Es por ello por lo que se propone el diseño de un plan estratégico de seguridad de la información "PESI", en el que se definen los lineamientos rectores para gestionar adecuadamente la seguridad de la información de los activos críticos de su infraestructura tecnológica; cubriendo la información almacenada, procesada y transferida en sus procesos informáticos, conservando los principios de seguridad, confidencialidad, integridad y disponibilidad de la información, que cumpla con las expectativas planteadas, en el que se incluyan los proyectos de seguridad de la información, generando procedimientos contextualizados bajo el rigor de un

esquema específico que supla las debilidades presentes, con el objeto de ampliar y crecer adecuadamente en el cumplimiento de sus actividades.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo diseñar un Plan Estratégico de Seguridad de la Información “PESI”, alineado con los objetivos estratégicos y conforme con los lineamientos de la Dirección de la Corporación de Alta Tecnología para la Defensa “**CODALTEC**” para garantizar la protección de la información de la empresa?

3. JUSTIFICACIÓN

A nivel mundial las organizaciones han sido atacadas en lo que respecta a su infraestructura tecnológica como también en la información, generando así un foco de inseguridad y un aumento de los riesgos afectando la integridad, disponibilidad y confiabilidad de su información exponiéndola a posibles atacantes.[45]

Como se aprecia en el documento de Allianz Risk Barometer, "*algunas situaciones producen incertidumbre y preocupación a las directivas de las empresas, causadas por los riesgos industriales, tales como la interrupción del negocio derivado de riesgos de ruptura en la cadena de suministro (46%), las catástrofes naturales (30%), el fuego y explosión (27%) son los principales riesgos que pueden llevar a escenarios disruptivos para las empresas a nivel global. Las causas de preocupación o factores de riesgo más significativos que siguen en el ranking de Allianz, a juicio de las empresas consultadas, están los Cyber-riesgos (17%) y los riesgos políticos (11%). En el documento de Allianz se señala que, a más largo plazo, las empresas se enfrentan a un doble reto. Por un lado, el derivado de la irrupción de innovaciones tecnológicas disruptivas, al mismo tiempo que a la exposición a condiciones ambientales más volátiles. Las empresas tendrán que hacer frente a los riesgos del negocio, así como las oportunidades, de las llamadas "tecnologías disruptivas", tales como la impresión 3D y la nanotecnología, a la vez que tener que lidiar con el impacto del cambio climático como un riesgo subyacente que no está dentro de su control directo. El riesgo más claramente identificado y temido por las empresas consultadas a 5 años vista son los ciber-riesgos, como ciberdelincuencia y fallos informáticos".*[46]

Según el documento de Allianz Risk Barometer, es claro que el uso de las tecnologías permiten grandes ventajas a las empresas y al desarrollo de sus negocios, pero este crecimiento conduce a la generación de altos riesgos como son ataques cibernéticos, robos y alteración de información critica que perjudican económicamente a las empresas y a su buen nombre perdiendo así credibilidad y competitividad; es por ello las empresas deben establecer planes estratégicos de seguridad de la información que contrarresten las actividades delictivas y el impacto que puedan causar.

Es importante resaltar la importancia de la información como dice el estándar internacional NTC-ISO/IEC 27002 "*la información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente*"

---

[45] LOZANO OLAVE, Marisol. Diseño de un Plan Estratégico de Seguridad de Información (PESI) para una compañía del sector asegurador. Tesis de especialista. Institución Universitaria Politécnico Grancolombiano. Bogotá, 2017.

[46] ALLIANZ RISK BAROMETER. Escenarios disruptivos y factores de riesgo. Prospectiva.eu. 16/01/2015

Como se puede apreciar, la base fundamental del estándar internacional NTC-ISO/IEC 27002, la información es un activo esencial, para todas las empresas y resulta inherente el uso de medios tecnológicos e informáticos para su excelente gestión. Sin embargo, parte de la falla, se debe a la poca apropiación de las directivas y los funcionarios a hacer uso activo de la seguridad de la información en todos los aspectos sean tecnológicos, operacionales, administrativos; estas debilidades de controles tecnológicos han permitido malas prácticas en el manejo seguro de la información creando espacios que son utilizados para posibles atacantes información, delitos cibernéticos y pérdidas económicas.

En el trabajo de grado llamado Diseño de un Plan Estratégico de Seguridad de Información (PESI) para una compañía del sector asegurador Marisol Lozano Olave[47], presenta la estructura del "PESI", conformada por 1) conocimiento de la organización, 2) diagnóstico, 3) alineación de los objetivos, 4) modelo de seguridad de la información, para terminar en la definición del plan estratégico de seguridad de la información donde se analizan y 5) priorizan las iniciativas y se establece el portafolio de proyectos de seguridad de la información.

Retomando la estructura presentada anteriormente como base teórica para el diseño de un Plan Estratégico para la Seguridad de la Información "PESI" para **"CODALTEC";** permitirá la construcción de una infraestructura segura en cuanto a software, hardware, comunicaciones, con el objeto de mejorar y de aplicar normas y lineamientos de seguridad tecnológica, para la construcción de los proyectos, destinados a fortalecer al sector defensa "Fuerzas Militares". En contexto con la intención de apoyar y orientar la adopción de buenas prácticas de seguridad de la información que contemple el detalle de la topología, los diferentes dispositivos de aseguramiento informático, la seguridad física y lógica; minimizando así las amenazas a las que está expuesta que lo hacen propenso a la materialización de incidentes relacionados con la seguridad de la información.

Según Lozano [48] se cuenta con varias herramientas orientadas a mitigar los impactos que conllevan la materialización de los riesgos de seguridad a los que está expuesta una organización, apoyándose en esta idea se fundamenta que es necesario diseñar un plan estratégico de seguridad de la información "PESI", identificando y priorizando el portafolio de proyectos de seguridad de la información que permitirá contribuir al cumplimiento del logro de los objetivos de negocio, siendo cada vez más competitivos a través del uso y apropiación de las nuevas tecnologías, cada vez más empoderados en la nueva era de transformación digital; una de ellas es la norma NTC-ISO-IEC 27001:2013, la cual genera un importante compromiso

[47] LOZANO OLAVE, Marisol. Diseño de un Plan Estratégico de Seguridad de Información (PESI) para una compañía del sector asegurador. Tesis de especialista. Institución Universitaria Politécnico Grancolombiano. Bogotá, 2017
[48] Ibíd

con la seguridad de la información, permitiendo grandes alcances en cada una de las áreas estructurales de la empresa.

El “PESI” brindará un gran apoyo al área de seguridad de la información de **“CODALTEC”** en el mejoramiento de la seguridad de la información que se maneja por medio de los recursos físicos y lógicos, diseñará los indicadores de seguridad, para medir el cumplimiento de éstos, y generar actividades de mejora continua, perfeccionando la gestión de los procesos de la gerencia y de las áreas de Infraestructura, Gestión de la configuración, arquitectura, bases de datos, oficina PMO, oficina de gestión de activos OGA, Recursos Humanos, seguridad de la información y desarrollo; que garanticen proteger, asegurar y minimizar el daño que pueda sufrir **“CODALTEC”** debido a una situación adversa que ocurra sobre sus activos de información, teniendo en cuenta la gestión de riesgos de seguridad de la Información, la optimización de recursos, entrega de valor, medición del desempeño de seguridad de la información y la integración del aseguramiento del proceso de acuerdo al PESI.

Es de tener en cuenta la importancia que conlleva el diseño de un plan estratégico de seguridad de la información “PESI”, para La Corporación de Alta Tecnología para la Defensa “**CODALTEC**” quien ha puesto sus esfuerzos en el desarrollo de la región de Villavicencio (Meta), ya que está trabajando con ingenieros, para el desarrollo de sus actividades en el campo tecnológico. De esta manera apoya el progreso de la región y de los profesionales brindando oportunidades de impacto social y laboral mejorando el nivel de vida de las familias del Departamento del Meta, permitiendo que crezcan y se desarrollen profesionalmente en nuestra región.

4. MARCO TEORICO

4.1 MARCO CONCEPTUAL

El estudio se apoya de acuerdo a la siguiente regulación de la seguridad de la información que presenta una estrategia organizada para el diseño de la seguridad y la metodología de planeación, ejecución, verificación y actuar basado en la NTC-ISO-IEC 27001:2013; iniciando en el entendimiento de la organización, elección de los procesos críticos de la operación de la seguridad, realización del diagnóstico de seguridad de la información, identificación de las principales vulnerabilidades y amenazas, aplicando una metodología de gestión del riesgos para la gestión y tratamiento de riesgos de seguridad de la información; basado en las mejores prácticas de seguridad de la información, haciendo uso de las siguientes metodologías y técnicas de seguridad:

- NTC-ISO-IEC 27001:2013, es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma a la cual se certifican las organizaciones por auditores externos los SGS de las organizaciones.[49]

  La norma NTC-ISO-IEC 27001:2013, es una metodología para implementar la gestión de la seguridad de la información y permite medir la realidad del cumplimiento de las metas de la dirección de la empresa con procesos seguros.

- NITC-ISO/IEC 27002:2013 Código de buenas prácticas en gestión de la seguridad de la información[50].

  Es una guía de buenas prácticas en seguridad de la información refiere en detalle los objetivos de control y controles descritos en el Anexo A (de la NTC-ISO-IEC 27001:2013), narra resumidamente los objetivos de control y controles para ser seleccionados es necesario argumentar el porqué de la no aplicabilidad de los controles no implementados durante el proceso de planificación enmarcado en el ciclo deming de un SGSI.

---

[49] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS “ICONTEC”. NTC-ISO-IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá, 2013.

[50] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS “ICONTEC”. NTC-ISO-IEC 27002. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Controles. Bogotá, 2013.

- Gestión de procesos de TI es ITIL v3, IT Infrastructure Library. Un marco de gestión de los servicios de tecnologías de la información, que consta de cinco partes: estrategia, diseño, transición, operación y mejora continua de servicios[51].

  Se hará uso de las directrices de ITIL, para la planeación y puesta en marcha de los procesos de seguridad de la información y establecimiento de los indicadores de control de dichos procesos para su evaluación y mejoramiento continuo.

- Metodología MAGERIT es una "metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica" (Ministerio de Hacienda y Administraciones Públicas, 2012) de España. Está enfocada a las tecnologías de información como respuesta a su creciente importancia en las organizaciones.[52].

Para el desarrollo del trabajo se seleccionó la Metodología Magerit, que permite un mejor control y descripción de los activos, amenazas, vulnerabilidades, el impacto, el riesgo y los salvaguardas. Adicionalmente se rigen por varias etapas como son: planificación, análisis de riesgos, la gestión de los riesgos y la selección más efectiva de salvaguardas que ayuden a garantizar la protección de la información de la corporación.

Magerit permite analizar en forma metódica cada uno de los procesos, actividades y demás labores que pueden estar en riesgo, así como determinar las necesidades de seguridad, las posibles vulnerabilidades, las amenazas, controles de seguridad y los riesgos a las que se encuentra expuesta, así como niveles.

Riesgos: Posibilidad de ocurrencia de situaciones que afecten de manera positiva o negativa la consecución de los objetivos[53].

Es decir que un riesgo es toda evento que pueda ocurrir y que pueda imposibilitar el progreso normal de las actividades de la empresa obstaculizando el logro de sus objetivos.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. El primer paso en la Gestión de riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren

---

[51] IT GOVERNANCE INSTITUTE. Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa. IT Governance Institute, 2008

[52] GUEVARA CHUMÁN, Javier Gustavo. Aplicación de la Metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruíz Gallo. Universidad Nacional Pedro Ruiz Gallo. España, 2015.

[53] GUEVARA CHUMÁN, Javier Gustavo. Aplicación de la Metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruíz Gallo. Universidad Nacional Pedro Ruiz Gallo. España, 2015.

protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los elementos de Información. Debido a que la Seguridad Informática tiene como propósitos garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.

Vulnerabilidades: La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, las vulnerabilidades son debilidades que son aprovechadas por amenazas y generan un riesgo; es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Salvaguardas: Dispositivo implementado para reducir los riesgos[54].

Una vez analizados los activos, las amenazas y las vulnerabilidades que pueden afectar a los activos, se debe realizar un análisis de los controles (las salvaguardas) o medidas de seguridad ya implantadas en la empresa, de esa manera poder determinar los controles a ser implementados o evaluar la efectividad de los ya implantados.

Sistema de Seguridad Informática: es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados[55]

Para el diseño del Plan estratégico de seguridad de la Información “PESI”, para “**CODALTEC**”; se hizo uso de todo el respaldo teórico antes mencionado, el cual contiene un conjunto de normas y modelos diseñados con la finalidad de brindar

[54] GUEVARA CHUMÁN, Javier Gustavo. Aplicación de la Metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruíz Gallo. Universidad Nacional Pedro Ruiz Gallo. España, 2015

[55] ALEXA MILENA RODRIGUEZ PINTO, Alexa Milena Diseño de un Plan Estratégico para la Seguridad de Información tributaria en una entidad pública. Tesis de especialista. Institución Universidad Nacional Abierta y a Distancia. Bogotá, 2015.

soluciones de seguridad de la información y apoyo a la construcción de documentación y proyectos; mejorando y alineando los procesos de:

- Identificación de recursos críticos de seguridad de la información dentro de la operación y Servicios informáticos de "**CODALTEC**".
- Identificación de las amenazas y vulnerabilidades a las que están supeditados los procesos de seguridad de la información y los activos críticos durante su operación.
- Estimación de la probabilidad de materialización de cada una de las amenazas identificadas al explotar vulnerabilidades existentes en la seguridad de la información.
- Estimación del impacto de comprometer las operaciones del negocio y amenazar la seguridad de la información con la materialización de amenazas.
- Identificación de los controles y su efectividad que actualmente se tienen implementados para la seguridad de la información y que permiten la mitigación en mayor o menor medida de las fuentes de riesgo.
- Estimación de los niveles de riesgo residual a los cuales aún se encuentra expuesta la seguridad de la información.
- Identificación de hallazgos y recomendaciones de mejora para el manejo de la seguridad de la información.

4.2 MARCO LEGAL

Dentro de la legislación colombiana aplicada a la seguridad informática se tiene que:

- Ley estatutaria 1266 de 2008

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las Información es que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países[56].

Permite fundamentar el derecho que tenemos sobre nuestra información para conocerla, actualizarla y rectificarla la que ha sido recogida por terceros para su tratamiento y circulación, de esta manera podemos estar seguros de que la información que se maneja es la real y no será alterada.

[56] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1266 de 2008, Ley de conocimiento, actualización y rectificación de información en bases de datos. Diario Oficial. Bogotá, 2008.

- Ley 1273 de 2009.

"Ley de delitos informáticos por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[57]."

Esta ley permite la preservación y protección de la información que se maneja en los sistemas basados en las "TIC", y demás información que se maneja por terceros. De acuerdo con la Revista Cara y Sello*, "Durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos* (Daccach, 2019)*"*. Esta ley trata lo concerniente a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, teniendo en cuenta el Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático o red de telecomunicación, Interceptación de datos informáticos, Daño informático, Uso de software malicioso, Violación de datos personales, Suplantación de sitios web para capturar datos personales, Circunstancias de agravación punitiva; También de los atentados informáticos y otras infracciones, Hurto por medios informáticos y semejantes, Transferencia no consentida de activos; entre otras.

- Ley estatutaria 1581 de 2012[58].

Reglamentada por el Decreto Nacional 1377 por la cual se dictan las disposiciones generales para la protección de datos personales. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las Información que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política relativo a la intimidad personal y el Habeas Data; así como el derecho a la información consagrado en el artículo 20 de la misma.

Del mismo modo se debe evitar que un tercero maneje a su acomodo, de manera fraudulenta o ilegal los datos personales contenidos en las bases de datos. Se debe asegurar la privacidad y la protección de la información de datos personales, como exige la legislación y la reglamentación, cuando sea aplicable. (Ley 1273 de 2009, ley 1581 de 2012 y el Registro Nacional de Bases de Datos, en la Superintendencia de Industria y Comercio SIC, adicionando las políticas de tratamiento de la información).

- Decreto 1360 de 1989

---

[57] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009, Código Penal. Diario Oficial. Bogotá, 2009.

[58] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 de 2012, Ley de conocimiento, actualización y rectificación de información en bases de datos. Diario Oficial. Bogotá, 2012.

- ✓ Artículo 1o. De conformidad con lo previsto en la Ley 23 de 1982 sobre Derechos de Autor, el soporte lógico (software) se considera como una creación propia del dominio literario.
- ✓ Artículo 2o. El soporte lógico (software) comprende uno o varios de los siguientes elementos: el programa de computador, la descripción de programa y el material auxiliar. [59]

Por medio del decreto 1360, se puede determinar los derechos de autor de esta manera prevalece la autoría sobre cada una de las creaciones literarias, y de desarrollo de software.

- Ley 1712 de 2014

Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y excepciones a la publicidad de la información se dictan otras disposiciones[60].

Esta ley genera las directrices para regir el manejo de la transparencia y del derecho de acceso a la Información Pública, tanto para las empresas como para la persona natural.

4.3 MARCO REFERNCIAL- ANTECEDENTES

Según el libro Ingeniería e Investigación, Vol, No 3 (2010), Javier Andrés Arias Sanabria, Félix Antonio Cortés Aldana y Jaime Orlando Cortés Aldana, Ingenieros de Sistemas, Universidad Nacional de Colombia, Bogotá, Colombia; La planeación estratégica de sistemas de información (PESI) es el proceso por medio del cual una organización determina el portafolio de aplicaciones. El PESI ha sido descrito en términos de fases y tareas específicas. Las tareas son usualmente realizadas a mano y requieren de experiencia, como la matriz de procesos - organización (MPO) y la matriz procesos – clases de datos (MPC). Para desarrollar el software se hizo énfasis en las etapas de análisis, diseño e implementación del ciclo de vida de desarrollo de sistemas. Durante la etapa de análisis fue importante la revisión de la literatura y entrevistas semiestructuradas con expertos en PESI. Una *contribución especial del presente trabajo es el diseño e implementación de reportes estadísticos asociados a cada matriz.* La automatización de esta tarea ha facilitado a los estudiantes el proceso de análisis de la MPO y la MPC durante el desarrollo de los talleres de PESI para la asignatura de Gestión y Gerencia de Sistemas de Información (Ingeniería de Sistemas, Universidad Nacional de Colombia)*[61]*". Este estudio realizado en la Universidad Nacional para la generación de un software computacional que permita ejecutar estos trabajos automáticamente, tareas que se requieren para la planeación estratégica de sistemas de información (PESI), es el

[59] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 1360 de 1989. Diario Oficial. Bogotá, 1989.
[60] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública. Diario Oficial. Bogotá, 2014.
[61] https://revistas.unal.edu.co/index.php/ingeinv/article/view/18185/0

modelo por medio del cual una organización determina el portafolio de proyectos de seguridad de la información para ayudar a lograr los objetivos de negocios.

El anterior estudio dio directrices para el desarrollo del diagnóstico de la situación actual de la seguridad de la información de las actividades de la gerencia y de las áreas de Infraestructura, gestión de la configuración, arquitectura, bases de datos, oficina PMO, oficina de gestión de activos OGA, recursos humanos, seguridad de la información y desarrollo; para verificar el cumplimiento de los lineamientos de la Norma técnica NTC-ISO/IEC 27001:2013, además la matriz de riesgos críticos de los activos de información de la infraestructura tecnológica realizada a "**CODALTEC**".

La implementación de un plan estratégico de seguridad de la información "PESI" para "**CODALTEC**" se refiere a poder contar con una guía para la protección de información, tomando en cuenta para ello la siguiente normatividad:

De acuerdo con Lozano[62], para la elaboración y formulación de un PESI se han identificado las siguientes cinco etapas: 1) conocimiento de la organización, 2) diagnóstico, 3) alineación de los objetivos, 4) modelo de seguridad de la información, para terminar en la definición del plan estratégico de seguridad de la información donde se analizan y 5) priorizan las iniciativas y se establece el portafolio de proyectos de seguridad de la información. Estos tendiente a plantear que la empresa alcance en su PESI un estado de madurez a tres (3) años, lo cual es lo deseado con el fin de contribuir con el logro de los objetivos de negocio y salvaguardar la información de la organización.

[62] LOZANO OLAVE, Marisol. Diseño de un Plan Estratégico de Seguridad de Información (PESI) para una compañía del sector asegurador. Tesis de especialista. Institución Universitaria Politécnico Grancolombiano. Bogotá, 2017.

5. METODOLOGÍA

5.1 ENFOQUE DE LA INVESTIGACIÓN

Por sus características el estudio se inscribe dentro del enfoque mixto (cuanti-cualitativo), para realizar el diagnóstico de la situación actual de la seguridad de la información en **"CODALTEC",** y dar inicio a la investigación se recopilaron datos a los que se les dio un tratamiento estadístico. además, se adelantó una investigación de tipo descriptiva, considerando que según Hernández Sampieri, Collado y Batista este tipo de investigación "únicamente pretenden medir o recoger información de manera independiente o conjunta sobre las variables a las que se refieren"[63].

Con estos hallazgos se diseñó un Plan Estratégico de Seguridad de la Información "PESI", alineado con los objetivos estratégicos y conforme con los lineamientos de la Dirección de la Corporación de Alta Tecnología para la Defensa. **"CODALTEC"** se refiere a poder contar con una guía para la protección de información, revisando y elaborando las políticas y estándares de seguridad de la información, tomando en cuenta para ello la siguiente metodología: OSSTMM (Open-Source Security Testing Methodology Manual - Manual de la Metodología Abierta de Testeo de Seguridad), Versión número 364, el objetivo de este manual es crear un método aceptado para ejecutar un test de seguridad minucioso y cabal. Con el uso de esta metodología se podrá realizar una prueba de seguridad con todos sus pasos que permita detectar las amenazas y debilidades a las que pueda estar expuesta la infraestructura de T.I., las redes de comunicación y la información de **"CODALTEC"** permitiendo determinar cuáles son los controles que se deberían implementar.

Igualmente, esta metodología se apoya en la Gestión de procesos de TI -ITIL v3[65], la cual consta de cinco partes: estrategia, diseño, transición, operación y mejora continua de servicios. Lo que permite la definición de una infraestructura computacional segura que se acople a un modelo de seguridad de la información que mejore los procesos actuales de la Organización. Con la implementación de este proyecto se propone que se maneje y procese la información, en un entorno físico que otorgue las medidas de seguridad necesarias como lo es la buena gestión de seguridad para una Red LAN Interna que maneje la intranet de la Organización, protegida por un firewall interno que sirva de corta fuegos a la DMZ LAN, un firewall

---

[63] HERNÁNDEZ SAMPIERI, Roberto; COLLADO, Carlos y BATISTA, Paola. Metodología de investogación. Sexta Edición. Editorial Mc Graw Hill. México, 2010.

[64] ROJAS CARRIEL, Ángel y CASTRO PESANTES, Fernando. Análisis y detección de vulnerabilidades en los servidores públicos del centro de cómputo de la empresa intermediaria de ventas utilizando la metodología internacional OSSTMM. Tesis de pregrado en Ingeniero en Networking y Telecomunicaciones. Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas, 2015. 207 p.

[65] QUINTERO GÓMEZ, Luisa Fernanda. Modelo basado en ITIL para la Gestión de los Servicios de TI en la Cooperativa de Caficultores de Manizales. Tesis de Magister en Gestión y Desarrollo de Proyectos de Software. Manizales: Universidad Autónoma de Manizales. Facultad de Ingeniería, Maestría en Gestión y Desarrollo de Proyectos de Software, 2015. 207 p.

externo, junto con un Router; todo lo anterior son los servicios que protegen e impiden el acceso riesgoso a los servidores y la información de “**CODALTEC**”.

Es de tener en cuenta que estos servicios y actividades descritas anteriormente no se están generando para todos los servidores y estructuras de “CODALTEC”, es por ello que se sugiere a la Corporación de Alta Tecnología para la Defensa **“CODALTEC”**, generar los espacios necesarios para efectuar mejores prácticas, robustecer sus procesos, proteger sus servidores y activos de información, dejando evidencia y trazabilidad de las actividades; esta gestión tendrá un propósito la mejora de la seguridad asentado en los proyectos que se proponen establecer con el diseño de un plan estratégico de seguridad de la información” PESI”, basado en la NTC-ISO-IEC 27001:2013 y la NTC-ISO/IEC 27002, se le ofrecerá un instrumento que facilite y ayude a la gestión del cambio a concientizar a sus funcionarios, en la importancia de la seguridad de la información, respondiendo a los requerimientos de la confidencialidad, integridad y disponibilidad de la misma.

A continuación, en el apartado siguiente se realiza el desarrollo de cada una de las actividades que hicieron posible la construcción del Diseño del PESI.

6. DISEÑO DEL PLAN ESTRAGEGICO DE SEGURIDAD DE LA INFORMACIÓN PESI

El diseño del Plan Estratégico de la Seguridad de la Información “PESI” nace a partir de la importancia que simboliza para la Corporación de Alta Tecnología para la Defensa “**CODALTEC**” mantener la seguridad de la información garantizando y brindado mejoras continuas en sus procesos, con el objeto de que las actividades y los riesgos de información que de ellas se deriven sean perfectamente gestionados y administrados.

6.1 DIAGNOSTICAR LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN “CODALTEC”

Para el diagnóstico de la situación actual de la seguridad de la información en “**CODALTEC**” con respecto a políticas, procedimientos, normas y estándares de acuerdo con la NTC-ISO/IEC 27001:2013, se revisó la estructura organizacional frente a los dominios conceptuales de seguridad de la información descritos en la lista de chequeo (Ver Anexo A lista de chequeo).

6.1.1 ALCANCE

El estudio de la situación actual tomará como base las actividades de la gerencia y de las áreas de Infraestructura, Gestión de la configuración, arquitectura, bases de datos, oficina PMO, oficina de gestión de activos OGA, Recursos Humanos, seguridad de la información y desarrollo, para verificar el cumplimiento de los lineamientos rectores de la Norma técnica NTC-ISO/IEC 27001:2013 para gestionar adecuadamente la seguridad de la información de los activos críticos de su infraestructura tecnológica; cubriendo la información almacenada, procesada y transferida en sus procesos informáticos, conservando los principios de seguridad, confidencialidad, integridad y disponibilidad de la información.

6.1.2 POBLACIÓN Y MUESTRA

Como población se consideró 100 empleados de la Corporación de Alta Tecnología para la Defensa **“CODALTEC”**, de la ciudad de Villavicencio (Meta), quienes hacen parte de la División de modelado y simulación.

Del grupo de los 100 funcionarios, se tomó como muestra escogida el equivalente a 18 funcionarios de **“CODALTEC”** de la sede de Villavicencio, constituido por los jefes y líderes son personas idóneas y conocedoras de las actividades y procesos de estas dependencias que cuentan con la experticia necesaria para el desarrollo de esta actividad, elegidos de las áreas de Infraestructura, Gestión de la configuración, arquitectura, bases de datos, oficina PMO, oficina de gestión de activos OGA, Recursos Humanos, seguridad de la información y desarrollo así como

las personas involucradas que apoyen en el proceso de determinar las amenazas y vulnerabilidades de la seguridad informática de esta empresa.

De la muestra escogida correspondiente a los 18 funcionarios, fueron a quienes se les aplicaron los instrumentos de recolección de información.

6.1.3 INSTRUMENTOS DE RECOLECCIÓN

Para recopilar la información se utilizó un cuestionario como principal instrumento, aplicado a modo de encuesta, el cual se diseñó en base a las normas NTC-ISO-IEC 27001:2013 y los estándares de seguridad e NTC-ISO/IEC 27002.

También se diseñó y aplicó una entrevista no estructurada, a empleados claves que deben velar por la seguridad de la información en **"CODALTEC"**. A continuación, se relacionan los profesionales a los cuales se les efectúo las entrevistas relacionados con el dominio a evaluar:

Ver Tabla 1 los profesionales entrevistados:

Tabla 1. Profesionales entrevistados

Dominio	Cargo	Nombre
A.5 Política de la Seguridad de la Información	Gerente de proyecto	Coronel Diego Andrés Hernández Mosquera
A.6 Organización de la Seguridad de la Información	Gerente de Proyecto	Coronel Diego Andrés Hernández Mosquera
A.7 Seguridad de los Recursos Humanos	Gerente de Proyecto	Coronel Diego Andrés Hernández Mosquera
	Coordinador Recursos Humanos	Luz Mary Vargas Peña
	Coordinados SG SST	Ricardo León Chamucero
A.8 Gestión de Activos	Coordinador de Oficina de Gestión de Activos OGA	Edilberto Robles Cruz
	Coordinador PMO	Edwar Iván Carranza Moya
	Coordinador equipo de seguridad de la información	Luis Enrique Ariza Vargas
	Coordinador infraestructura	Julián Quintaco
	Administrador de servidores Infraestructura	Javier Leonardo Cerón Puentes
	Coordinador del Almacén - Inventarios	Nicolas Díaz

A.9 Control de Acceso	Coordinador Gestión de Acceso	Jhonattan Smith Peláez
	Coordinador infraestructura	Julián Quintaco
	Administrador de servidores Infraestructura	Javier Leonardo Cerón Puentes
	Coordinador de bases de datos	Ana María Hernández
	Administrador base de datos	Hugo Nelson Lizca
A.10 Criptografía	Coordinador infraestructura	Julián Quintaco
	Administrador de servidores Infraestructura	Javier Leonardo Cerón Puentes
A.11 Seguridad Física y del Entorno	Coordinador de Oficina de Gestión de Activos OGA	Edilberto Robles Cruz
	Asistente OGA	Angi Julieth Vargas
A.12 Seguridad de las Operaciones y A.13 Seguridad de las Comunicaciones	Coordinador infraestructura	Julián Quintaco
	Administrador de servidores Infraestructura	Javier Leonardo Cerón Puentes
	Arquitecto de software	Hernán Darío Díaz
	Coordinador de bases de datos	Ana María Hernández
	Administrador base de datos	Hugo Nelson Lizca
	Coordinador equipo de seguridad de la información	Luis Enrique Ariza Vargas
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	Coordinador de desarrollo	Numa Fernando Caicedo Ruíz
	Coordinador PMO	Edwar Iván Carranza Moya
	Coordinador infraestructura	Julián Quintaco
	Administrador de servidores Infraestructura	Javier Leonardo Cerón Puentes
	Seguridad de la información	Luis Enrique Ariza Vargas
	Arquitecto de software	Hernán Darío Díaz
	Coordinador de pruebas	Nicolás Mauricio Díaz Pérez
	Documentador	Erica Sofía Cely Granado
	Líder de modulo	Erika Velásquez
	Equipo de implementación	Jenifer Céspedes
A.15 Relaciones con los Proveedores	Gerente de Proyecto	Coronel Diego Andrés Hernández Mosquera
	Seguridad de la información	Luis Enrique Ariza Vargas

A.17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocio	Seguridad de la información	Luis Enrique Ariza Vargas
A.18 Cumplimiento	Gerente de Proyecto	Coronel Diego Andrés Hernández Mosquera
	Seguridad de la información	Luis Enrique Ariza Vargas

Fuente: Elaboración propia.

6.1.4 RESULTADOS

De acuerdo con la información suministrada por el personal entrevistado, se realizó un análisis, con porcentaje de cumplimiento de acuerdo con los controles descritos en la lista de chequeo (Ver Tabla 14 Anexo A lista de chequeo) concerniente a la NTC-ISO-IEC 27001:2013.

En la siguiente matriz se encuentran los resultados de la verificación del estándar NTC-ISO-IEC 27001:2013. Los hallazgos representan las deficiencias que podrían afectar en forma negativa la seguridad de la información (Ver Tabla 15 Anexo B matriz de hallazgos, recomendaciones y riesgos de los objetivos de control NTC – ISO/IEC 27001:2013).

Se realizó la valoración cuantitativa en la Matriz de cumplimiento por dominio según los objetivos de control del Anexo A de la norma ISO 27001:2013, permitiendo conocer los niveles de riesgo de cada objetivo de control (Ver Tabla 16 Anexo C valoración cuantitativa de los riesgos de los objetivos de control NTC – ISO/IEC 27001:2013).

El juicio de experto permite establecer los rangos para calificar el porcentaje de cumplimiento para cada control evaluado, de la siguiente forma:

Tabla 2. Rango de cumplimiento

% Cumplimiento	Descripción
76 a 100	Se califica cuando la organización implementa, cumple, revisa, monitorea y mejora continuamente, TODOS los requisitos que exige la NTC-ISO-IEC 27001:2013.
26 a 75	Se califica cuando la organización adopta ALGUNAS prácticas de seguridad de la información de la NTC-ISO-IEC 27001:2013.
0 a 25	Se califica cuando la organización NO logra cumplir las expectativas de seguridad que exige la NTC-ISO-IEC 27001:2013.

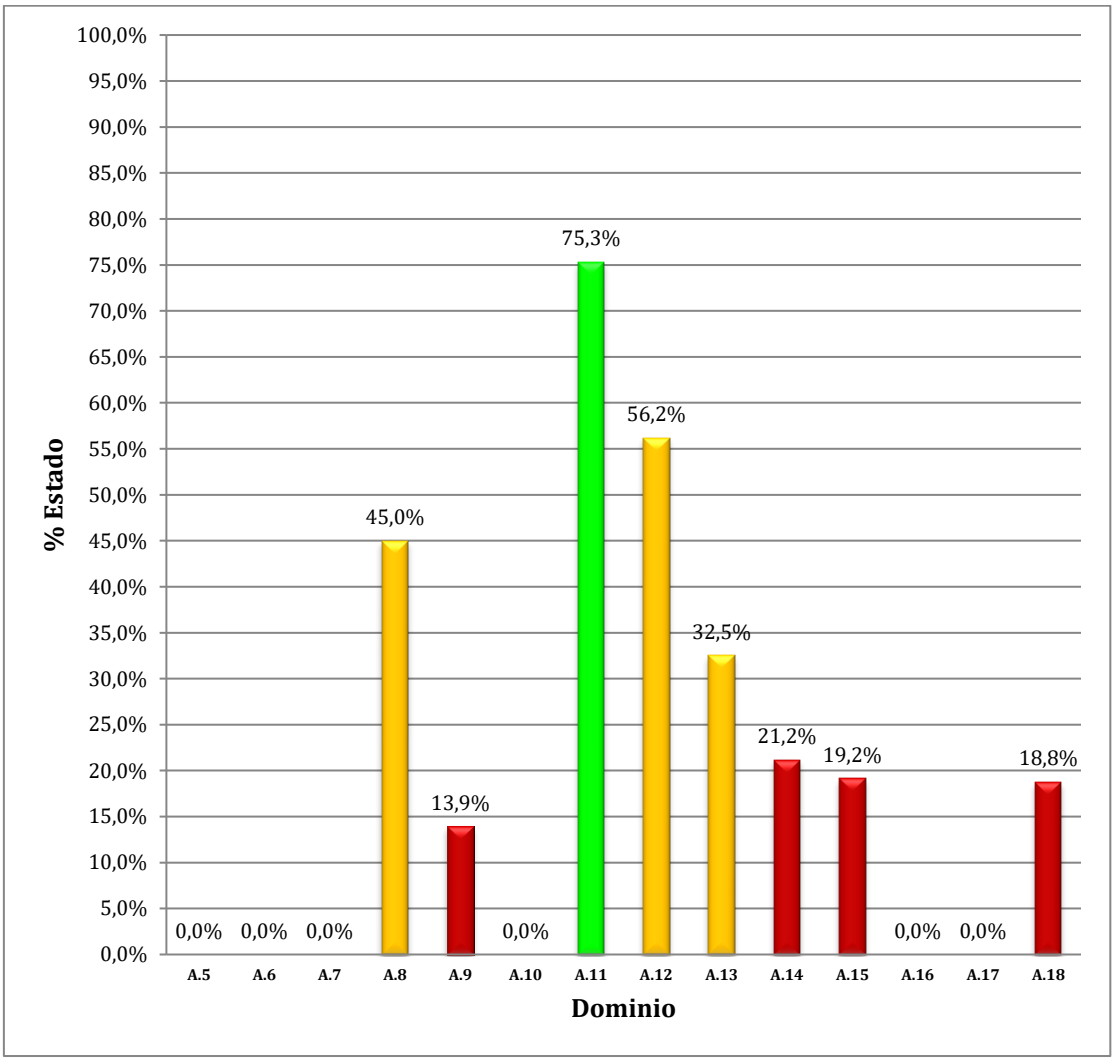
Fuente: Elaboración propia.

En la Figura 1 Cumplimiento por dominio de la NTC-ISO/IEC 27001:2013, muestra en escalas por colores y porcentajes de cumplimiento, la calificación de los dominios de la norma, la escala del nivel de cumplimento de 0% al 25% se califica cuando la organización NO logra cumplir las expectativas de seguridad de la información que exige la NTC-ISO/IEC 27001:2013 y se representa de color rojo. Allí están los dominios A.5, A.6, A.7, A.9, A.10, A.14, A.15, A.16, A.17 y A.18.

Para la escala del nivel de cumplimento entre 26% al 75% se califica cuando la organización adopta ALGUNAS prácticas de seguridad de la información de la NTC-ISO/IEC 27001:2013 y se representa de color amarillo. En esta escala están los dominios el A.8, A.12 y A.13.

Finalmente, en la Escala del nivel de cumplimento entre 76% al 100% se califica cuando la organización según su objeto implementa, cumple, revisa, monitorea y/o mejora continuamente, Todos los requisitos que exige la NTC-ISO/IEC 27001:2013, y se representa de color verde. En esta escala de calificación está el dominio A.11.

Figura 1. Cumplimiento por dominio NTC - ISO/IEC 27001:2013



A.5 Política de la Seguridad de la Información
A.6 Organización de la Seguridad de la Información
A.7 Seguridad de los Recursos Humanos
A.8 Gestión de Activos
A.9 Control de Acceso
A.10 Criptografia
A.11 Seguridad Fisica y Ambiental
A.12 Seguridad de las Operaciones
A.13 Seguridad de las Comunicaciónes
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas
A.15 Relaciónes con los Proveedores
A.16 Gestión de Incidentes de la Seguridad de la Información
A.17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad de Negocio
A.18 Cumplimiento

Fuente: Elaboración propia.

En la Figura 1 se presentan la compilación del resultado del análisis del cumplimiento por dominio de los objetivos de control de la NTC-ISO/IEC 27001:2013 que de manera parcial y no formal se encuentran aplicados en la Corporación de Alta Tecnología para la Defensa "**CODALTEC**".

Los resultados obtenidos de la situación actual del cumplimiento por dominio de los objetivos de control de la NTC-ISO/IEC 27001:2013, son base fundamental para el desarrollo de actividades encaminadas a la búsqueda de la seguridad de la información en "**CODALTEC**". El proceso de evaluar el riesgo surge de un peligro teniendo en cuenta la suficiencia de los controles existentes y de decidir si el riesgo es aceptable o no. Los riesgos de seguridad detectados del cumplimiento por dominio de los objetivos de control de la NTC-ISO/IEC 27001:2013 se encuentran definidos en la Tabla 15 Anexo B Matriz de Hallazgos, Recomendaciones y Riesgos, la valoración se realizó de acuerdo con el impacto y a la probabilidad de ocurrencia de la materialización de los riegos por dominio de los objetivos de control de la NTC-ISO/IEC 27001:2013, los que fueron valorados en Riesgo Extremo, Riesgo Medio, Riesgo Alto, Riesgo Inusual y Riesgo Bajo.

La probabilidad se clasifica en 1-Insignificante, 2- Menor, 3- Moderado, 4-Mayor y 5- Catastrófico y el impacto se define como 1-Raro, 3-Posible, 4-Probable y 5-Certero.

Los riesgos arrojados del cumplimiento por dominio de los objetivos de control de la NTC-ISO/IEC 27001:2013, fueron valorados según el criterio del experto, la información arrojada en el análisis de las entrevistas, la probabilidad y el impacto del riesgo.

Los cuadrantes de color Rojo son riesgos que presentan condiciones críticas que afectan de manera critica el impacto.

Los riegos que se encuentran en los cuadrantes de color naranja y color amarillo se pueden corregir y adoptar medidas de control para mitigar el impacto.

Los riesgos de color Verde pueden mejorar si es posible. Los riesgos en el cuadrante de color Azul, se deben mantener las medidas de control en forma periódica asegurando que el riesgo es aceptable.

6.2 DISEÑAR EL PROCEDIMIENTO PARA LA IDENTIFICACIÓN DE RIESGOS DE LAS OPERACIONES Y LA SEGURIDAD DE LA INFORMACIÓN DE “CODALTEC”

A continuación, se relaciona el procedimiento que se diseñó para hacer la identificación de riesgos de las operaciones y la seguridad de la información:
A partir de toda la información recopilada referente a los activos de información de las áreas de Infraestructura, Gestión de la configuración, arquitectura y bases de datos, en la Corporación de Alta Tecnología para la Defensa en **“CODALTEC”**, relacionada con el análisis y evaluación de los riesgos a los que están expuestos sus activos de información.

En la Tabla 7 se encuentra la clasificación de los activos según la metodología MAGERIT y NTC-ISO-IEC 27001:2013, de acuerdo con los pilares de seguridad confidencialidad, integridad y disponibilidad de los activos de información (Ver Tabla 7).

La Tabla 8 relaciona la matriz de riesgos activos críticos informáticos bajo la metodología MAGERIT y NTC-ISO-IEC 27001:2013, donde se incluye información como: propietario responsable del activo, la ubicación de este activo dentro de las diferentes áreas de la empresa y clasificación (Ver Tabla 8), con los que cuenta la empresa y sobre los cuales se realiza el proceso de identificación y evaluación de riesgos.

6.2.1 IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

A continuación, se clasifican los activos de información de acuerdo con las siguientes nomenclaturas de la metodología MAGERIT:

Tabla 3. Nomenclatura según MAGERIT

NOMENCLATURA	DESCRIPCIÓN
[D]	DATOS
[K]	CLAVES CRIPTOGRAFICAS
[S]	SERVICIOS
[SW]	SOFTWARE
[HW]	EQUIPAMENTO INFORMÁTICO
[COM]	REDES DE COMUNICACIONES
[Media]	SOPORTE DE INFORMACIÓN
[AUX]	EQUIPAMENTO AUXILIAR
[L]	INSTALACIONES

Fuente: Magerit

6.2.2 VALORACIÓN DE ACTIVOS

La valoración de los activos se realizó a empleados propietarios de los activos que deben velar por la seguridad de la información en **"CODALTEC"**.

Para realizar la valoración de los activos, es necesario hacer uso de la información referentes a dimensiones y escala de valoración, sugeridas por la Metodología Magerit.

Tabla 4. Dimensiones valoración de activos

Nomenclatura	Descripción
[D]	Disponibilidad
[I]	Integridad de los Datos
[C]	Confidencialidad de la Información

Fuente: Magerit V3 libro 2 Catalogo de elementos

6.2.3 DETERMINAR AMENAZAS Y VULNERABILIDADES

Se procede a identificar y asociar las amenazas, vulnerabilidad y el riesgo que cada activo.

Tabla 5. Análisis de amenazas según Magerit

ID Activo	Evento de amenaza	Capacidad	Motivación
1	[E2] Errores del administrador	3	3
2	[E2] Errores del administrador	3	3
3	[E2] Errores del administrador	2	1
4	[E2] Errores del administrador	2	1
5	[E2] Errores del administrador	2	1
6	[E2] Errores del administrador	1	1
7	[E2] Errores del administrador	1	1
8	[E2] Errores del administrador	2	1
9	[E2] Errores del administrador	2	1
10	[E2] Errores del administrador	2	1
11	[E2] Errores del administrador	1	1
12	[E20] Vulnerabilidades de los programas (software)	3	2
13	[E20] Vulnerabilidades de los programas (software)	3	2
14	[E20] Vulnerabilidades de los programas (software)	3	2
15	[E2] Errores del administrador	1	2
16	[E2] Errores del administrador	3	2
17	[E1] Errores de los usuarios	3	2
18	[E2] Errores del administrador	1	2
19	[E8] Difusión de software dañino	1	2
20	[E2] Errores del administrador	2	2
21	[E2] Errores del administrador	2	2
22	[E2] Errores del administrador	2	2
23	[E2] Errores del administrador	2	2
24	[E2] Errores del administrador	2	2
25	[E20] Vulnerabilidades de los programas (software)	2	3

ID Activo	Evento de amenaza	Capacidad	Motivación
26	[E20] Vulnerabilidades de los programas (software)	2	3
27	[E20] Vulnerabilidades de los programas (software)	2	3
28	[E20] Vulnerabilidades de los programas (software)	2	3
29	[E20] Vulnerabilidades de los programas (software)	2	3
30	[E20] Vulnerabilidades de los programas (software)	1	3
31	[E20] Vulnerabilidades de los programas (software)	2	3
32	[E2] Errores del administrador	2	3
33	[E20] Vulnerabilidades de los programas (software)	2	3
34	[E20] Vulnerabilidades de los programas (software)	1	3
35	[E20] Vulnerabilidades de los programas (software)	1	3
36	[E1] Errores de los usuarios	1	3
37	[E1] Errores de los usuarios	2	3
38	[E1] Errores de los usuarios	2	3
39	[E1] Errores de los usuarios	2	3
40	[E2] Errores del administrador	3	2
41	[E2] Errores del administrador	3	2
42	[E2] Errores del administrador	2	2
43	[E2] Errores del administrador	2	2
44	[E2] Errores del administrador	2	2
45	[A24] Denegación de servicio	2	2
46	[I8] Fallo de servicios de comunicaciones	2	2
47	[A24] Denegación de servicio	3	3
48	[I8] Fallo de servicios de comunicaciones	3	2
49	[I8] Fallo de servicios de comunicaciones	3	2
50	[I8] Fallo de servicios de comunicaciones	3	2
51	[I8] Fallo de servicios de comunicaciones	3	2
52	[I8] Fallo de servicios de comunicaciones	3	2
53	[I8] Fallo de servicios de comunicaciones	3	2
54	[I8] Fallo de servicios de comunicaciones	3	2
55	[I8] Fallo de servicios de comunicaciones	3	2
56	[I8] Fallo de servicios de comunicaciones	2	2
57	[I8] Fallo de servicios de comunicaciones	3	2
58	[E23] Errores de mantenimiento / actualización de equipos (hardware)	3	2
59	[E23] Errores de mantenimiento / actualización de equipos (hardware)	3	2
60	[E23] Errores de mantenimiento / actualización de equipos (hardware)	3	2
61	[E23] Errores de mantenimiento / actualización de equipos (hardware)	1	2
62	[E23] Errores de mantenimiento / actualización de equipos (hardware)	1	2

Fuente: Elaboración propia

La Tabla 6 en la que se relaciona las vulnerabilidades identificadas sobre los activos de información a través de la valoración de estos de acuerdo con el grado de afectación.

Tabla 6. Análisis de vulnerabilidades según Magerit

ID ACTIVO	VULNERABILIDAD	SEVERIDAD	EXPOSICIÓN
1	Falta de control de accesos	3	3
2	Falta de seguridad en los servidores que prestan los servicios de la empresa.	3	3
3	Falta de seguridad en los servidores que prestan los servicios de la empresa.	2	1
4	Falta de seguridad en los servidores que prestan los servicios de la empresa.	2	1
5	Falta de seguridad en los servidores que prestan los servicios de la empresa.	2	1
6	Falta de seguridad en los servidores que prestan los servicios de la empresa.	1	1
7	Falta de seguridad en los servidores que prestan los servicios de la empresa.	1	1
8	Falta de seguridad en los servidores que prestan los servicios de la empresa.	2	1
9	Falta de seguridad en los servidores que prestan los servicios de la empresa.	2	1
10	Falta de seguridad en los servidores que prestan los servicios de la empresa.	2	1
11	Falta de seguridad en los servidores que prestan los servicios de la empresa.	1	1
12	Falta de monitoreo y seguimiento a la calidad del software desarrollado	3	3
13	Falta de monitoreo y seguimiento por el administrador	3	3
14	Falta de monitoreo y seguimiento por el administrador	3	3
15	Falta de monitoreo y seguimiento por el administrador	1	2
16	Falta de monitoreo y seguimiento por el administrador	3	2
17	Falta de monitoreo, seguridad y seguimiento por el administrador	3	2
18	Falta de monitoreo, seguridad y seguimiento por el administrador	1	2
19	Falta de monitoreo, seguridad y seguimiento por el administrador	1	2
20	Falta de monitoreo, seguridad y seguimiento por el administrador	2	2
21	Falta de monitoreo, seguridad y seguimiento por el administrador	2	2
22	Falta de monitoreo, seguridad y seguimiento por el administrador	2	2
23	Falta de monitoreo, seguridad y seguimiento por el administrador	2	2
24	Falta de monitoreo, seguridad y seguimiento por el administrador	2	2
25	Errores de usuarios, programadores y administrador	2	3
26	Errores de usuarios, programadores y administrador	2	3
27	Errores de usuarios, programadores y administrador	2	3
28	Errores de usuarios, programadores y administrador	2	3

ID ACTIVO	VULNERABILIDAD	SEVERIDAD	EXPOSICIÓN
29	Errores de usuarios, programadores y administrador	2	3
30	Errores de usuarios, programadores y administrador	1	3
31	Errores de usuarios, programadores y administrador	2	3
32	Errores de omisión por el administrador	2	3
33	Errores de usuarios, programadores y administrador	2	3
34	Errores de usuarios, programadores y administrador	1	3
35	Errores de usuarios, programadores y administrador	1	3
36	Errores de usuarios, programadores y administrador	1	3
37	Errores de usuarios, programadores y administrador	2	3
38	Errores de usuarios, programadores y administrador	2	3
39	Errores de usuarios, programadores y administrador	2	3
40	Falta de control sobre el HW de la empresa por el administrador.	3	2
41	Falta de control sobre el HW de la empresa por el administrador.	3	2
42	Falta de control sobre el HW de la empresa por el administrador.	2	2
43	Falta de control sobre el HW de la empresa por el administrador.	2	2
44	Falta de control sobre el HW de la empresa por el administrador.	2	2
45	Falta de control sobre el HW de la empresa por el administrador.	2	2
46	Falta de control sobre el HW de la empresa por el administrador.	2	2
47	Errores de omisión por el administrador	3	3
48	Falta de control sobre el HW de la empresa por el administrador.	3	2
49	Falta de control sobre el HW de la empresa por el administrador.	3	2
50	Falta de control sobre el HW de la empresa por el administrador.	3	2
51	Falta de control sobre el HW de la empresa por el administrador.	3	2
52	Falta de control sobre el HW de la empresa por el administrador.	3	2
53	Falta de control sobre el HW de la empresa por el administrador.	3	2
54	Falta de control sobre el HW de la empresa por el administrador.	3	2
55	Falta de control sobre el HW de la empresa por el administrador.	3	2
56	Falta de control sobre el HW de la empresa por el administrador.	2	2
57	Falta de control sobre el HW de la empresa por el administrador.	3	2
58	Falta de control sobre el HW de la empresa por el administrador.	3	2
59	Falta de control sobre el HW de la empresa por el administrador.	3	2
60	Falta de control sobre el HW de la empresa por el administrador.	3	2
61	Falta de control sobre el HW de la empresa por el administrador.	1	2
62	Falta de control sobre el HW de la empresa por el administrador.	1	2

ALTO	*3*	*MEDIO*	*2*	*BAJO*	*1*

Fuente: Elaboración propia

Tabla 7. Clasificación de activos según Magerit

ID	Activo de información	Confidencialidad	Integridad	Disponibilidad	Total	Valor
1	(S) Control de acceso	25	25	25	25	Critico
2	(S) Disponibilidad Servicio Directorio Activo	25	25	25	25	Critico
3	(S) Certificados VPN para acceso remoto a la LAN	25	25	25	25	Critico
4	(S) Disponibilidad del Programa para gestión documental ORFEO, se utiliza para almacenar la información de todo el proyecto	25	25	25	25	Critico
5	(S) Disponibilidad del Servicio de Chat Corporativo	15	15	15	15	Medio
6	(S) Disponibilidad de Plataforma de monitoreo Zabbix	15	15	15	15	Medio
7	(S) Disponibilidad del Servicio TFS	15	15	15	15	Medio
8	(S) Disponibilidad del Servicio Canal de Internet dedicado	20	20	20	20	Alto
9	(S) Disponibilidad del Servicio Canal de Internet compartido	20	20	20	20	Alto
10	(S) Disponibilidad del Servicio Canal MPLS (Century Link)	20	20	20	20	Alto
11	(S) Disponibilidad del Certificado SSL (BlueHost)	15	15	15	15	Medio
12	(SW) Disponibilidad del Programa para gestión documental ALFRESCO, se utiliza para almacenar la información de toda la empresa.	25	25	25	25	Critico
13	(SW) Disponibilidad del Firewall	25	25	25	25	Critico
14	(SW) Disponibilidad Servicio de WAF	25	25	25	25	Critico
15	(SW) Vigencia del Software Licenciado - Mantenimiento	15	15	15	15	Medio
16	(S) Políticas de Backup - Drive, Alfresco, Servidor de Virtualización, Backup Retención	25	25	25	25	Critico
17	(S) Histórico de ataques informáticos detectados - Incidentes de seguridad	25	25	25	25	Critico
18	(S) Disponibilidad del Agente de Seguridad DLP	15	15	15	15	Medio
19	(SW) Disponibilidad del antivirus Symantec.	15	15	15	15	Medio
20	(S) Base de Datos Desarrollo (DEV - DEVPRO)	20	20	20	20	Alto
21	(S) Base de Datos Pruebas (QA - QAPRO)	20	20	20	20	Alto
22	(S) Backups Productivo	20	20	20	20	Alto
23	(S) Backups Desarrollo	20	20	20	20	Alto
24	(S) Backups Pruebas	20	20	20	20	Alto
25	(SW) Código PL/SQL - Objetos BD	15	15	15	15	Medio
26	(SW) Código ETL	15	15	15	15	Medio
27	(SW) Diseño Modelo base de datos	15	15	15	15	Medio
28	(D) Archivos Credenciales de acceso	15	15	15	15	Medio
29	(D) Desarrollo (DEV - DEVPRO)	15	15	15	15	Medio
30	(D) Pruebas (QA - QAPRO)	15	15	15	15	Medio
31	(SW) Código fuente	15	15	15	15	Medio
32	(S) Credenciales de acceso	15	15	15	15	Medio
33	(D) Despliegue de Datos aplicativo	15	15	15	15	Medio

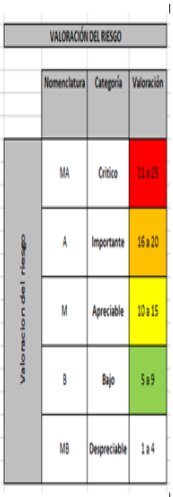
ID	Activo de información	Confidencialidad	Integridad	Disponibilidad	Total	Valor
34	(D) Documento de estándar de codificación	9	9	9	9	Bajo
35	(D) Documento de arquitectura	9	9	9	9	Bajo
36	(D) Manual del servicio Web IVR	20	20	20	20	Alto
37	(D) Manual del servicio de escaner	20	20	20	20	Alto
38	(D) Manual de instalación de Impresora de carnet	20	20	20	20	Alto
39	(SW) Diagramas de procesos del área de arquitectura	9	9	9	9	Bajo
40	(HW) Repositorio Google Drive	25	25	25	25	Critico
41	(HW) Controlador de Dominio	25	25	25	25	Critico
42	(HW) PFSENSE GOLD, Exportar a Xml	20	20	20	20	Alto
43	(HW) Servidor VPN, CORREOS DE RESPUESTA	20	20	20	20	Alto
44	(HW) Servidor WAF local y producción	20	20	20	20	Alto
45	(HW) Infraestructura local	20	20	20	20	Alto
46	(HW) Infraestructura Google	20	20	20	20	Alto
47	(S) Servicios de Terceros	25	25	25	25	Critico
48	(HW) Equipo de la Gerencia	25	25	25	25	Critico
49	(HW) Equipo de Seguridad de la Información	25	25	25	25	Critico
50	(HW) Equipo de Arquitectura	25	25	25	25	Critico
51	(HW) Equipo de Administrador de Base de Datos	25	25	25	25	Critico
52	(HW) Equipo de Administrador Infraestructura	25	25	25	25	Critico
53	(HW) Infraestructura Github	25	25	25	25	Critico
54	(HW) Servidor de datos pruebas Infraestructura local	20	20	20	20	Alto
55	(HW) Servidor de datos Infraestructura local	25	25	25	25	Alto
56	(HW) Servidor de aplicativos Infraestructura local	25	25	25	25	Alto
57	(HW) Servidor de redes Infraestructura local	25	25	25	25	Alto
58	(HW) Daños archivos del Repositorio Google Drive	15	15	15	15	Medio
59	(HW) Repositorio de Google Drive	25	25	25	25	Alto
60	(HW) Servidor de Infraestructura Local	25	25	25	25	Alto
61	(HW) Equipos PC Infraestructura Local	15	15	15	15	Medio
62	(HW) Equipos portátiles Infraestructura Local	15	15	15	15	Medio

CRITICO	25	ALTO	20	MEDIO	15	BAJO	10

Fuente: Elaboración propia

Tabla 8. Matriz de riesgos activos críticos Magerit NTC - ISO/IEC 27001:2013

METODOLOGIA DE MAGERIT: VALORACION DEL RIESGO - APROBADA POR EL DIRECTOR.



VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Crítico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
(S) Control de acceso	CRITICO	25	20	25	25	25	24
(S) Disponibilidad Servicio Directorio Activo	CRITICO	25	20	25	25	25	24
(S) Certificados VPN para acceso remoto a la LAN	CRITICO	25	20	25	25	25	24
(S) Disponibilidad del Programa para gestión documental ORFEO.	CRITICO	25	20	25	25	25	24
(S) Disponibilidad del Servicio de Chat Corporativo	APRECIABLE	15	15	15	15	15	15
(S) Disponibilidad de Plataforma de monitoreo Zabbix	APRECIABLE	15	15	15	15	15	15
(S) Disponibilidad del Servicio TFS	APRECIABLE	15	15	15	15	15	15
(S) Disponibilidad del Servicio Canal de Internet dedicado	IMPORTANTE	20	20	20	20	20	20
(S) Disponibilidad del Servicio Canal de Internet compartido	IMPORTANTE	20	20	20	20	20	20
(S) Disponibilidad del Servicio Canal MPLS (Century Link)	IMPORTANTE	20	20	20	20	20	20
(S) Disponibilidad del Certificado SSL (BlueHost)	APRECIABLE	15	15	15	15	15	15
(SW) Disponibilidad del Programa para gestión documental ALFRESCO.	CRITICO	25	20	25	25	25	24
(SW) Disponibilidad del Firewall	CRITICO	25	20	25	25	25	24
(SW) Disponibilidad Servicio de WAF	CRITICO	25	20	25	25	25	24
(SW) Vigencia del Software Licenciado - Mantenimiento	APRECIABLE	15	15	15	15	15	15
(S) Políticas de Backup - Drive, Alfresco, Servidor de Virtualización, Backup Retención	CRITICO	25	20	25	25	25	24
(S) Histórico de ataques informáticos detectados - Incidentes de seguridad	CRITICO	25	20	25	25	25	24
(S) Disponibilidad del Agente de Seguridad DLP	APRECIABLE	15	15	15	15	15	15
(SW) Disponibilidad del antivirus Symantec.	APRECIABLE	15	15	15	15	15	15
(S) Base de Datos Desarrollo (DEV - DEVPRO)	IMPORTANTE	20	20	20	20	20	20
(S)Base de Datos Pruebas (QA - QAPRO)	IMPORTANTE	20	20	20	20	20	20
(S) Backups Productivo	IMPORTANTE	20	20	20	20	20	20
(S) Backups Desarrollo	IMPORTANTE	20	20	20	20	20	20
(S) Backups Pruebas	IMPORTANTE	20	20	20	20	20	20
(SW) Código PL/SQL - Objetos BD	APRECIABLE	15	15	15	15	15	15

(SW) Código ETL	APRECIABLE	15	15	15	15	15	15
(SW) Diseño Modelo base de datos	APRECIABLE	15	15	15	15	15	15
(D) Archivos Credenciales de acceso	APRECIABLE	15	15	15	15	15	15
(D) Desarrollo (DEV - DEVPRO)	APRECIABLE	15	15	15	15	15	15
(D) Pruebas (QA - QAPRO)	APRECIABLE	15	15	15	15	15	15
(SW) Código fuente	APRECIABLE	15	15	15	15	15	15
(S) Credenciales de acceso	APRECIABLE	15	15	15	15	15	15
(D) Despliegue de Datos aplicativo	APRECIABLE	15	15	15	15	15	15
(D) Documento de estándar de codificación	BAJO	9	9	9	9	9	9
(D) Documento de arquitectura	BAJO	9	9	9	9	9	9
(D) Manual del servicio Web IVR	IMPORTANTE	20	20	20	20	20	20
(D) Manual del servicio de escaner	IMPORTANTE	20	20	20	20	20	20
(D) Manual de instalación de Impresora de carnet	IMPORTANTE	20	20	20	20	20	20
(SW) Diagramas de procesos del área de arquitectura	BAJO	9	9	9	9	9	9
(HW) Repositorio Google Drive	CRITICO	25	20	25	25	25	24
(HW) Controlador de Dominio	CRITICO	25	20	25	25	25	24
(HW) PFSENSE GOLD, Exportar a Xml	IMPORTANTE	20	20	20	20	20	20
(HW) Servidor VPN, CORREOS DE RESPUESTA	IMPORTANTE	20	20	20	20	20	20
(HW) Servidor WAF local y producción	IMPORTANTE	20	20	20	20	20	20
(HW) Infraestructura local	IMPORTANTE	20	20	20	20	20	20
(HW) Infraestructura Google	IMPORTANTE	20	20	20	20	20	20
(S) Servicios de Terceros	CRITICO	25	20	25	25	25	24
(HW) Equipo de la Gerencia	CRITICO	25	20	25	25	25	24
(HW) Equipo de Seguridad de la Información	CRITICO	25	20	25	25	25	24
(HW) Equipo de Arquitectura	CRITICO	25	20	25	25	25	24
(HW) Equipo de Administrador de Base de Datos	CRITICO	25	20	25	25	25	24
(HW) Equipo de Administrador Infraestructura	CRITICO	25	20	25	25	25	24
(HW) Infraestructura Github	CRITICO	25	20	25	25	25	24
(HW) Servidor de datos pruebas Infraestructura local	IMPORTANTE	20	20	20	20	20	20
(HW) Servidor de datos Infraestructura local	CRITICO	25	20	25	25	25	24
(HW) Servidor de aplicativos Infraestructura local	CRITICO	25	20	25	25	25	24
(HW) Servidor de redes Infraestructura local	CRITICO	25	20	25	25	25	24
(HW) Daños de archivos del Repositorio Google Drive	APRECIABLE	15	15	15	15	15	15
(HW) Repositorio de Google Drive	CRITICO	25	20	25	25	25	24
(HW) Servidor de Infraestructura Local	CRITICO	25	20	25	25	25	24
(HW) Equipos PC Infraestructura Local	APRECIABLE	15	15	15	15	15	15

Fuente: Elaboración propia

6.3 ANALIZAR LAS NECESIDADES E INICIATIVAS PARA EL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

Para la identificación de las necesidades e iniciativas para el diseño del plan estratégico de seguridad de la información PESI, primeramente se realizó el diagnóstico de la situación actual de la seguridad de la información en **"CODALTEC"**, tomando como guía la NTC-ISO-IEC 27001:2013 revisando cada uno de los dominios y objetivos de control frente a las actividades de cada dependencia, el resultado de este estudio se puede apreciar en la Figura 1 Cumplimiento por Dominio NTC-ISO-IEC 27001:2013.

Al valorar los resultados obtenidos en la aplicación de este estudio (Ver Anexo A lista de chequeo). Valoración cuantitativa de los riesgos hallados en la metodología de Magerit, se pudo identificar las necesidades en materia de Seguridad de la Información, por ello, después de un análisis se determinó que la prioridad de riesgos se encontraban en el cumplimiento de los objetivos de control de la Política de la Seguridad de la Información, Organización de la Seguridad de la Información, Seguridad de los Recursos Humanos, Control de acceso, Criptografía, Adquisición, desarrollo y mantenimiento de sistemas, Relaciones con los proveedores, Aspectos de seguridad de la información de la gestión de la continuidad de negocio y Cumplimiento.

En la Tabla 8 Matriz de riesgos activos críticos Magerit NTC-ISO/IEC 27001:2013, se evidencia que no se logran cumplir las expectativas de seguridad que exige la NTC-ISO-IEC 27001:2013; esta actividad permitió verificar estos resultados, dejando ver falencias en la seguridad de la información en **"CODALTEC"**.

6.3.1 PRIORIZACIÓN DE NECESIDADES E INICIATIVAS PARA EL PESI

A partir de identificar las necesidades e iniciativas para el PESI, del diagnóstico situación actual, el análisis y evaluación de riesgo, de realizar la valoración cuantitativa de la matriz de riesgos activos críticos según metodología Magerit y NTC-ISO-IEC 27001:2013 (ver tabla 4), permitiendo conocer los niveles de riesgo de cada objetivo de control (Ver Anexo C valoración cuantitativa de los riesgos de los objetivos de control NTC – ISO/IEC 27001:2013), del desarrollo minucioso realizado en el capítulo de la identificación de riesgos de las operaciones y la seguridad de la información y del análisis de sus resultados se puede determinar claramente las necesidades de seguridad de la información en **"CODALTEC",** las que se pueden minimizar con el diseño del plan estratégico de seguridad de seguridad de la información "PESI".

Para el Plan Estratégico de Seguridad de la Información "PESI", es de primordial importancia implementar el Sistema de gestión de seguridad de la información SGSI, en la Corporación de Alta Tecnología para Defensa "**CODALTEC**", ya que

según el análisis realizado a la situación actual de la seguridad de la información en "**CODALTEC**", esta es una de sus necesidades más apremiantes.

6.4 GENERAR UNA PLANEACIÓN PARA FORMULAR EL PORTAFOLIO DE PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta las necesidades priorizadas en "**CODALTEC**" en cuanto a la Seguridad de la Información se formula el siguiente portafolio de proyectos, el cual se basa en el diseño del plan estratégico de seguridad de la información PESI alineado a las necesidades de la corporación.

Tabla 9. Portafolio de proyectos de seguridad de la información para CODALTEC

PROYECTO	NOMBRE DEL PROYECTO	AÑOS			
		1	2	3	4
01	Planeación y aprobación del plan estratégico de seguridad de la información PESI.	X			
02	Elaboración del plan estratégico de seguridad de la información PESI.	X			
03	Creación del Comité de Seguridad de la Información CSI	X			
04	Planeación y ejecución del Sistema de Gestión de Seguridad de la Información SGSI	X			
05	Implementar la metodología y los procesos periódicos de Gestión de Riesgos de Seguridad de la información	X			
06	Implementación del Directorio Activo y el Sistema de control de acceso para dispositivos móviles e Implementación VPN'S en Teletrabajo.	X			
07	Adaptación de metodología para el desarrollo Seguro en las aplicaciones.	X			
08	Gestión de herramienta para cuentas privilegiadas	X			
9	Proyecto para la adquisición de herramienta para la mejor solución de respaldo y recuperación de Backup		X		
10	Proyecto de adquisición de software antivirus.		X		
11	Proyecto de adquisición de licenciamiento de software		X		
12	Implementación de Software para borrado seguro de Información		X		
13	Gestionar la adquisición de herramientas para soportar la infraestructura tecnológica en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.		X		
14	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información SGSI		X		
15	Auditorías internas de cumplimiento del Sistema de Gestión de Seguridad de la Información SGSI		X		
16	Adquisición de Software o servicio de análisis de vulnerabilidades y hacking Ético (plan de compras, grupo de trabajo, análisis de requerimientos)			X	
17	Adquisición de herramientas de cifrado de información automatizados, Repositorio centralizado de información cifrada.			X	

18	Gestionar una herramienta WAF para la protección de las aplicaciones WEB de **"CODALTEC"**			X	
19	Gestión de herramienta para cuentas privilegiadas			X	
20	Gestionar una solución de DLP (Data Los Prevention) para el correo Electrónico y equipos críticos.			X	
21	Auditorías internas de cumplimiento del Sistema de Gestión de Seguridad de la Información SGSI			X	
22	Proyecto de renovación tecnológica impresoras, servidores y PCs				X
23	Implementar el Desarrollo y Gestión del Proyecto del programa de continuidad del Negocio.				X
24	Implementar el Desarrollo y Gestión del Proyecto del programa de Recuperación ante desastres.				X
25	Implementación de Software para borrado seguro de Información				X
26	Verificación, Operación y mantenimiento del Sistema de Gestión de Seguridad de la información				X
27	Auditorías internas de cumplimiento del Sistema de Gestión de Seguridad de la Información SGSI				X

Fuente: Elaboración propia

6.4.1 IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI "CODALTEC"

Las buenas prácticas para desarrollar las estrategias de Tecnología de Información, y la implementación del Sistema de Gestión de la Información en "**CODALTEC**", se basan en el aseguramiento de la información, sus procesos, procedimientos y demás actividades, que son el pedestal sobre el que se construye la toma de decisiones de la Corporación. Con buenas prácticas de seguridad, la alta Dirección tiene certidumbre de que la información sobre la que sustentan sus decisiones es confiable, segura y está disponible cuando se le necesita. El Aseguramiento de la Información permite la utilización de información y de diferentes actividades operativas, con el fin de proteger la información, los sistemas de información y las redes de forma que se preserve la disponibilidad, integridad, confidencialidad, autenticación y el no repudio, ante el riesgo de impacto de amenazas locales, o remotas a través de comunicaciones e Internet.

Para lo cual se hace necesario la implementación del sistema de gestión de seguridad de la información- SGSI, además de contar con el apoyo incondicional de la gerencia y del recurso humano de "**CODALTEC**". Esta necesidad nace a partir de la importancia que representa para la Corporación de Alta Tecnología para Defensa "**CODALTEC"**, mantener la seguridad de la información garantizando y brindado mejoras continuas en sus procesos y la construcción de una infraestructura segura en cuanto a software, hardware, comunicaciones y construcción de sus proyectos.

La implementación del SGSI abarca claramente el marco de trabajo a corto, mediano y largo plazo alineado con las directrices vigentes de "**CODALTEC**", para

dar cumplimiento a los requisitos establecidos por la norma, se debe realizar un proceso juicioso y exhaustivo que cuente con un previo análisis, revisión y aprobación por la alta dirección.

Para el diseño e implementación del sistema de gestión de seguridad de la información SGSI, se deberá conformar el grupo de trabajo implementador del SGSI, quienes como metodología de trabajo para implementar el SGSI, "**CODALTEC**" tomarán como referencia la NTC-ISO-IEC 27001:2013, con el objeto de establecer, mantener y mejorar continuamente la seguridad de la información en la Corporación. Para el desarrollo de este proyecto se hace necesario el conocimiento del ciclo PHVA (Planear, Hacer, Verificar y Actuar).

Como parte integral para la implementación del SGSI se hace necesario en la etapa de planeación por parte del equipo implementador del SGSI tener en cuenta que se debe mantener una trazabilidad en la inter relación de las operaciones entre las diferentes dependencias manteniendo los principios de la seguridad como lo son la confidencialidad, integridad y disponibilidad de la información, todo lo anterior permitirá a "**CODALTEC**", preservar la seguridad de la información a nivel interno y externo además de mantener vigente la base del conocimiento de cada actividad que se ejecuta en la seguridad de la información.

6.5 FORMULAR LOS INDICADORES DE SEGURIDAD DE LA INFORMACIÓN EN CONCORDANCIA CON LO ELABORADO

6.5.1 IDENTIFICACIÓN DE INDICADORES

Para el diseño de los indicadores se seleccionaron las áreas más críticas como son bases de datos, arquitectura, documentación, e infraestructura y gestión de la configuración.

6.5.2 ANÁLISIS DE INDICADORES

La implementación de los indicadores de seguridad de la información, nació a partir de la importancia que representa para la Corporación de Alta Tecnología para Defensa "**CODALTEC"**, mantener la seguridad de la información garantizando y brindado mejoras continuas en sus procesos y la construcción de una infraestructura segura en cuanto a software, hardware, comunicaciones y construcción de sus proyectos, con el objeto de medir el rendimiento y la eficacia de las actividades que se implementarán como son los controles, salvaguardas y mecanismos de seguridad que proporcionaran la implementación del PESI alineado al SGSI, con el objetivo de especializar las actividades tecnológicas de cada área de la corporación.

De los indicadores analizados se resaltan como de mayor importancia por su criticidad las Políticas de Backup (Drive, Alfresco (Sistema gestor documental y contenidos), Servidor de Virtualización, Backup Retención), Histórico de ataques

informáticos detectados - Incidentes de seguridad, Vigencia del Software Licenciado - Disponibilidad agente de seguridad DLP y Disponibilidad del antivirus Symantec.

6.5.3 PRIORIZACIÓN DE INDICADORES

La priorización de los indicadores y de los aspectos de ordenación, seguimiento y valoración de los indicadores de seguridad de la información, dependen de la identificación de la criticidad de los riesgos que se han analizado para cada activo de la información en "**CODALTEC**". El diseño de los indicadores presentados para las áreas de bases de datos, arquitectura, documentación, e infraestructura y gestión de la configuración, permiten llevar una trazabilidad del cumplimiento de los controles de seguridad, contribuyen a minimizar y mitigar los riesgos latentes, sugerir posibilidades de intervención y seguir de cerca los resultados, en búsqueda de una mejora continua.

Para realizar un adecuado seguimiento y evaluar los procesos actuales se elaboran los siguientes indicadores de seguridad de la información:

Tabla 10. Indicadores de seguridad de la información, área infraestructura y gestión de la configuración

Nombre Activo	Variable Seguridad Información	Variable Seguridad Información	Formula	Valoración del Cumplimiento	Afecta	Riesgos	Controles	Evidencia
Control de Acceso	VSI16: Número de solicitudes de control de acceso recibidas en el mes. - Creación/modificación de cuentas de correo electrónico - Creación/modificación de usuarios del dominio - Creación/modificación de certificados VPN para acceso a la LAN de Codaltec - Creación/modificación de usuarios de Alfresco - Creación/modificación de usuarios del chat corporativo - Creación/modificación de usuarios de Team Foundation Server (TFS) - Creación/modificación de usuarios en los repositorios de código (GitHub) - Creación/modificación de usuarios para acceso a Wi-Fi.	VSI17 = Número de solicitudes de control de acceso atendidas en el mes	ISITI07 = (VSI17 * 100) / VSI16	ISITI07 > = 90% Satisfactorio 60% < = ISITI07 < 90% Regular ISITI07 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Pierda información • Roben información • Modificación información • No se genere el proceso de control de acceso	• Última versión en Correo • Informe mensual con el total de solicitudes recibidas y atendidas. • Control de acceso al equipo clave.	• Estadística herramienta GLPI • Solicitudes y respuestas por correo
Disponibilidad Servicio Directorio Activo	VSI18 Tiempo total transcurrido	VSI19 suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI08 = VSI18 - VSI19 /VSI18	ISITI08 > = 90% Satisfactorio 60% < = ISITI08 < 90% Regular ISITI08 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Plataforma de monitoreo zabbix del controlador de dominio
Disponibilidad servicio BlueHost (Zona DNS - Hosting - Site Backup Pro)	VSI120 = Tiempo total transcurrido	VSI21 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI09 = VSI20 - VSI21 /VSI20	ISITI09 > = 90% Satisfactorio 60% < = ISITI09 < 90% Regular ISITI09 < 60% No Satisfactorio	Disponibilidad Integridad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Evaluar monitoreo del servicio con Microsoft Insights
Disponibilidad del Programa para gestión documental ORFEO (sgd.codaltec.com), se utiliza para almacenar la información de todo el proyecto	VSI22 = Tiempo total transcurrido	VSI23 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI10 = VSI22 - VSI23 /VSI22	ISITI10 > = 90% Satisfactorio 60% < = ISITI10 < 90% Regular ISITI10 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Pierda • Roben • Modificación • No se genere	• Última versión en Correo • Backup del equipo del usuario • Backup Google Drive • Control de acceso al equipo clave. • Respaldo en el cliente	Evaluar monitoreo del servicio con Microsoft Insights

Disponibilidad del Programa para gestión documental ALFRESCO (files.codaltec.com), se utiliza para almacenar la información de todo el proyecto.	VSI24 = Tiempo total transcurrido	VSI25 = suma del tiempo de inactividad (minutos) D13	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI11= VSI24 - VSI25 /VSI24	ISITI11 > = 90% Satisfactorio 60% < = ISITI11 < 90% Regular ISITI11 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Pierda • Roben • Modificación • No se genere	• Última versión en Correo • Backup del equipo del usuario • Backup Google Drive • Control de acceso al equipo clave. • Respaldo en el cliente	Evaluar monitoreo del servicio con Microsoft Insights
Disponibilidad del Firewall	VSI26 = Tiempo total transcurrido	VSI27 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI12 = VSI26 - VSI27 /VSI26	ISITI12 > = 90% Satisfactorio 60% < = ISITI12 < 90% Regular ISITI12 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Monitoreo con zabbix
Disponibilidad Servicio de WAF	VSI28 = Tiempo total transcurrido	VSI29 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI13 = VSI28 - VSI29 /VSI28	ISITI13 > = 90% Satisfactorio 60% < = ISITI13 < 90% Regular ISITI13 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Monitoreo con Amplify y zabbix
Políticas de Backup - Drive, Alfresco, Servidor de Virtualización, Backup Retención	VSI30 = Cantidad de Backup cumplido Periodo de verificación	VSI31 = Cantidad de Backup realizados	ISITI14 = VSI30 /VSI31	ISITI14 > = 90% Satisfactorio 60% < = ISITI14 < 90% Regular ISITI14 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Evaluar monitoreo del servicio
Histórico de ataques informáticos detectados - Incidentes de seguridad	VSI32 = Cantidad de incidentes de seguridad Periodo de ver	VSI33 = Suma de incidentes de seguridad Ëxitosos	ISITI15 = VSI32 /VSI33 ISITI15 =Cantidad de incidentes de seguridad / Suma de incidentes de seguridad Ëxitosos	ISITI15 > = 90% Satisfactorio 60% < = ISITI15 < 90% Regular ISITI15 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Evaluar monitoreo del servicio

Disponibilidad del Servicio Canal de Internet dedicado (Claro)	VSI34 = Tiempo total transcurrido	VSI35 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI16= VSI34 - VSI35 /VSI34	ISITI16 >= 90% Satisfactorio 60% <= ISITI16 < 90% Regular ISITI16 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Reportes con el proveedor del servicio - Histórico de Ping
Disponibilidad del Servicio Canal de Internet compartido (Claro)	VSI36 = Tiempo total transcurrido	VSI37= suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI17 = VSI36 - VSI37/VSI36	ISITI17 >= 90% Satisfactorio 60% <= ISITI17 < 90% Regular ISITI17 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Reportes con el proveedor del servicio - Histórico de Ping
Disponibilidad del Servicio Canal MPLS (Century Link)	VSI38 = Tiempo total transcurrido	VSI39 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI18 = VSI38 - VSI39 /VSI38	ISITI18 >= 90% Satisfactorio 60% <= ISITI18 < 90% Regular ISITI18 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Reportes con el proveedor del servicio - Histórico de Ping
Vigencia del Software Licenciado - Disponibilidad agente de seguridad DLP Disponibilidad del antivirus Symantec.	VSI40 = Cantidad de licencias requeridas	VSI41 = cantidad de licencias renovadas	ISITI19 = VSI40/VSI41	ISITI19 >= 90% Satisfactorio 60% <= ISITI19 < 90% Regular ISITI19 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Matriz de licenciamiento
Disponibilidad del Servicio de Chat Corporativo	VSI42 = Tiempo total transcurrido	VSI43 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI20 = VSI42 - VSI43 /VSI42	ISITI20 >= 90% Satisfactorio 60% <= ISITI20 < 90% Regular ISITI20 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Evaluar monitoreo del servicio con Microsoft Insights

Disponibilidad de Plataforma de monitoreo Zabbix Codaltec	VSI44 = Tiempo total transcurrido	VSI45 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI21= VSI44 - VSI45 /VSI44	ISITI21 > = 90% Satisfactorio 60% < = ISITI21 < 90% Regular ISITIO21 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Disponibilidad local con zabbix
Disponibilidad de la Plataforma de monitoreo Zabbix Datacenter	VSI46 = Tiempo total transcurrido	VSI47 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI22 = VSI46 - VSI47 /VSI46	ISITI22 > = 90% Satisfactorio 60% < = ISITI22 < 90% Regular ISITI22 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Disponibilidad local con zabbix
Disponibilidad del Servicio TFS B2O	VSI48 = Tiempo total transcurrido	VSI49 = suma del tiempo de inactividad (minutos)	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI23 = VSI48- VSI49 /VSI48	ISITI23 > = 90% Satisfactorio 60% < = ISITI23 < 90% Regular ISITI23 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Evaluar monitoreo del servicio con Microsoft Insights

Fuente: Elaboración propia

Tabla 11. Indicadores de seguridad de la información, área documentación

Nombre Activo	Variable Seguridad Información	Variable Seguridad Información	Formula	Valoración del Cumplimiento	Afecta	Riesgos	Controles	Evidencia
Disponibilidad del Programa para gestión documental ALFRESCO (files.codaltec.com), se utiliza para almacenar la información de todo el proyecto.	VSI01 = Tiempo total transcurrido	VSI02 = suma del tiempo de inactividad (minutos) D13	Porcentaje de disponibilidad = (tiempo total transcurrido - suma del tiempo de inactividad)*100 / tiempo total transcurrido ISITI11= VSI01 - VSI02 /VSI01	ISIDOCO1 > = 90% Satisfactorio 60% < = ISIDOCO1 < 90% Regular ISIDOCO1 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Pierda • Roben • Modificación • No se genere	• Última versión en Correo • Backup del equipo del usuario • Backup Google Drive • Control de acceso al equipo clave. • Respaldo en el cliente	Evaluar monitoreo del servicio con Microsoft Insights
Disponibilidad repositorio GitHub	VSI03: Número de solicitudes recibidas en el mes. Repositorio de GitHub	VSI04 = Número de solicitudes atendidas en el mes	ISIDOCO2 = (VSI04 * 100) / VSI03	ISIDOCO2 > = 90% Satisfactorio 60% < = ISIDOCO2 < 90% Regular ISIDOCO2 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Pierda información • Roben información • Modificación información • No se genere el proceso de control de acceso	• Última versión en Correo • Informe mensual con el total de solicitudes recibidas y atendidas. • Control de acceso al equipo clave.	• Estadística herramienta GLPI • Solicitudes y respuestas por correo
Disponibilidad backups equipo de cómputo de cada integrante de documentación	VSI05 = Porcentaje cumplido de Backup por equipo Periodo de verificación = mensual	VSI06 = Porcentaje de Backup realizados	ISIDOC03 = VSI05 /VSI06	ISIDOCO3 > = 90% Satisfactorio 60% < = ISIDOCO3 < 90% Regular ISIDOCO3 < 60% No Satisfactorio	Disponibilidad	• Pierda información • Roben información • Modificación información • No se genere el proceso de Monitoreo	• Verificación periódica al cumplimiento de los indicadores	Evaluar monitoreo del servicio

Fuente: Elaboración propia

Tabla 12. Indicadores de seguridad de la información, área arquitectura

Nombre Activo	Variable Seguridad Información	Variable Seguridad Información	Formula	Valoración del Cumplimiento	Afecta	Riesgos	Controles	Evidencia
Creación de reléase para el código de aplicación	VSI01 = Número de reléase de código de aplicación generados por fase de desarrollo.	VSI02 = Número de despliegues de aplicación en ambiente productivo.	ISIARQ01= (#VSI01/#VSI02) *100 **METAS** MÍNIMA 75-80% SATISFACTORIA 80- 90% SOBRESALIENTE 100%	ISIARQ01 > = 90% Satisfactorio 60% < = ISIARQ01 < 90% Regular ISIARQ01 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Acceso no autorizado al repositorio de aplicación donde se alojen el versionamiento de Salud.SIS. • Alteración al código de aplicación sin realizar el versionamiento del reléase por despliegue.	• Control de acceso al repositorio de aplicación en GitHub. • Control de versionamiento del reléase de código de aplicación para cada despliegue en ambiente productivo.	• Repositorio de aplicación en herramienta GitHub.
Cantidad de ataques identificados en capa de aplicación e ignorados por el WAF	VSI03 = Número de ataques identificados en la aplicación de producción.	VSI04 = 1 mes	ISIARQ02= #VSI03/#VSI04 **METAS** ALERTA > 5 PROBABLE 1-5 ESPERADO 0	ISIARQ02 = 0 Satisfactorio 1 < = ISIARQ02 < 5 Regular ISIARQ02 > 5 No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Indisponibilidad total de la aplicación • Afectación en la integridad de los datos • Robo de información • Suplantación de identidad • Uso no autorizado del sistema	• Capa interna de protección de seguridad adicional en la aplicación	• Monitoreo en Herramienta Application Insights.

Fuente: Elaboración propia

Tabla 13. Indicadores de seguridad de la información, área base de datos

Nombre Activo	Variable Seguridad Información	Variable Seguridad Información	Formula	Valoración del Cumplimiento	Afecta	Riesgos	Controles	Evidencia
Implementación de ambientes (desarrollo y pruebas)	VSI01 = Número de copias de respaldo generadas en ambiente productivo para la implementación de ambientes (desarrollo - pruebas).	VSI02 = Número de ambientes (desarrollo - pruebas) implementados.	ISIBD01 = (#VSI01/#VSI02)*100 **METAS** MÍNIMA 75-80% SATISFACTORIA 80- 90% SOBRESALIENTE 100%	ISITI01 > = 90% Satisfactorio 60% < = ISITI01 < 90% Regular ISITI01 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Acceso no autorizado al repositorio donde se aloje el backup de ambiente productivo. • Corrupción de datos en el archivo de backup que impida su restablecimiento en los ambientes a implementar. • Pérdida del archivo con el backup de ambiente productivo.	• Control de acceso al repositorio de datos donde se aloje el backup de ambiente productivo. • Control de acceso al repositorio de datos que se defina en el servidor donde se implementará el ambiente (desarrollo o pruebas).	• Correos • Log de restauración del backup en los ambientes a implementar.
Creación de reléase para el código de base de datos	VSI03 = Número de reléase de código de base de datos generados por fase de desarrollo.	VSI04 = Número de despliegues de base de datos en ambiente productivo.	ISIBD02= (#VSI03/#VSI04) *100 **METAS** MÍNIMA 75-80% SATISFACTORIA 80- 90% SOBRESALIENTE 100%	ISITI02 > = 90% Satisfactorio 60% < = ISITI02 < 90% Regular ISITI02 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Acceso no autorizado al repositorio de base de datos donde se alojen el versionamiento del modelo de datos. • Alteración al código de base de datos sin realizar el versionamiento del reléase por despliegue.	• Control de acceso al repositorio de base de datos en GitHub. • Control de versionamiento del reléase de código de base de datos para cada despliegue en ambiente productivo.	• Repositorio de base de datos en herramienta GitHub.
Generación de modelos de datos	VSI05: Número de modelo de datos generados por fase de desarrollo.	VSI06: Número de reléase de código de base de datos con alteración al modelo de datos.	ISIBD03= (#VSI05/#VSI06) *100 **METAS** MÍNIMA 75-80% SATISFACTORIA 80- 90% SOBRESALIENTE 100%	ISITI03 > = 90% Satisfactorio 60% < = ISITI03 < 90% Regular ISITI03 < 60% No Satisfactorio	Confidencialidad Disponibilidad Integridad	• Acceso no autorizado al repositorio de base de datos donde se alojen el versionamiento del modelo de datos. • Alteración al modelo de datos sin realizar el versionamiento del mismo.	• Control de acceso al repositorio de base de datos en GitHub. • Control de versionamiento del modelo de datos con respecto a los despliegues de base de datos en ambiente productivo.	• Repositorio de base de datos en herramienta GitHub.

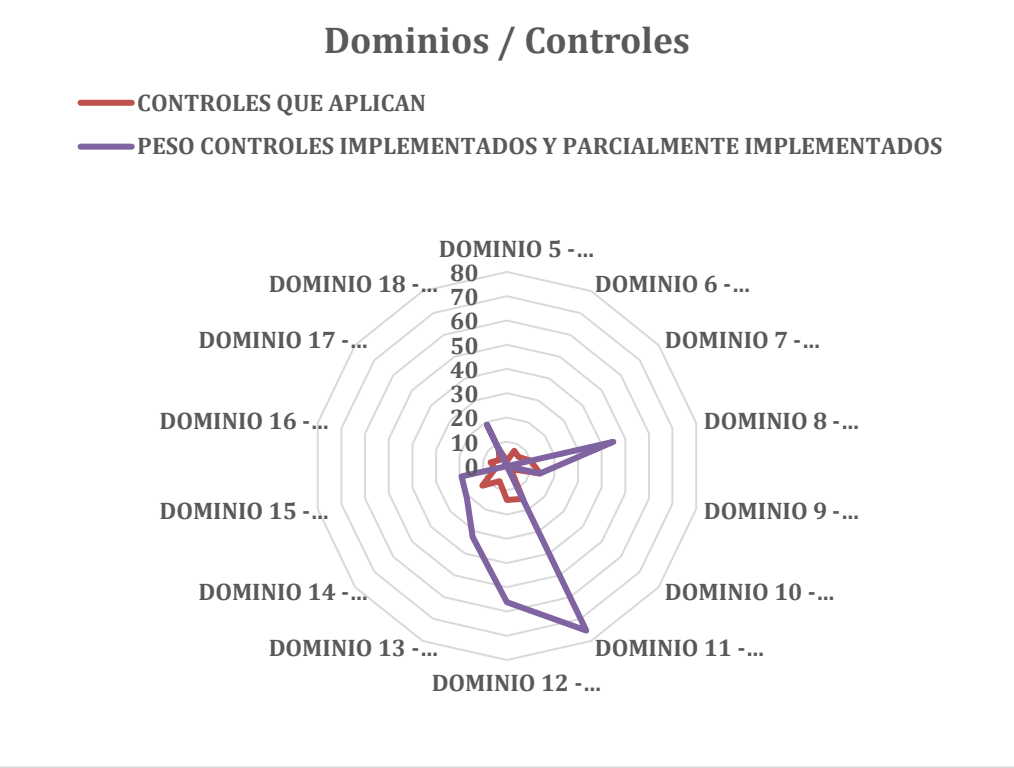
Fuente: Elaboración propia

7. RESULTADOS

Del resultado obtenido en el desarrollo de cada uno de los objetivos propuestos para la implementación del PESI en "**CODALTEC**", en este documento se describe como se realizó el diagnóstico de la situación actual de la seguridad de la información en "**CODALTEC**"; se narra cómo se realizaron las actividades para identificar, analizar y priorizar las necesidades e iniciativas para el Plan Estratégico de Seguridad de la Información "PESI"; especificando las necesidades para formular el portafolio de proyectos de seguridad de la información, y se generó la identificación de riesgos de las operaciones y la seguridad de la información de "**CODALTEC**", por último se formularon los indicadores de seguridad de la Información en concordancia con lo elaborado.

Con el fin de realizar el PESI en "**CODALTEC**" se requiere conocer el nivel actual de madurez en seguridad de la información en que se encuentra la Corporación de Alta Tecnología para la Defensa "**CODALTEC**" de acuerdo con el análisis de estándares de control NTC-ISO-IEC 27001:2013.

Figura 2. Dominios y controles cumplimiento NTC - ISO/IEC 27001:20132

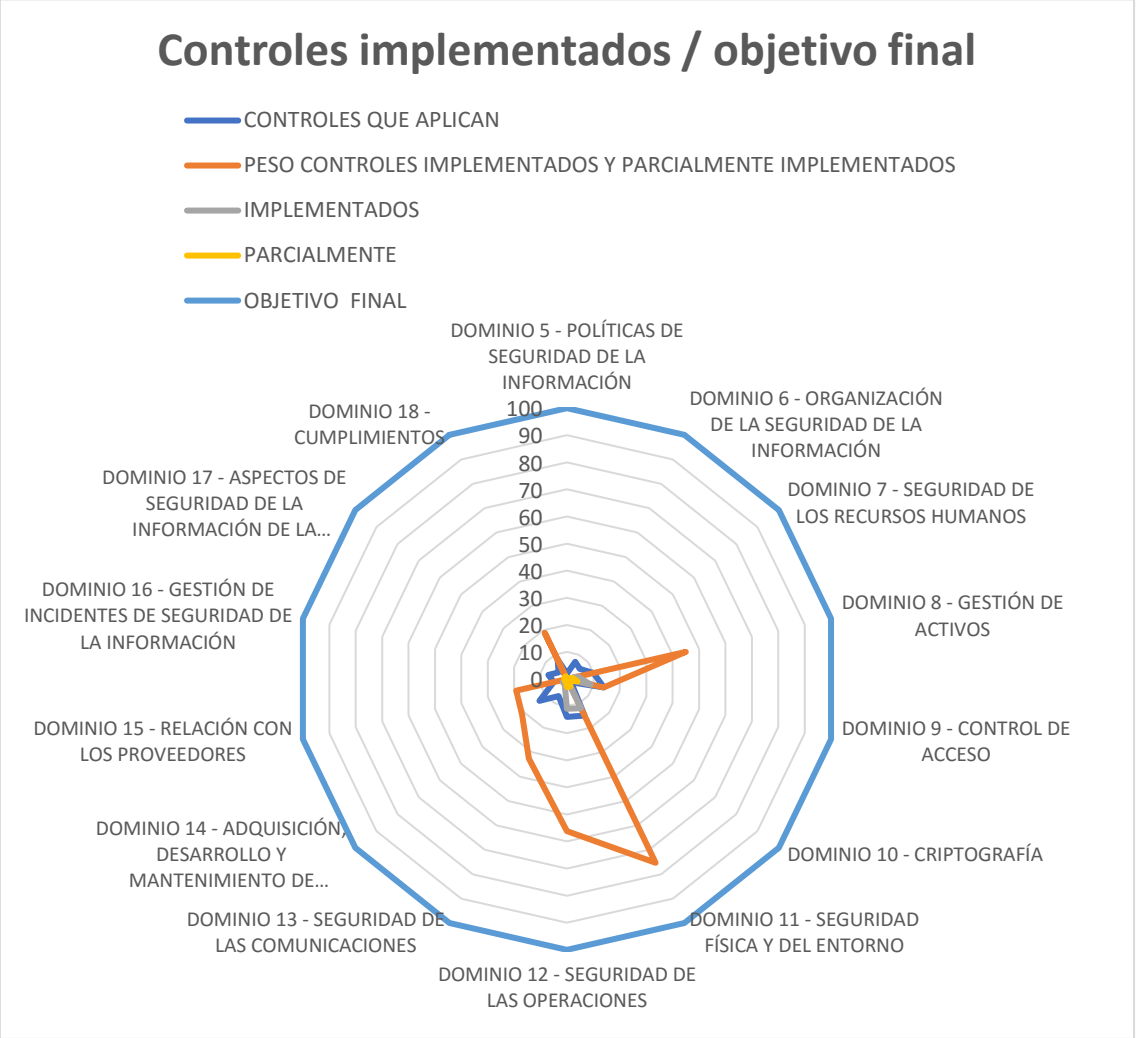


Fuente: Elaboración propia

De los resultados obtenidos en la Figura 1 Dominios y Controles cumplimiento NTC-ISO-IEC 27001:2013, se generan las bases para alcanzar la mejora continua del proceso de Seguridad de la Información de **CODALTEC**, a su vez identificar las decisiones de seguridad de la información. De acuerdo con los niveles de madurez alcanzados por cada uno de los dominios se plantea las prioridades sobre su implementación para alcanzar el nivel de madurez exigido por la NTC-ISO-IEC 27001:2013.

Para representar el nivel de madurez del modelo de seguridad de la información en "**CODALTEC**" y su porcentaje de cumplimiento de cada uno de los 14 dominios de NTC-ISO-IEC 27001:2013. Como se presenta en la Figura 3.

Figura 3. Controles implementados / objetivo final NTC ISO/IEC 27001:2013



Fuente: Elaboración propia

De los resultados obtenidos en la Figura 3 Controles implementados / objetivo final, es necesario realizar la implementación del Sistema de Gestión de seguridad de la Información SGSI en "**CODALTEC**", el cual conlleva a la valoración y tratamiento de riesgos, que tiene como objetivo proporcionar y realizar la identificación de controles, de acuerdo al análisis, valoración e implementación de acciones de mitigación para los riesgos potenciales de cada dependencias, con el fin de administrar y controlar eventos que pueden afectar el cumplimiento de los objetivos de seguridad de "**CODALTEC**".

Dentro de las mejores prácticas que pueden establecerse en "**CODALTEC**", existen disciplinas que, aplicándose de manera adecuada, proporcionaran estabilidad y confianza. Como las siguientes:

- Implementar y hacer cumplir las políticas de seguridad
- Detallar los aspectos organizativos para la seguridad
- Establecer controles de seguridad ligada al personal
- Implementar procesos y procedimientos
- Gestión de comunicaciones y de operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas

8. CONCLUSIONES

El diseño del Plan Estratégico de Seguridad de la Información (PESI) para **“CODALTEC”**, basado en las mejores prácticas de seguridad según la NTC-ISO/IEC 27001:2013, ha permitido determinar las necesidades y mejoras que se pueden establecer en la Corporación de alta tecnología para la defensa “CODALTEC”; el cumplimiento de las directrices establecidas en el diseño del PESI, permitirán cumplir y mantener el modelo de seguridad y privacidad de la información propuesto en este trabajo y que se lleva a la practica con el cumplimiento del portafolio de proyectos, manteniendo su realización forjando en el tiempo una adecuada y sostenible ejecución de cada una de las actividades que lo componen, logrando obtener altos estándares de seguridad de la Información.

Por ello es muy importante continuar con el apoyo y la aprobación de la alta gerencia de **“CODALTEC”**, y con el compromiso de todas las áreas involucradas en este proyecto, dando cumplimiento a los requisitos y temas regulatorios y además lograr apalancar los objetivos estratégicos de **“CODALTEC”.**

Todo lo anterior nos permite cumplir con el objetivo general de este trabajo el cual es viable y conforme a lo planteado en el diseño del Plan Estratégico de Seguridad de la Información (PESI) para **“CODALTEC”**, estableciendo con su ejecución la seguridad de la información garantizando la confiabilidad, integridad, confidencialidad y disponibilidad de la información.

El diagnóstico de la situación actual de la seguridad de la información en **“CODALTEC”**, se puede apreciar en la Figura 1. Cumplimiento por Dominio NTC-ISO/IEC 27001:2013. En la que se evidencia que sólo el dominio seguridad física y ambiental cumple con el 75.3% de los requerimientos de la NTC-ISO/IEC 27001:2013, además se identificó que la organización adopta algunas prácticas de seguridad en los dominios de Gestión de Activos (45%), Seguridad de las Operaciones (56.2%) y Seguridad de las Comunicaciones (32.5%) y los demás dominios no logran cumplir las expectativas de seguridad que exige NTC-ISO-IEC 27001:2013; por su parte la matriz de activos según metodología Magerit permitieron verificar estos resultados, dejando ver falencias en la seguridad de la información en **“CODALTEC”**.

Al valorar los resultados obtenidos en la aplicación de este estudio por medio de la ejecución del procedimiento para la aplicación de los riesgos de las operaciones y la seguridad de la información (Ver Anexo B matriz de hallazgos, recomendaciones y riesgos de los objetivos de control NTC – ISO/IEC 27001:2013). Valoración cuantitativa de los riesgos hallados con la Metodología de Magerit, se pudo identificar las necesidades en materia de Seguridad de la Información, por ello, después de un análisis se determinó que la prioridad de riesgos se encontraban en el cumplimiento de los objetivos de control de la Política de la Seguridad de la Información, Organización de la Seguridad de la Información, Seguridad de los

Recursos Humanos, Control de acceso, Criptografía, Adquisición, desarrollo y mantenimiento de sistemas, Relaciones con los proveedores, Aspectos de seguridad de la información de la gestión de la continuidad de negocio y Cumplimiento.

Aplicando el conocimiento obtenido del estudio realizado a la situación actual permitiendo conocer los niveles de riesgo de cada objetivo de control (Ver Anexo C valoración cuantitativa de los riesgos de los objetivos de control NTC – ISO/IEC 27001:2013), del desarrollo minucioso realizado en el capítulo de la identificación de riesgos de las operaciones y al diagnóstico obtenido, de realizar la valoración cuantitativa de la matriz de riesgos activos críticos según la metodología Magerit y NTC-ISO-IEC 27001:2013 (ver tabla 8), y la seguridad de la información, se identificaron claramente las necesidades e iniciativas de seguridad de la información**,** las que se pueden minimizar con el diseño del plan estratégico de seguridad de seguridad de la información “PESI”.

En consideración a los resultados obtenidos se procedió a generar una planeación para formular el portafolio de proyectos de seguridad de la información, la cual se basa en el diseño y elaboración de dos proyectos el Plan Estratégico de Seguridad de la Información “PESI” y el Sistema de Gestión en Seguridad de la Información “SGSI”.

Con los proyectos formulados se diseñó el procedimiento para la identificación de riesgos de los activos de información de las operaciones y la seguridad de la información de “**CODALTEC**”, el cual se basa en la matriz de riesgos, siendo funcional a la norma NTC-ISO/IEC 27001:2013.

Para finalizar se formularon indicadores de Seguridad de la Información en concordancia con lo elaborado, por lo cual fueron diseñados para las áreas de bases de datos, arquitectura, documentación, e infraestructura y gestión de la configuración.

Por todo lo anterior se concluye que con el desarrollo del presente estudio se logró diseñar un Plan Estratégico de Seguridad de la Información “PESI”, alineado con los objetivos estratégicos y conforme con los lineamientos de la Dirección de la Corporación de Alta Tecnología para la Defensa “**CODALTEC**” generando políticas y proyectos de seguridad de la información; que garanticen la protección de la información de la empresa.

9. RECOMENDACIONES

Considerando los resultados obtenidos en el presente estudio, se recomienda:

A la dirección de la Corporación de Alta Tecnología para la Defensa "**CODALTEC**" de la ciudad de Villavicencio evaluar el Plan Estratégico de Seguridad de la Información "PESI", diseñado en el presente estudio con el fin de implementarlo a la menor brevedad.

Igualmente, a la gerencia de la Corporación de Alta Tecnología para la Defensa "**CODALTEC**" que continúe con la implementación del Sistema de Gestión de Seguridad de la Información SGSI, desarrollando el ciclo PHVA (planear, ejecutar, verificar y actuar) en relación con la seguridad de la información con el fin de ir mejorando cada vez más su seguridad, pues a diario resultan nuevas amenazas, gracias a los avances de las tecnologías.

En búsqueda de mejorar y optimizar todos los procesos actuales, que garanticen la calidad, oportunidad, control y seguimiento de la información, se implemente los indicadores de seguridad de la información, realizando un constante seguimiento a su cumplimiento y resultados medibles frente a las necesidades de seguridad de "**CODALTEC**".

A los futuros Especialistas en Seguridad Informática de la UNAD, que continúen realizando proyectos de grado en modalidad de proyecto aplicado, pues de esta forma se contribuye a solucionar problemáticas que las empresas colombianas no podrían mitigar si incurrir en costos de honorarios en profesionales en el tema, de esta forma se realiza un aporte social a la comunidad.

BIBLIOGRAFIA

CORPORACIÓN DE ALTA TECNOLOGÍA PARA LA DEFENSA "**CODALTEC**". Plan estratégico de **CODALTEC**. Villavicencio, 2015.

CRUZ, Yolanda. Metodología OSSTMM para la detección de errores de seguridad y vulnerabilidad en sistemas operativos de 64 bits a nivel de usuario final. Escuela Superior Politécnica de Chimorazo. Riobamba, 2016.

FINDETER. Plan de tratamiento de riesgos de seguridad y privacidad de la información. Findeter. Bogotá, 2018.

GUEVARA CHUMÁN, Javier Gustavo. Aplicación de la Metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruíz Gallo. Universidad Nacional Pedro Ruiz Gallo. España, 2015.

HERNÁNDEZ SAMPIERI, Roberto; COLLADO, Carlos y BATISTA, Paola. Metodología de investogación. Sexta Edición. Editorial Mc Graw Hill. México, 2010.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS "ICONTEC". NTC-ISO-IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá, 2013.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS "ICONTEC". NTC-ISO-IEC 27002. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Controles. Bogotá, 2013.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS "ICONTEC". NTC 1486 Documentación, Presentación de tesis, trabajos de grado y otros trabajos de investigación. Sexta actualización. Bogotá, 2008.

IT GOVERNANCE INSTITUTE. Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa. IT Governance Institute, 2008.

LOZANO OLAVE, Marisol. Diseño de un Plan Estratégico de Seguridad de Información (PESI) para una compañía del sector asegurador. Tesis de especialista. Institución Universitaria Politécnico Grancolombiano. Bogotá, 2017.

QUINTERO GÓMEZ, Luisa Fernanda. Modelo basado en ITIL para la Gestión de los Servicios de TI en la Cooperativa de Caficultores de Manizales. Tesis de Magister en Gestión y Desarrollo de Proyectos de Software. Manizales: Universidad Autónoma de Manizales. Facultad de Ingeniería, Maestría en Gestión y Desarrollo de Proyectos de Software, 2015. 207 p.

ROJAS CARRIEL, Ángel y CASTRO PESANTES, Fernando. Análisis y detección de vulnerabilidades en los servidores públicos del centro de cómputo de la empresa intermediaria de ventas utilizando la metodología internacional OSSTMM. Tesis de pregrado en Ingeniero en Networking y Telecomunicaciones. Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas, 2015. 207 p.

TOAPANTA, Moisés. Seguridad de redes. Universidad Politécnica Salesiana. Guayaquil, 2014.

ANEXOS

Tabla 14. Anexo A lista de chequeo

CONTROL DE APLICACIÓN DE CHECK LIST ANEXO A ISO 27001-2013															
			Principales Roles Entrevistados												
Num	**Objetivo de Control**	**Encuesta**	**Gerente Proyecto**	**Infraestructura**	**Bases de Datos**	**Arquitectura**	**Almacén**	**Gestión Accesos**	**OGA**	**R.H.**	**SGSST**	**Desarrollo**	**Pruebas**	**PMO**	**S. Información**
A5	**POLITICAS DE LA SEGURIDAD DE LA INFORMACION**														
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**														
A.5.1.1	¿Cuentan ustedes con una política de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿La política ha sido publicada y comunicada a todos los empleados y partes	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	externas pertinentes?														
A.5.1.2	¿La política de seguridad de la información es revisada con regularidad?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Cada cuánto es revisada la política de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.6	**ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACION**														
A.6.1	**Organización Interna**														
A.6.1.1	¿Se encuentran definidos y asignados todos los roles y responsabilidades de la seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.6.1.2	¿Cuentan ustedes con un representante de la	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	organización que coordine las actividades de seguridad de la información?														
A.6.1.3	¿Se mantiene un contacto apropiado con las autoridades pertinentes para la seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.6.1.4	¿La organización mantiene contacto con grupos de interés especiales (foros especializados, asociaciones de profesionales) respecto a la seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.6.1.5	¿Sabe dónde deben ser tratados los temas relativos a la seguridad de	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	la información?														
A.6.2	**Dispositivos móviles y teletrabajo**														
A.6.2.1	¿Entienden la política y las medidas de seguridad para el uso de dispositivos móviles?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.6.2.2	¿Cuentan con una política de seguridad de la información para el teletrabajo?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**														
A.7.1	**Antes de asumir el empleo**														
A.7.1.1	¿Se realiza una verificación de los antecedentes de los candidatos a un empleo según las leyes y reglamentación pertinentes?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.7.1.2	¿Son claros los acuerdos y responsabilidades entre la organización y el empleado para el manejo de la seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.7.2	**Durante la ejecución del empleo**														
A.7.2.1	¿La dirección exige a los empleados la aplicación de la política de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.7.2.2	¿Se realizan campañas de sensibilización respecto a la seguridad de la información cada que es necesario?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.7.2.2	¿Cuentan ustedes con políticas y procedimientos como acciones disciplinarias para los	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	empleados que transgreden las reglas de seguridad de la información?														
A.7.3	**terminación y cambio de empleo**														
A.7.3.1	¿Son comunicadas a los empleados las responsabilidades y deberes de seguridad de la información que permanecen validos después de la terminación del contrato?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Los empleados cumplen las responsabilidades y deberes de seguridad de la información que permanecen validos después de la	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	terminación del contrato?														
A.8	**GESTION DE ACTIVOS**														
A.8.1	**Responsabilidad por los activos**														
A.8.1.1	¿Se encuentran identificados los activos de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Se encuentran identificadas las instalaciones de procesamiento de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Se cuenta con un inventario de los activos e instalaciones de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.1.2	¿Cuentan con un propietario para cada activo, y está consignado en el inventario?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.1.3	¿Cuentan con reglamentación para el uso	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	adecuado de las instalaciones y activos de información?														
	¿Se encuentra documentadas las reglas para el uso adecuado de las instalaciones y activos de información, y son implementadas?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.1.4	¿El empleado al terminar el contrato, devuelve todos los activos de la organización?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Los derechos de acceso de un empleado son retirados al finalizar su contrato?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.2	**Classification de la información**														
A.8.2.1	¿Cuentan con un método de clasificación de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.8.2.2	¿La información se encuentra etiquetada?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.2.3	¿Se encuentran implementados los procedimientos para el manejo de activos según la clasificación de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.3	**Manejo de Medios**														
A.8.3.1	¿Se encuentran implementados procedimientos para la gestión de medios removibles según el esquema de clasificación?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.3.2	¿Cuentan con procedimientos formales para disponer de los medios de forma segura?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.8.3.3	¿Se encuentran	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	protegidos los medios que contienen información contra acceso no autorizado?														
A.9	**CONTROL DE ACCESO**														
A.9.1	**Requisitos de negocio para control de acceso**														
A.9.1.1	¿Comprenden la política de control de acceso basada en la seguridad de la información y los requisitos del negocio?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.1.2	¿Solo aquellos que tienen permiso, acceden a las redes y a servicios de red?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.2	**Gestión de acceso de usuarios**														
A.9.2.1	¿Cuentan con un registro y cancelación del registro de usuarios para la asignación	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	de derechos de acceso?														
A.9.2.2	¿Cuentan con la implementación de un proceso de suministro de acceso de usuarios para asignar o revocar los derechos de acceso?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.2.3	¿Se encuentra restringida y controlada la gestión de derechos de acceso privilegiado?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.2.4	¿Se encuentra controlada la asignación de información de autenticación secreta?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.2.5	¿Los propietarios de los activos revisan los derechos de acceso de los usuarios?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.2.6	¿Son retirados los derechos de acceso de los empleados	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	al terminar su contrato?														
A.9.3	**Responsabilidad de los usuarios**														
A.9.3.1	¿Los usuarios cumplen las prácticas para el uso de información de autenticación secreta?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.4	**Control de acceso a sistemas y aplicaciones**														
A.9.4.1	¿Cuentan con métodos de restricción para acceso a la información y funciones de los sistemas?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.4.2	¿Cuentan con un proceso de ingreso seguro a los sistemas y aplicaciones?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.4.3	¿Los sistemas de gestión de contraseñas son interactivos y aseguran la calidad de las contraseñas?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.9.4.4	¿Se encuentra restringido el uso de programas utilitarios?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.9.4.5	¿Se encuentra restringido el acceso a los códigos fuente de los programas?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.10	**CRIPTOGRAFIA**														
A.10.1	**Controles Criptográficos**														
A.10.1.1	¿Entienden ustedes la política sobre el uso de controles criptográficos para la protección de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.10.1.2	¿Cuentan ustedes con una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.11	**SEGURIDAD FISICA Y DEL ENTORNO**														
A.11.1	**Áreas seguras**														
A.11.1.1	¿Los perímetros de seguridad, protegen áreas que contengan información confidencial o crítica, e instalaciones de manejo de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.1.2	¿Se encuentran protegidas las áreas seguras?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.1.3	¿Se encuentra aplicada la seguridad física a oficinas, recintos e instalaciones?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.1.4	¿Se encuentra aplicada la protección física contra desastres naturales, ataques maliciosos o accidentes?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.11.1.5	¿Conocen los procedimientos para trabajo en áreas seguras?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.1.6	¿Se encuentran controlados los puntos de acceso, tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Se encuentran aislados los puntos de acceso de las instalaciones de procesamiento de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.2	**Equipos**														
A.11.2.1	¿Se encuentran protegidos los equipos de las amenazas y peligros del entorno y de las	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	posibilidades de acceso no autorizado?														
A.11.2.2	¿Se encuentran protegidos los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.2.3	¿Se encuentra protegido el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.2.4	¿Se realiza el mantenimiento de los equipos para asegurar su disponibilidad e integridad continua?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.2.5	¿Se permite el retiro de activos de su sitio sin	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	autorización previa?														
A.11.2.6	¿Conocen cuáles son las medidas de seguridad que se aplican a los activos que se encuentran fuera de las instalaciones de la organización?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Sabe cuáles son los riesgos de trabajar fuera de las instalaciones?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.2.7	¿Cree que son verificados los elementos de almacenamiento de los equipos antes de su disposición o reuso?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.2.8	¿Se les da protección a los equipos desatendidos?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.11.2.9	¿Entienden la política de escritorio limpio y pantalla limpia?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.12	**SEGURIDAD DE LAS OPERACIONES**														
A.12.1	**Procedimientos Operacionales y responsabilidades**														
A.12.1.1	¿Se encuentran documentados los procedimientos de operación y están a disposición de los usuarios que los necesitan?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.1.2	¿Cuentan con una gestión de cambios en la organización en los procesos que pueda afectar la seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.1.3	¿Se realiza seguimiento para los requisitos de capacidad futura?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.12.1.4	¿Se encuentra separado el ambiente de desarrollo, pruebas y operación?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.2	**Protección contra códigos maliciosos**														
A.12.2.1	¿Se encentra protegido contra código malicioso?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.3	**Copias de respaldo**														
A.12.3.1	¿Entiende la importancia de realizar copias de respaldo de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Se han puesto a prueba o verificado las copias de respaldo de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.4	**Registro y seguimiento**														
A.12.4.1	¿Cuentan con un registro de actividades del usuario, excepciones, fallas y eventos de	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	seguridad de la información?														
A.12.4.2	¿Se encuentran protegidas las instalaciones y la información de registro contra alteraciones y acceso no autorizado?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.4.3	¿Se cuenta con un registro de las actividades del administrador y operador del sistema?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Se revisa con regularidad los registros de las actividades del administrador y operador del sistema?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.4.4	¿Se encuentran sincronizados los relojes de todos los sistemas de procesamiento de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.12.5	**Control de software operacional**														
A.12.5.1	¿Cuentan con un procedimiento para controlar la instalación de software en sistemas operativos?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.6	**Gestión de la vulnerabilidad técnica**														
A.12.6.1	¿Se obtiene oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se utilizan?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Se cuenta con un método para evaluar la exposición de la organización a las vulnerabilidades?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.12.6.2	¿Los usuarios comprenden las reglas para la instalación de software?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.12.7	**Consideraciones sobre auditorias de sistemas de información**														
A.12.7.1	¿Han sido planificados y acordados los requisitos y actividades de auditoria de los sistemas de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.13	**SEGURIDAD DE LAS COMUNICACIONES**														
A.13.1	**Gestión de la seguridad de las redes**														
A.13.1.1	¿Cuentan con un método de gestión y control de las redes?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.13.1.2	¿Se encuentran identificados los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	servicios de red?														
A.13.1.3	¿Se encuentran separados los grupos de servicios de información, usuarios y sistemas de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.13.2	**Transferencia de información**														
A.13.2.1	¿Entienden la política de procedimientos y controles de transferencia formales de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.13.2.2	¿Cree que la política de transferencia de información es tratada de forma segura?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.13.2.3	¿Sabe cómo proteger adecuadamente la información electrónica?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.13.2.4	¿Se encuentran documentado	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	acuerdos de confidencialidad o no divulgación de la información?														
	¿Son revisados regularmente los acuerdos de confidencialidad?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA**														
A.14.1	**Requisitos de seguridad sistemas de información**														
A.14.1.1	¿Se encuentran incluidos los requisitos de seguridad información en los requisitos para nuevos sistemas de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.1.2	¿Se encuentra protegida la información de servicios de	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	las aplicaciones en redes públicas de ataques fraudulentos, modificación no autorizada, disputas contractuales y divulgación?														
A.14.1.3	¿Se encuentra protegida la información involucrada en las transacciones de los servicios de las aplicaciones?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.2	**Seguridad en los procesos de desarrollo y de soporte**														
A.14.2.1	¿Saben los desarrolladores cuales son las políticas de desarrollo de software y de sistemas?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.2.2	¿Se encuentran procedimientos de control de cambios a los sistemas	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	dentro del ciclo de vida de desarrollo?														
A.14.2.3	¿Cuentan con la realización de pruebas cuando hay cambios en las plataformas de operación?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.2.4	¿Cuentan con restricciones para cambios en los paquetes de software?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.2.5	¿Cuentan con principios para la construcción de sistemas seguros?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.2.6	¿Se encuentran protegidos los ambientes de desarrollo seguro?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.2.7	¿Se realiza supervisión y seguimiento del desarrollo contratado externamente?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.2.8	¿Realizan durante el desarrollo pruebas de	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	seguridad de los sistemas?														
A.14.2.9	¿Se encuentran establecidos programas de pruebas para aceptación de los sistemas?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.14.3	**Datos de prueba**														
A.14.3.1	¿Son protegidos los datos de prueba?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.15	**RELACIONES CON LOS PROVEEDORES**														
A.15.1	**Seguridad de la información en las relaciones con los proveedores**														
A.15.1.1	¿Comprende la política de seguridad de la información para las relaciones con proveedores?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
	¿Se encuentra documentada la política de seguridad de la información	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	para las relaciones con proveedores?														
A.15.1.2	¿Son establecidos y acordados todos los requisitos de seguridad de la información con cada proveedor?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.15.1.3	¿Cuentan con requisitos para tratar los riesgos de seguridad de la información relacionados con la cadena de suministro de tecnología de información y comunicación?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.15.2	**Gestión de la prestación de servicios de proveedores**														
A.15.2.1	¿Se realiza supervisión y seguimiento de la prestación de servicios de los proveedores?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.15.2.2	¿Son gestionados los cambios en los servicios de los proveedores?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**														
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**														
A.16.1.1	¿Se encuentran establecidas las responsabilidades y procedimientos de gestión que aseguren una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.16.1.2	¿Son apropiados los canales de	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	gestión para informar sobre eventos de seguridad de la información?														
A.16.1.3	¿Los empleados reportan cualquier debilidad de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.16.1.4	¿Los eventos de seguridad de la información son evaluados y clasificados?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.16.1.5	¿Se da respuesta a los incidentes de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.16.1.6	¿Considera que se aprende de los incidentes de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.16.1.7	¿Se aplican procedimientos para la recolección de la información	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	que pueda servir como evidencia?														
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO**														
A.17.1	**Continuidad de seguridad de la información**														
A.17.1.1	¿Cuentan con requisitos y continuidad de la seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.17.1.2	¿Se encuentran documentados e implementada la continuidad a los procesos, procedimientos y controles de la seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.17.1.3	¿Se realiza regularmente	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

	verificación, revisión y evaluación de la continuidad de la seguridad de la información?														
A.17.2	**Redundancias**														
A.17.2.1	¿Cuentan con disponibilidad de instalaciones de procesamiento de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.18	**CUMPLIMIENTO**														
A.18.1	**Cumplimiento de requisitos legales y contractuales**														
A.18.1.1	¿Se encuentran identificados, actualizados y documentados explícitamente todos los requisitos estatutarios, reglamentarios y contractuales pertinentes?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

A.18.1.2	¿Cuentan con procedimientos apropiados para tratar los derechos de propiedad intelectual?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.18.1.3	¿Se encuentran protegidos los registros contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.18.1.4	¿Es asegurada la privacidad y protección de datos personales como se exige en la legislación?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.18.1.5	¿Cuentan con sistemas y técnicas criptográficas para proteger la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.18.2	**Revisiones de seguridad de la información**														

A.18.2.1	¿Cuentan con una revisión independiente de la seguridad de la información (ejm: objetivos de control, las políticas, ¿los procesos)?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.18.2.2	¿Los directores revisan regularmente el cumplimiento con las políticas y normas de seguridad de la información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x
A.18.2.3	¿Son revisados periódicamente los sistemas de información?	1-Si	x	x	x	x	x	x	x	x	x	x	x	x	x

Fuente: Elaboración propia

Tabla 15. Anexo B matriz de hallazgos, recomendaciones y riesgos de los objetivos de control NTC – ISO/IEC 27001:2013

Soporte	Recomendación	Control ISO/IEC 270001:2013	Riesgos	Impacto	Probabilidad	Riesgo	Calculo del Riesgo	Valoración del Riesgo
Entrevista con el Gerette	Definir, aprobar, publicar, comunicar y revisar a intervalos planificados las políticas de seguridad de la información para el proyecto .	A.5.1.1 A.5.1.2	• Pérdida y/o robo de información sensible o confidencial del proyecto . • Accesos no autorizados a la red de datos y a los equipos. • Exposición a acciones indeseadas de seguridad en la información. • Divulgación de información confidencial. • Interceptación de la información en las redes de comunicación. • Exposición a peligros del entorno por instalaciones inseguras. • Acceso o cambios no autorizados en los ambientes de operación. • Vulnerabilidades técnicas en los sistemas de información. • Cambios sin control en el desarrollo del aplicativo . • Acceso a la información confidencial del proyecto por parte de los proveedores. • Sin redundancias suficientes para cumplir los objetivos del proyecto . • Sanciones legales por el incumplimiento de los aspectos legales.	5-Certero	5- Catastrófico	R1	25	Riesgo Extremo
Entrevista con el Gerette	• Definir y asignar todas las responsabilidades de la seguridad de la información para el proyecto. • Separar los deberes y las áreas en conflicto para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos asignados en el proyecto . • Mantener contactos apropiados con las autoridades pertinentes de la seguridad de la información dentro del proyecto . • Mantener contactos apropiados con grupos especializados en seguridad de la información para . • Aplicar la seguridad de la información en la gestión del proyectos, independientemente del tipo del proyecto. • Adoptar políticas y medidas de seguridad al interior del proyecto , que permitan gestionar los riesgos asociados por el uso de dispositivos móviles. • Implementar políticas y medidas de seguridad al interior del proyecto , para proteger la información a la que tiene acceso, que es procesada o almacenada en lugares en los que se realiza el teletrabajo.	A.6.1.1 A.6.1.2 A.6.1.3 A.6.1.4 A.6.1.5 A.6.2.1 A.6.2.2	• Modificaciones no autorizadas o intencionales a la información. • Sin respuestas oportunas en caso de incidentes. • Desconocimiento de temas específicos y especializados en la seguridad de la información para la solución de problemas. • Riesgos informáticos en el uso de dispositivos móviles sin control y supervisión. • Pérdida de la información en lugares donde se realiza teletrabajo.	5-Certero	5- Catastrófico	R2	25	Riesgo Extremo
Entrevista con el Gerette	Verificar los antecedentes de todo el personal asociado al proyecto . La verificación debe llevarse a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos del proyecto, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.	A.7.1.1	Contratar personal para el proyecto con sanciones, inhabilidades o en conflicto de intereses.	3-Posible	3- Moderado	R3	9	Riesgo Medio
• Acuerdo de compromiso de confidencialidad CODALTEC. • Área Administrativa	Mantener la aplicación de los acuerdos contractuales sobre la seguridad de la información, con todos los empleados y contratistas vinculados con el proyecto .	A.7.1.2	Demandas legales por parte de los empleados que no firman los acuerdos de confidencialidad y propiedad intelectual del proyecto .	5-Certero	2- Menor	R4	10	Riesgo Alto

Entrevista con el Gerette	Exigir a todos los empleados y contratistas el cumplimiento de la seguridad de la información de acuerdo con las políticas y procedimientos que establezca la dirección de la desde el momento de la contratación.	A.7.2.1	• Pérdida y/o robo de información sensible o confidencial del proyecto . • Accesos no autorizados a la red de datos y a los equipos. • Exposición a acciones indeseadas de seguridad en la información. • Divulgación de información confidencial. • Acceso o cambios no autorizados en los ambientes de operación. • Vulnerabilidades técnicas en los sistemas de información. • Cambios sin control en el desarrollo del aplicativo . • Acceso a la información confidencial del proyecto por parte de los proveedores. • Sanciones legales por el incumplimiento de los aspectos legales.	5-Certero	4-Mayor	R5	20	Riesgo Extremo
Capacitaciones y socializaciones	Todos los empleados del proyecto deben recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a la seguridad de la información.	A.7.2.2	Desconocimiento de nuevas amenazas, virus informáticos, vulnerabilidades, prácticas de desarrollo seguro, tecnologías para proteger y salvaguardar la información, y temas especializados con la seguridad de la información que afecten en el proyecto .	3-Posible	3- Moderado	R6	9	Riesgo Medio
Entrevista con el Gerette	Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido violaciones a la seguridad de la información del proyecto .	A.7.2.3	No emprender las acciones legales y conformes, a los empleados que hayan cometido violaciones a la seguridad de la información del proyecto .	4-Probable	4-Mayor	R7	16	Riesgo Extremo
Entrevista con el Gerette	Definir, comunicar y hacer cumplir al empleado o contratista del proyecto las responsabilidades y los deberes de seguridad de la información que permanecen válidos al cambiar las responsabilidades dentro del proyecto.	A.7.3.1	Incumplir las responsabilidades y deberes por cambio de rol en el proyecto .	4-Probable	3- Moderado	R8	12	Riesgo Alto
Entrevista Jefe OGA Oficina Gestión de adquisiciones	Identificar todos los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener el inventario de todos los activos asignados a .	A.8.1.1	Pérdidas financieras, operativas y/o de imagen para el proyecto .	5-Certero	5- Catastrófico	R9	25	Riesgo Extremo
Entrevista Jefe OGA Oficina Gestión de adquisiciones	Identificar, controlar y asignar los responsables o propietarios de cada recurso tecnológico de acuerdo al inventario de activos.	A.8.1.2	Pérdida o manipulación intencionada de los recursos tecnológicos por cualquier empleado.	3-Posible	3- Moderado	R10	9	Riesgo Medio
Entrevista con el Gerette	Identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información del proyecto .	A.8.1.3	Pérdida de los recursos tecnológicos con información sensible del proyecto	4-Probable	2- Menor	R11	8	Riesgo Medio
Entrevista Jefe OGA Oficina Gestión de adquisiciones	Al finalizar la relación laboral se debe actualizar el inventario de activos. Se debe dar tratamiento seguro a la información contenida en los equipos entregados antes de la reasignarlos.	A.8.1.4	Divulgación o modificación de información sensible del proyecto .	5-Certero	2- Menor	R12	10	Riesgo Alto
Entrevista con el Gerette	• Clasificar la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. • Desarrollar e implementar los procedimientos para el etiquetado de la información de acuerdo al esquema de clasificación de información diseñado por la dirección del proyecto.	A.8.2.1 A.8.2.2	Divulgar información sensible del proyecto , por no estar etiquetada o clasificada.	5-Certero	3- Moderado	R13	15	Riesgo Extremo
Entrevista Jefe OGA Oficina Gestión de adquisiciones	Desarrollar e implementar procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información que adopte la dirección del proyecto.	A.8.2.3	Acciones intencionadas de robo, alteración, eliminación u otras por parte de los empleados que tienen acceso a los activos de información.	4-Probable	2- Menor	R14	8	Riesgo Medio
Entrevistas Jefe Infraestructura	Implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación de información adoptado por la dirección.	A.8.3.1	Pérdida, alteración o robo de información sensible del proyecto por la falta de medidas de seguridad en el uso de medios removibles.	5-Certero	5- Catastrófico	R15	25	Riesgo Extremo
Entrevista Jefe OGA Oficina Gestión de adquisiciones	Disponer en forma segura de todos los medios de almacenamiento cuando ya no se requieran, utilizando procedimientos formales para la destrucción, reubicación o reutilización.	A.8.3.2	Divulgación de información sensible del proyecto , contenida en unidades de almacenamiento sin procedimientos de destrucción, reubicación o reutilización.	3-Posible	4-Mayor	R16	12	Riesgo Alto

Entrevista Jefe OGA Oficina Gestión de adquisiciones e Infraestructura	Proteger los medios físicos que contienen información contra acceso no autorizado, uso indebido o corrupción durante su transporte, con métodos de cifrado de información y claves robustas, entre otras medidas de seguridad.	A.8.3.3	Pérdida, daño o alteración de medios físicos con información sensible para el proyecto	5-Certero	2- Menor	R17	10	Riesgo Alto
Entrevista con el Gerette	Establecer, documentar y revisar una política de control de acceso a los sistemas de información con base en los requisitos del proyecto y de seguridad de la información.	A.9.1.1	Acceso sin control a los sistemas de información afectando la confidencialidad, disponibilidad e integridad de la información del proyecto .	5-Certero	5- Catastrófico	R18	25	Riesgo Extremo
Entrevistas Jefe Infraestructura	Controlar y monitorear el acceso al servicio de internet. Definir la política para compartir archivos y carpetas en la red. Definir los procedimientos para la creación, modificación y suspensión de usuarios que acceden a los servicios de tecnología.	A.9.1.2	Exposición al contagio de virus, malware y software dañino. Las carpetas compartidas en la red sin control de acceso se pueden modificar y borrar la información contenida en ellas. Asimismo las credenciales compartidas de acceso a la base de datos permite copiar, modificar y borrar la información contenida en la base de datos sin el control y seguimiento de los usuarios que accedan a ella.	5-Certero	5- Catastrófico	R19	25	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración	Implementar un proceso formal de registro y de cancelación de registro de usuarios, para controlar la asignación de los derechos de acceso.	A.9.2.1	Tener usuarios innecesarios y con derechos de acceso que puedan realizar copias, modificaciones y el borrado de la información sensible del proyecto.	5-Certero	4-Mayor	R20	20	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración	Implementar un proceso de suministro de acceso formal de usuarios, para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios enmarcados en el proyecto.	A.9.2.2	Usuarios alteren, copien, dañen o destruyan información sensible para el proyecto por conocer los nombres de usuario y claves de acceso a los sistemas de información de los demás empleados.	5-Certero	4-Mayor	R21	20	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	Restringir y controlar la asignación y uso de derechos de acceso privilegiado a los recursos tecnológicos asignados al proyecto .	A.9.2.3	Asignar derechos privilegiados por error a los empleados, sin establecer su participación y responsabilidad en el proyecto .	3-Posible	4-Mayor	R22	12	Riesgo Alto
Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	Controlar por medio de un proceso de gestión formal, la asignación de información de autentificación secreta de todos los servicios a los que tienen acceso los usuarios.	A.9.2.4	Exposición de las claves de acceso del correo electrónico corporativo, a personal que no está autorizado, ocasionando robo o alteración de información sensible del proyecto.	3-Posible	3- Moderado	R23	9	Riesgo Medio
Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	• Los propietarios de activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares en el proyecto. • Retirar los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información al terminar el contrato con el proyecto.	A.9.2.5 A.9.2.6	Exposición de la información del proyecto a personas que ya no tiene vinculo laboral con la corporación, ocasionando pérdida y robo de la información sensible y confidencial.	4-Probable	3- Moderado	R24	12	Riesgo Alto
Entrevista Jefe Gestión de la Configura+ción	Exigir a los usuarios del proyecto que cumplan las prácticas de la organización para el uso de información de autentificación secreta.	A.9.3.1	Uso de claves débiles para acceder a los diferentes sistemas de información.	4-Probable	3- Moderado	R25	12	Riesgo Alto

Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	• Restringir el acceso a la información y a las funciones de los sistemas de las aplicaciones de acuerdo con la política de control de acceso . • Controlar el acceso a sistemas y aplicaciones del proyecto mediante un proceso de ingreso seguro según lo requiera la política de control de acceso. • La gestión de contraseñas deben ser interactivos y asegurar la calidad de las contraseñas del proyecto .	A.9.4.1 A.9.4.2 A.9.4.3	Acceso a los sistemas de información por usar contraseñas débiles y falta de controles de acceso en los aplicativos, por parte de empleados no autorizados.	4-Probable	5- Catastrófico	R26	20	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	Restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones .	A.9.4.4	Descargar e instalar programas sin control, posibilitan el contagio de virus, malware, y otro tipo de software dañino, que pueden afectar la información y el proyecto .	5-Certero	5- Catastrófico	R27	25	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración, Infraestructura	Restringir y controlar el acceso a los códigos fuente de los programas .	A.9.4.5	Realizar copias del código fuente del aplicativo y de la información del proyecto con fines mal intencionados.	5-Certero	5- Catastrófico	R28	25	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración, Infraestructura	• Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información en la solución . • Desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida en el proyecto .	A.10.1.1 A.10.1.2	La información confidencial y sensible del proyecto se encuentra legible y está expuesta a accesos no autorizados, alteraciones, robo y/o pérdida.	5-Certero	5- Catastrófico	R29	25	Riesgo Extremo
OGA e Infraestructura	Definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información .	A.11.1.1	El ingreso de personas no autorizadas dentro de las instalaciones de los sistemas de información del proyecto , pueden ocasionar alteraciones, robo de información e instalación de software malicioso.	5-Certero	5- Catastrófico	R30	25	Riesgo Extremo
OGA e Infraestructura	Proteger las áreas de procesamiento de información mediante controles de acceso apropiados para asegurar que solo se permite el acceso al personal autorizado en el proyecto .	A.11.1.2	Alteración de información o daño a los recursos tecnológicos por la falta de controles de acceso a las instalaciones de procesamiento de información.	5-Certero	5- Catastrófico	R31	25	Riesgo Extremo
OGA e Infraestructura	Mejorar los controles de acceso físicos en las oficinas, recintos e instalaciones en el proyecto .	A.11.1.3	Se presenten incidentes de seguridad y no lograr encontrar los responsables.	3-Posible	2- Menor	R32	6	Riesgo Medio
Informe visita centros de datos I	Implementar el sistema de respaldo de energía regulada para todos los equipos conectados a la red.	A.11.1.4	Pérdida de la información ocasionando daños del hardware y software en los equipos tecnológicos. Retraso en la operaciones diarias por falta del sistema de energía ininterrumpida.	5-Certero	5- Catastrófico	R33	25	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	Diseñar y aplicar procedimientos para trabajo en áreas seguras en el proyecto .	A.11.1.5	Accidentes de trabajo que afecten la operatividad del proyecto .	1-Raro	2- Menor	R34	2	Riesgo Inusual

Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	Controlar los puntos de acceso del proyecto . Puntos de acceso donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	A.11.1.6	Permitir el ingreso a las instalaciones de procesamiento de información a personal no autorizado.	5-Certero	3- Moderado	R35	15	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	Ubicar y proteger los equipos de la para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	A.11.2.1	Daños de hardware por temas ambientales, amenazas y peligros del entorno.	5-Certero	3- Moderado	R36	15	Riesgo Extremo
Entrevista Jefe Gestión de la Configuración, Infraestructura y PMO	Proteger los equipos del proyecto contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro eléctrico.	A.11.2.2	Daños en los recursos tecnológicos por fallas de energía.	3-Posible	3- Moderado	R37	9	Riesgo Medio
Infraestructura	Proteger el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información del proyecto la contra interceptación, interferencia o daño.	A.11.2.3	Interferencias o daño al cableado por estar expuesto a la manipulación malintencionada de los empleados.	3-Posible	2- Menor	R38	6	Riesgo Medio
Infraestructura	Implementar programas de mantenimiento preventivo y correctivo a todos los equipos del proyecto, para asegurar la disponibilidad e integridad.	A.11.2.4	Disponer de recursos tecnológicos en condiciones no óptimas para el trabajo que requiere en el proyecto .	1-Raro	3- Moderado	R39	3	Riesgo Bajo
Infraestructura	Aplicar medidas de seguridad a los activos del proyecto que se encuentran fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	A.11.2.5 A.11.2.6	Pérdida de los recursos tecnológicos con información sensible del proyecto	5-Certero	4-Mayor	R40	20	Riesgo Extremo
Infraestructura	Verificar los elementos que contengan información almacenada para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.	A.11.2.7	Pérdida o divulgación de información contenida en unidades de almacenamiento.	3-Posible	5- Catastrófico	R41	15	Riesgo Extremo
Infraestructura	Asegurar que los equipos del proyecto desatendidos se les da protección apropiada.	A.11.2.8	Pérdida o divulgación de información confidencial o sensible del proyecto a personal no autorizado.	3-Posible	4-Mayor	R42	12	Riesgo Alto
Infraestructura	Adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información del proyecto .	A.11.2.9	Pérdida o alteración de información confidencial o sensible del proyecto a personal no autorizado.	3-Posible	4-Mayor	R43	12	Riesgo Alto
Infraestructura	Documentar los procedimientos de operación para todos los usuarios , ya que contienen información necesaria para llevar a cabo de manera precisa y secuencial, las tareas y actividades operativas que son asignadas a cada integrante, de la misma forma, determina la responsabilidad en la labores a desarrollar.	A.12.1.1	Las tareas o actividades se llene a cabo de forma intuitiva o no se realicen por la falta de los procedimientos operacional del proyecto .	4-Probable	3- Moderado	R44	12	Riesgo Alto
CSI e Infraestructura	Se deben controlar los cambios en los procesos, en las instalaciones y en los sistemas de procesamiento de información de la que afecten la seguridad de la información.	A.12.1.2	Realizar cambios en los procesos, en las instalaciones y en los sistemas de procesamiento que afecten el éxito del proyecto .	5-Certero	5- Catastrófico	R45	25	Riesgo Extremo
CSI e Infraestructura	Hacer seguimiento al uso de recursos, hacer ajustes y proyecciones de la capacidad futura del sistema del proyecto.	A.12.1.3	No tener la capacidad disponible de los recursos tecnológicos afectando la continuidad y el desempeño requerido de los sistemas de información.	5-Certero	4-Mayor	R46	20	Riesgo Extremo
CSI e Infraestructura	Separar los ambientes de desarrollo, pruebas y operación, para reducir riesgos de acceso o cambios no autorizados al ambiente de producción .	A.12.1.4	Acceder o realizar cambios no autorizados al ambiente de producción .	5-Certero	5- Catastrófico	R47	25	Riesgo Extremo
CSI e Infraestructura	Implementar controles de detección, de prevención y de recuperación contra código malicioso en los sistemas de información del proyecto.	A.12.2.1	Exposición a amenazas informáticas, ocasionando vulnerabilidades, pérdida y/o robo de la información, errores y fallas en el sistema de información, y la continuidad del proyecto .	5-Certero	5- Catastrófico	R48	25	Riesgo Extremo

CSI e Infraestructura	• Crear las políticas de copias de respaldo de la información . • Realizar copias de seguridad de la información, software o imágenes de acuerdo a las políticas de respaldo de la información del proyecto.	A.12.3.1	Perdida parcial y/o total de la información del proyecto .	5-Certero	5- Catastrófico	R49	25	Riesgo Extremo
CSI e Infraestructura	Se debe elaborar, conservar y revisar regularmente los registros asociados a las copias de seguridad en el proyecto.	A.12.4.1 A.12.4.2	No disponer de registros de los actualizados y controlados de las copias de seguridad de la información del proyecto .	5-Certero	5- Catastrófico	R50	25	Riesgo Extremo
CSI e Infraestructura	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad en el proyecto.	A.12.4.3	Modificaciones sin control por parte de los administradores en los sistemas de información del proyecto .	5-Certero	5- Catastrófico	R51	25	Riesgo Extremo
CSI e Infraestructura	Todo los sistemas de procesamientos del proyecto se deben sincronizar con una única fuente de referencia de tiempo.	A.12.4.4	Los sistemas de información tendrán registros a diferentes tiempos y no habrá concordancia de estos para revisión de los logs del sistema, además los procesos tendrán alteraciones o inconsistencias generando errores y fallas de sincronización.	3-Posible	3- Moderado	R52	9	Riesgo Medio
CSI e Infraestructura	Implementar procedimientos para controlar la instalación de software en sistemas operativos del proyecto.	A.12.5.1	Instalación de software o herramientas innecesarios creando vulnerabilidades en los sistemas de información.	5-Certero	5- Catastrófico	R53	25	Riesgo Extremo
CSI e Infraestructura	Obtener, evaluar y tomar conciencia de la información sobre las vulnerabilidades técnicas que permitan tratar los riesgos asociados al proyecto.	A.12.6.1	Desconocimiento de las vulnerabilidades existentes ocasionado daños, errores y fallas en los sistemas de información .	4-Probable	4-Mayor	R54	16	Riesgo Extremo
CSI e Infraestructura	Establecer las reglas para la instalación de software a todos los empleados del proyecto.	A.12.6.2	Afectación a los sistemas de información por software malicioso, virus y programas innecesarios en el proyecto .	4-Probable	5- Catastrófico	R55	20	Riesgo Extremo
CSI e Infraestructura	Planificar y controlar cuidadosamente la verificación de los sistemas de información, para minimizar las interrupciones en los procesos .	A.12.7.1	Desconocer las fallas actuales sin poder dar respuesta de estos incidentes y no minimizar las interrupciones en los procesos .	3-Posible	3- Moderado	R56	9	Riesgo Medio
CSI e Infraestructura	Gestionar y controlar las redes para proteger la información en sistemas y aplicaciones .	A.13.1.1	Aparición de amenazas informáticas, creación de vulnerabilidades, pérdida y/o robo de la información, errores y fallas en el sistema de información, y afectación en la continuidad del proyecto .	5-Certero	5- Catastrófico	R57	25	Riesgo Extremo
CSI e Infraestructura	Identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión de los servicios de red internos y externos del proyecto.	A.13.1.2	Alteraciones de los servicios de comunicación y afectando a los usuarios de la red.	3-Posible	4-Mayor	R58	12	Riesgo Alto
CSI e Infraestructura	Separar las redes de los servicios de información, de usuarios y sistemas de información.	A.13.1.3	Intrusiones de delincuentes informáticos que quieren dañar los sistemas de información .	4-Probable	4-Mayor	R59	16	Riesgo Extremo
CSI e Infraestructura	Definir las políticas, procedimientos y controles de transferencia formal para proteger la transferencia de información en todo tipo de instalaciones de comunicación .	A.13.2.1	Transferir información sensible por medio de inseguros del proyecto .	5-Certero	5- Catastrófico	R60	25	Riesgo Extremo
CSI e Infraestructura	Definir acuerdos sobre la transferencia segura de información desde el interior de la organización a partes externas vinculadas al proyecto .	A.13.2.2	Transferir información por medio de inseguros desde y hacia las partes externas involucradas en el proyecto .	3-Posible	3- Moderado	R61	9	Riesgo Medio
CSI e Infraestructura	Proteger adecuadamente la información incluida en la mensajería electrónica del proyecto.	A.13.2.3	Pérdida o fuga de la información contenida en las cuentas de correo por la falta de las copias de respaldo.	3-Posible	3- Moderado	R62	9	Riesgo Medio
Entrevista OGA Ofcina Gestión de la Configuración	Identificar, revisar regularmente y documentar los requisitos de los acuerdos de confidencialidad o no divulgación para la protección de la información relacionada con .	A.13.2.4	En el proceso de contratación los empleados no firmen los acuerdos de confidencialidad o no divulgación para la protección de la información relacionada con .	1-Raro	1-Insignificante	R63	1	Riesgo Inusual
Entrevista Jefe Gestión de la configuración	Proteger la información del proyecto , que usa redes públicas contra actividades como fraudes, disputas contractuales, divulgación o modificación no autorizada.	A.14.1.2	Fraude, disputa contractual, divulgación o modificación no autorizada de la información del proyecto al exponerse sin medidas de seguridad en redes públicas.	5-Certero	4-Mayor	R64	20	Riesgo Extremo

Entrevista Jefe Gestión de la configuración	Evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada para el proyecto .	A.14.1.3	Transmisiones incompletas, enrutamiento errado, alteración no autorizada de mensajes, divulgación no autorizada y duplicación o reproducción de mensajes no autorizada para el proyecto .	5-Certero	5- Catastrófico	R65	25	Riesgo Extremo
Entrevista Jefe Gestión de la configuración	Establecer y aplicar las reglas de desarrollo de software y de sistemas que se enmarquen dentro de la política de desarrollo seguro para el proyecto.	A.14.2.1	Demora en la atención de solución de problemas por no existir unanimidad en el código fuente.	5-Certero	4-Mayor	R66	20	Riesgo Extremo
Entrevista Jefe Gestión de la configuración	Revisar los cambios de plataformas de operación críticas del negocio, y realizar las pruebas sobre los cambios para evitar algún impacto adverso en las operaciones de seguridad de la información del proyecto .	A.14.2.3	Realizar cambios en la plataforma sin autorización y desconociendo el impacto sobre el proyecto vertical de la salud.	5-Certero	2- Menor	R67	10	Riesgo Alto
Entrevista PMO, INFRAESTRUCTURA	Controlar estrictamente y desalentar los cambios o modificaciones a los paquetes de software del proyecto.	A.14.2.4	Poner en el ambiente productivo versiones del aplicativo que no estén validadas y probadas.	5-Certero	3- Moderado	R68	15	Riesgo Extremo
Entrevista PMO	Establecer, documentar y mantener principios para la construcción de sistemas seguros .	A.14.2.5	Construir del software inseguro.	5-Certero	5- Catastrófico	R69	25	Riesgo Extremo
Entrevista Jefe Gestión de la configuración	Establecer y proteger adecuadamente los ambientes de desarrollo seguro contemplados dentro del ciclo de vida del desarrollo de sistemas de información del proyecto.	A.14.2.6	Cambios no autorizados por parte del personal de desarrollo afecte directamente el código fuente o el producto final.	5-Certero	5- Catastrófico	R70	25	Riesgo Extremo
Entrevista Jefe Gestión de la configuración y PMO	Supervisar y hacer seguimiento de las actividades de desarrollo de sistemas contratados externamente .	A.14.2.7	No cumplir los compromisos y las expectativas del cliente, por la falta de controles de supervisión en las actividades de desarrollo.	3-Posible	3- Moderado	R71	9	Riesgo Medio
Entrevista Jefe Gestión de la configuración y PMO	Realizar las pruebas de funcionalidad de la seguridad de la información .	A.14.2.8	Desplegar el aplicativo en el ambiente productivo con vulnerabilidades en seguridad.	5-Certero	5- Catastrófico	R72	25	Riesgo Extremo
Entrevista Jefe Gestión de la configuración y PMO	Establecer los programas de pruebas y criterios de aceptación de los sistemas nuevos, actualizados y nuevas versiones para el proyecto.	A.14.2.9	Rechazo por parte de los Clientes debido a que los aplicativos desarrollados no se les hacen pruebas de aceptación.	3-Posible	2- Menor	R73	6	Riesgo Medio
Entrevista Jefe Gestión de la configuración y PMO	Seleccionar, proteger y controlar cuidadosamente los datos de pruebas del proyecto .	A.14.3.1	Fuga, pérdida o daño de los datos usados para realizar las pruebas.	3-Posible	2- Menor	R74	6	Riesgo Medio
CSI y PMO	Diseñar la política con los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de información por parte de los proveedores del proyecto.	A.15.1.1	Acceso no controlado a la información para los proveedores del proyecto , permitiendo fuga, robo, daño, alteración u otra actividad malintencionada.	5-Certero	5- Catastrófico	R75	25	Riesgo Extremo
CSI y OGA	Establecer y acordar todos los requisitos de seguridad de la información pertinentes para cada proveedor en cuanto al acceso, procesamiento, almacenado, comunicado y suministro de componentes de infraestructura de la información del proyecto.	A.15.1.2	No acordar los requisitos de seguridad de la información del proyecto a los proveedores con respecto al acceso, procesamiento, almacenado y comunicado.	3-Posible	4-Mayor	R76	12	Riesgo Alto
Entrevista Jefe de iNFRAESTRUCTURA	Incluir en la cadena de suministro los requisitos para tratar los riesgos asociados con productos y servicios de tecnología de la información y comunicación .	A.15.1.3	Los proveedores desconozcan los acuerdos para tratar los riesgos de seguridad de la información, asociados a los productos y servicios de tecnología.	4-Probable	4-Mayor	R77	16	Riesgo Extremo
Entrevista CSI. INFRAESTRUCTURA , Gestión de la configuración	Realizar control en el seguimiento, revisión y auditoría de la prestación de servicios de los proveedores .	A.15.2.1	La capacidad en la prestación de servicios prestados por los proveedores sean insuficientes para el proyecto .	3-Posible	2- Menor	R78	6	Riesgo Medio

Entrevista CSI. INFRAESTRUCTURA, Gestión de la configuración	Gestionar los cambios, mantenimiento y mejora de las políticas, procedimientos y controles para los servicios que prestan los proveedores.	A.15.2.2	No gestionar los cambios en el suministro de servicios que prestan los proveedores que afecten el proyecto .	4-Probable	2- Menor	R79	8	Riesgo Medio
Entrevista CSI. INFRAESTRUCTURA, Gestión de la configuración	Establecer las responsabilidades y procedimientos de gestión de incidentes de seguridad de la información de manera rápida, eficaz y ordenada para el proyecto .	A.16.1.1	No atender los incidentes de seguridad de la información para el proyecto .	5-Certero	5- Catastrófico	R80	25	Riesgo Extremo
Entrevista CSI. INFRAESTRUCTURA, Gestión de la configuración	• Informar los eventos de seguridad de la información del proyecto a través de los canales de gestión apropiados, lo antes posible. • Exigir a los empleados y contratistas del proyecto , que reporten cualquier debilidad asociada a la seguridad de la información.	A.16.1.2 A.16.1.3	No informar a las personas a cargo o responsables sobre los eventos que se presenten durante la operatividad del proyecto .	5-Certero	5- Catastrófico	R81	25	Riesgo Extremo
Entrevista CSI. INFRAESTRUCTURA, Gestión de la configuración	• Evaluar y clasificar los eventos de seguridad de la información . • Establecer los procedimientos para dar respuesta a los eventos de seguridad de la información del proyecto.	A.16.1.4 A.16.1.5	Eventos repetitivos sin resolver sobre la seguridad de la información.	5-Certero	5- Catastrófico	R82	25	Riesgo Extremo
Entrevista CSI. INFRAESTRUCTURA, Gestión de la configuración	Transmitir el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la posibilidad e impacto de incidentes futuros del proyecto .	A.16.1.6	Incidentes repetitivos de seguridad de la información sin reducir el impacto sobre el proyecto .	5-Certero	5- Catastrófico	R83	25	Riesgo Extremo
Entrevista CSI. INFRAESTRUCTURA, Gestión de la configuración	Crear los procedimientos para la identificación, recolección, adquisición y preservación de las evidencias asociadas a los incidentes de la seguridad de la información.	A.16.1.7	No identificar, recolectar y preservar las evidencias asociadas a los incidentes de la seguridad de la información, por falta de los procedimientos.	5-Certero	4-Mayor	R84	20	Riesgo Extremo
Entrevista CSI. INFRAESTRUCTURA, Gestión de la configuración	• Planificar la continuidad de la seguridad de la información . • Establecer, documentar, implementar y mantener proceso, procedimientos y controles para asegurar el nivel de continuidad para situaciones adversas. • Verificar, revisar y evaluar a intervalos los controles de la continuidad de la seguridad de la información, con el fin de asegurar su validez y eficacia durante situaciones adversas del proyecto. • Cumplir los requisitos de disponibilidad con redundancia suficiente para las instalaciones de procesamiento ante situaciones adversas .	A.17.1.1 A.17.1.2 A.17.1.3 A.17.2.1	La continuidad del proyecto , por falta del plan de continuidad antes desastres, crisis o situaciones adversas.	5-Certero	5- Catastrófico	R85	25	Riesgo Extremo
Entrevista Jefe CSI y PMO	• Identificar todos los requisitos estatutarios, reglamentarios y contra actuales aplicables al proyecto , y mantenerlos actualizados. • Implementar procedimientos para el cumplimiento de los requisitos legislativos, de reglamentación y contra actuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentado en . • Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contra actuales y del proyecto . • Asegurar la privacidad y la protección de la información de datos personales, como lo exige la legislación y la reglamentación pertinentes, cuando sea aplicable para el proyecto. • Usar controles criptográficos en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes . • Realizar revisiones independientes de la seguridad de la información. • El personal a cargo de las áreas, revisará con regularidad el cumplimiento de los procesos y procedimientos dentro de cada área, asociados la seguridad de la información del proyecto. • Periódicamente revisar los sistemas de información para determinar el cumplimiento de las políticas y normas la seguridad de la información del proyecto.	A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5 A.18.2.1 A.18.2.2 A.18.2.3	Incumplir los requisitos legales, de reglamentación o contra actuales relacionados con los derechos de propiedad intelectual y de uso de productos de software. No asegurar la privacidad y la protección a los datos personales conforme a la legislación.	5-Certero	5- Catastrófico	R86	25	Riesgo Extremo

Fuente: Elaboración propia

Tabla 16. Anexo C valoración cuantitativa de los riesgos de los objetivos de control NTC – ISO/IEC 27001:2013

METODOLOGIA DE MAGERIT: VALORACION DEL RIESGO - APROBADA POR EL DIRECTOR.

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
POLITICA DE LA SEGURIDAD DE LA INFORMACION	CRITICO	15	25	25	25	25	23
Orientacion de la Direccion para la Gestion de la Segu	CRITICO	15	25	25	25	25	23
Politicas para la Seguridad de la Informacion	CRITICO	15	25	25	25	25	23
Revision de las Politicas para Seguridad de la Informa	CRITICO	15	25	25	25	25	23
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACI	CRITICO	15	25	25	25	25	23
Organización Interna	CRITICO	15	25	25	25	25	23
Seguridad de la Informacion Roles y Responsabilidade	CRITICO	15	25	25	25	25	23
Separacion de Deberes	CRITICO	15	25	25	25	25	23
Contacto con las Autoridades	CRITICO	15	25	25	25	25	23
Contactos con grupos de interes especial	CRITICO	15	25	25	25	25	23
Seguridad de la Informacion en Gestion de Proyectos	CRITICO	15	25	25	25	25	23
Dispositivos moviles y teletrabajo	CRITICO	15	25	25	25	25	23
Politica para dispositivos moviles	CRITICO	15	25	25	25	25	23
Teletrabajo	CRITICO	15	25	25	25	25	23
SEGURIDAD DE LOS RECURSOS HUMANOS	CRITICO	15	25	25	25	25	23
Antes de asumir el empleo	CRITICO	15	25	25	25	25	23
Selección	CRITICO	15	25	25	25	25	23
Terminos y Condiciones del empleo	CRITICO	15	25	25	25	25	23
Durante la Ejecucion del empleo	CRITICO	15	25	25	25	25	23
Responsabilidades de la Direccion	CRITICO	15	25	25	25	25	23
Toma de conciencia, educacion y formacion de la segu	CRITICO	15	25	25	25	25	23
Proceso disciplinario	CRITICO	15	25	25	25	25	23
Terminacion y cambio de empleo	CRITICO	15	25	25	25	25	23
Terminacion o cambio de responsabilidades de emple	CRITICO	15	25	25	25	25	23
GESTION DE ACTIVOS	IMPORTANTE	15	20	20	20	20	19
Responsabilidad por los Activos	IMPORTANTE	15	20	20	20	20	19
Inventario de Activos	IMPORTANTE	15	20	20	20	20	19
Propiedad de los Activos	IMPORTANTE	15	20	20	20	20	19
Uso Aceptable de los activos	IMPORTANTE	15	20	20	20	20	19
Devolucion de los Activos	IMPORTANTE	15	20	20	20	20	19
Clasificacion de la Informacion	IMPORTANTE	15	20	20	20	20	19
Clasificacion de la Informacion	IMPORTANTE	15	20	20	20	20	19
Etiquetado de la Informacion	IMPORTANTE	15	20	20	20	20	19
Manejo de Activos	IMPORTANTE	15	20	20	20	20	19
Manejo de medios de soporte	IMPORTANTE	15	20	20	20	20	19
Gestion de medios de soporte removibles	IMPORTANTE	15	20	20	20	20	19
Disposicion de los medios de soporte	IMPORTANTE	15	20	20	20	20	19
Transferencia de medios de soporte fisicos	IMPORTANTE	15	20	20	20	20	19

CONTROL DE ACCESO	CRITICO	15	25	25	25	25	23
Requisitos del negocio para control de acceso	CRITICO	15	25	25	25	25	23
Politica de control de acceso	CRITICO	15	25	25	25	25	23
Acceso a redes y servicios en red	CRITICO	15	25	25	25	25	23
Gestion de Acceso de usuarios	CRITICO	15	25	25	25	25	23
Registro y cancelacion del registro de usuarios	CRITICO	15	25	25	25	25	23
Suministro de acceso a usuarios	CRITICO	15	25	25	25	25	23
Gestion de derechos de acceso privilegiado	CRITICO	15	25	25	25	25	23
Gestion de Informacion de autenticacion secreta de us	CRITICO	15	25	25	25	25	23
Revision de los derechos de acceso de usuarios	CRITICO	15	25	25	25	25	23
Cancelacion o ajuste de los derechos de acceso	CRITICO	15	25	25	25	25	23
Responsabilidades de los usuarios	CRITICO	15	25	25	25	25	23
Uso de Informacion secreta	CRITICO	15	25	25	25	25	23
Control de Acceso a Sistemas y Aplicaciones	CRITICO	15	25	25	25	25	23
Restriccion de acceso a informacion	CRITICO	15	25	25	25	25	23
Procedimiento de conexión segura	CRITICO	15	25	25	25	25	23
Sistema de Gestion de contraseña	CRITICO	15	25	25	25	25	23
Uso de programas utilitarios privilegiados	CRITICO	15	25	25	25	25	23
Control de acceso a codigos fuente de programas	CRITICO	15	25	25	25	25	23
CRIPTOGRAFIA	CRITICO	15	25	25	25	25	23
Controles Criptograficos	CRITICO	15	25	25	25	25	23
Politica sobre el uso de controles criptograficos	CRITICO	15	25	25	25	25	23
Gestion de Claves	CRITICO	15	25	25	25	25	23
SEGURIDAD FISICA Y AMBIENTAL	BAJO	15	4	4	4	4	6
Areas Seguras	BAJO	15	4	4	4	4	6
Perimetro de seguridad fisica	BAJO	15	4	4	4	4	6
controles fisicos de entrada	BAJO	15	4	4	4	4	6
Seguridad de oficinas, salones e instalaciones	BAJO	15	4	4	4	4	6
Proteccion contra amenazas externas y ambientales	BAJO	15	4	4	4	4	6
trabajo en areas seguras	BAJO	15	4	4	4	4	6
Areas de Despacho y carga	BAJO	15	4	4	4	4	6
Equipos	BAJO	15	4	4	4	4	6
Ubicación y proteccion de los equipos	BAJO	15	4	4	4	4	6
Servicios publicos de soporte	BAJO	15	4	4	4	4	6
Seguridad del cableado	BAJO	15	4	4	4	4	6
Mantenimiento de equipos	BAJO	15	4	4	4	4	6
Retiro de activos	BAJO	15	4	4	4	4	6
Seguridad de equipos y activos fuera del predio	BAJO	15	4	4	4	4	6
Disposicion segura o reutilizacion de equipos	BAJO	15	4	4	4	4	6
Equipos sin la supervision de los usuarios	BAJO	15	4	4	4	4	6
Politica de escritorio limpio y pantalla limpia	BAJO	15	4	4	4	4	6
SEGURIDAD DE LAS OPERACIONES	IMPORTANTE	15	20	20	20	20	19
Procedimientos operacionales y responsabilidades	IMPORTANTE	15	20	20	20	20	19
Procedimientos de operación documentadas	IMPORTANTE	15	20	20	20	20	19
Gestion de cambios	IMPORTANTE	15	20	20	20	20	19
Gestion de Capacidad	IMPORTANTE	15	20	20	20	20	19
Separacion de los ambientes de desarrollo, ensayo y c	IMPORTANTE	15	20	20	20	20	19
Proteccion contra codigos maliciosos	IMPORTANTE	15	20	20	20	20	19
Controles contra codigos maliciosos	IMPORTANTE	15	20	20	20	20	19
Copias de Respaldo	IMPORTANTE	15	20	20	20	20	19
Copias de respaldo de la informacion	IMPORTANTE	15	20	20	20	20	19
Registro y Seguimiento	IMPORTANTE	15	20	20	20	20	19
Registro de eventos	IMPORTANTE	15	20	20	20	20	19

Proteccion de la Informacion de registro	IMPORTANTE	15	20	20	20	20	19
Registros del administrador y del operador	IMPORTANTE	15	20	20	20	20	19
Sincronizacion de Relojes	IMPORTANTE	15	20	20	20	20	19
Control de Software Operacional	IMPORTANTE	15	20	20	20	20	19
Instalacion de software en Sistemas Operativos	IMPORTANTE	15	20	20	20	20	19
Gestion de Vulnerabilidad Tecnica	IMPORTANTE	15	20	20	20	20	19
Gestion de las vulnerabilidades tecnicas	IMPORTANTE	15	20	20	20	20	19
Restricciones sobre la instalacion de software	IMPORTANTE	15	20	20	20	20	19
Consideraciones sobre auditoria de Sistemas de Inforr	IMPORTANTE	15	20	20	20	20	19
Controles sobre auditorias de sistemas de informacior	IMPORTANTE	15	20	20	20	20	19
SEGURIDAD DE LAS COMUNICACIONES	IMPORTANTE	15	20	20	20	20	19
Gestion de Seguridad de Redes	IMPORTANTE	15	20	20	20	20	19
Controles de redes	IMPORTANTE	15	20	20	20	20	19
Seguridad de los Servicios de Red	IMPORTANTE	15	20	20	20	20	19
Separacion en las redes	IMPORTANTE	15	20	20	20	20	19
Transferencia de Informacion	IMPORTANTE	15	20	20	20	20	19
Politicas y procedimientos de transferencia de Informa	IMPORTANTE	15	20	20	20	20	19
Acuerdos sobre transferencia de informacion	IMPORTANTE	15	20	20	20	20	19
Mensajes electronicos	IMPORTANTE	15	20	20	20	20	19
Acuerdos de confidencialidad o de no divulgacion	IMPORTANTE	15	20	20	20	20	19
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE S	CRITICO	15	25	25	25	25	23
Requisitos de Seguridad de los Sistemas de Informacio	CRITICO	15	25	25	25	25	23
Analisis y especificacion de requisitos de seguridad de	CRITICO	15	25	25	25	25	23
Seguridad de servicios de las aplicaciones en las rede	CRITICO	15	25	25	25	25	23
Proteccion de transacciones de servicios de aplicacior	CRITICO	15	25	25	25	25	23
Seguridad en los procesos de desarrollo y de soporte	CRITICO	15	25	25	25	25	23
Politica de desarrollo seguro	CRITICO	15	25	25	25	25	23
procedimiento de control de cambios en sistemas	CRITICO	15	25	25	25	25	23
Revision tecnica de aplicaciones despues de cambios	CRITICO	15	25	25	25	25	23
Restricciones sobre los cambios de paquetes de softw	CRITICO	15	25	25	25	25	23
Principios de construccion de sistemas seguros	CRITICO	15	25	25	25	25	23
ambiente de desarrollo seguro	CRITICO	15	25	25	25	25	23
Desarrollo contratado externamente	CRITICO	15	25	25	25	25	23
Pruebas de seguridad de sistemas	CRITICO	15	25	25	25	25	23
Pruebas de aceptacion de sistemas	CRITICO	15	25	25	25	25	23
Datos de Ensayo	CRITICO	15	25	25	25	25	23
Proteccion de datos de ensayo	CRITICO	15	25	25	25	25	23
RELACIONES CON LOS PROVEEDORES	CRITICO	15	25	25	25	25	23
Seguridad de la Informacion en las relaciones con los	CRITICO	15	25	25	25	25	23
Politica de seguridad de la informacion para la relacio	CRITICO	15	25	25	25	25	23
Tratamiento de la seguridad dentro de los acuerdos co	CRITICO	15	25	25	25	25	23
Cadena de suministro de tecnologia de informacion y	CRITICO	15	25	25	25	25	23
Gestion de la Prestacion de Servicios de proveedores	CRITICO	15	25	25	25	25	23
Seguimiento y revision de los servicios de los proveed	CRITICO	15	25	25	25	25	23
Gestion de cambios a los servicios de los proveedores	CRITICO	15	25	25	25	25	23
GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INF	IMPORTANTE	15	20	20	20	20	19
Gestion de Incidentes y Mejoras en la Seguridad de la	IMPORTANTE	15	20	20	20	20	19
Responsabilidades y procedimientos	IMPORTANTE	15	20	20	20	20	19
Informe de eventos de seguridad de la informacion	IMPORTANTE	15	20	20	20	20	19
Informe de debilidades de seguridad de la informacior	IMPORTANTE	15	20	20	20	20	19
Evaluacion de eventos de seguridad de la informacion	IMPORTANTE	15	20	20	20	20	19
Respuesta a incidentes de la seguridad de la informac	IMPORTANTE	15	20	20	20	20	19
Aprendizaje obtenido de los incidentes de seguridad d	IMPORTANTE	15	20	20	20	20	19
Recoleccion de la evidencia	IMPORTANTE	15	20	20	20	20	19

ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA	CRITICO	15	25	25	25	25	23
Continuidad de Seguridad de la Informacion	CRITICO	15	25	25	25	25	23
Planificacion de la continuidad de la seguridad de la in	CRITICO	15	25	25	25	25	23
Implementacion de la continuidad de la seguridad de l	CRITICO	15	25	25	25	25	23
Verificacion, revision y evaluacion de la continuidad d	CRITICO	15	25	25	25	25	23
Redundancia	CRITICO	15	25	25	25	25	23
Disponibilidad de instalaciones de procesamiento de i	CRITICO	15	25	25	25	25	23
CUMPLIMIENTO	CRITICO	15	25	25	25	25	23
Cumplimiento de requisitos legales y contractuales	CRITICO	15	25	25	25	25	23
Identificacion de los requisitos de legislacion y contra	CRITICO	15	25	25	25	25	23
Derechos de propiedad intelectual	CRITICO	15	25	25	25	25	23
Proteccion de registros	CRITICO	15	25	25	25	25	23
Privacidad y proteccion de la informacion identificable	CRITICO	15	25	25	25	25	23
Reglamentacion de controles criptograficos	CRITICO	15	25	25	25	25	23
Revisiones de Seguridad de la Informacion	CRITICO	15	25	25	25	25	23
Revision independiente de la seguridad de la informac	CRITICO	15	25	25	25	25	23
Cumplimiento con las politicas y normas de seguridad	CRITICO	15	25	25	25	25	23
Revision del cumplimiento tecnico	CRITICO	15	25	25	25	25	23

Fuente: Elaboración propia