DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL FONDO DE EMPLEADOS FEBIMBO EN EL ÁREA DE TECNOLOGÍA

JUAN CARLOS OSPINA REYES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL FONDO DE EMPLEADOS FEBIMBO EN EL ÁREA DE TECNOLOGÍA

JUAN CARLOS OSPINA REYES

PROYECTO DE GRADO – PROYECTO APLICADO PRESENTADO PARA OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Ing. JOEL CARROLL VARGAS M.Sc
DIRECTOR PROYECTO DE GRADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 21 Junio 2023

TABLA DE CONTENIDO

Pág.

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

GLOSARIO

ACTIVO DE INFORMACION: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de FEBIMBO y, en consecuencia, debe ser protegido.

ACUERDO DE CONFIDENCIALIDAD: documento en los que los funcionarios de FEBIMBO o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Entidad.

AMENAZA: es la probabilidad de que un evento revele una vulnerabilidad en particular. Esta es cualquier probabilidad que pueda conducir a un resultado no deseado para la organización o para un activo en particular.

AUTENTICACIÓN: es un procedimiento que verifica la identidad de un usuario o recurso tecnológico, para acceder a un recurso o sistema.

CIFRADO: es el camio criptográfico de datos para crear datos encriptados y asegurar su información personal. La codificación es útil para predecir fugas de información.

CONFIDENCIALIDAD: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

CONTROL: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

DISPONIBILIDAD: información accesible y utilizable una vez que lo necesite una entidad u empresa.

INTEGRIDAD: “es la garantía de que la información a la que se accede no se ha alterado y que lo que allí se lee es exactamente lo que se pretende.”[1]

ISO27001: regla universal la cual posibilita gestionar la estabilidad de la información.

RIESGO: posibilidad de que los activos de información reciban cualquier efecto negativo de una amenaza.

SEGURIDAD DE LA INFORMACIÓN: “la seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas

[1] Seguridad en Sistemas de Información: Confidencialidad, Integridad y Disponibilidad. (s. f.). https://www.tecnologias-informacion.com/seguridad.html

tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos."[2]

SGSI: "parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información."[3]

VULNERABILIDAD: agotamiento de un activo o control que podría ser explotado por una o más amenazas.

[2] Colaboradores de Wikipedia. (2022b, noviembre 20). Seguridad de la información. Wikipedia, la enciclopedia libre. https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n

[3] Subsistema de Seguridad de la Información (SGSI) - Universidad Distrital Francisco José de Caldas. (s. f.). http://planeacion.udistrital.edu.co:8080/sigud/s/sgsi

RESUMEN

Hoy en día, toda organización debe asegurar sus activos, he información, adicional estas deben contar con un sistema de seguridad básico o avanzado, para proteger la información procesada y almacenada en cualquier empresa, ya que actualmente la información es lo más importante, he indispensables de cualquier empresa.

Al poder diseñar el SGSI se podrá conocer las fortalezas y debilidades, para generar controles adecuados a la información y diseñar las políticas de seguridad de información que hacen parte del sistema, esto también ayudara a mejorar los procesos de auditorías y mejoras continuas.

Aquí se realizará el diseño de un SGSI para Febimbo, todo esto para mejorar su área de tecnología y a su vez asegurar mejores prácticas.

Todos los elementos que esto con lleva, documentación y los métodos requeridos son necesarios para realizar el SGSI. Por tanto, se realizará un estudio cualitativo y cuantitativo de amenazas, vulnerabilidades y demás de la organización, debido a que en la actualidad no muchas empresas cuentan con recursos destinados para IT, en este caso se ayudó a la organización para diseñar y luego a futuro poder implementarlo.

ABSTRACT

Nowadays, every organization must ensure its assets, and information, in addition these must have a basic or advanced security system, to protect the information processed and stored in any company, since currently the information is the most important, and indispensable of any company.

By being able to design the ISMS it will be possible to know the strengths and weaknesses, to generate adequate controls to the information and to design the information security policies that are part of the system, this will also help to improve the audits and continuous improvement processes.

Here we will design an ISMS for Febimbo, all this to improve its technology area and in turn ensure best practices.

All the elements that this with leads, documentation and the required methods are necessary to realize the ISMS. Therefore, a qualitative and quantitative study of threats, vulnerabilities and others of the organization will be made, due to the fact that currently not many companies have resources for IT, in this case we helped the organization to design and then in the future to implement it.

INTRODUCCIÓN

Desde hace unos años, la información se define como el activo más importante de una empresa, uno de los cuales vuelve a ser el patrimonio informativo de cualquier organización, todo este tema en la actualidad está tomando prioridad y estamos viendo cómo se fortalece cada día la seguridad informática.

Por eso es bien conocido que los sistemas de información que soportan o controlan los procesos de cualquier organización o negocio, se resisten a perder su información y sus insumos llevan a que el producto o servicio se convierta en un activo o ítem de la empresa.

Efectivamente, la información es uno de los recursos más relevantes de toda empresa, tanto del sector privado como público, la cual debe ser protegida por un SGSI que permita prevenir las pérdidas ocasionadas por muchas organizaciones.

Con el diseño del SGSI, podrán establecer una cultura de calidad dentro de Febimbo que opere de manera confiable. La seguridad de IT es un proceso en el que el riesgo debe evaluarse y gestionarse mediante políticas y estándares que satisfagan las necesidades de seguridad de la organización.

El SGSI aquí realizado es fundamental para proteger los activos de IT y toda la información y comunicaciones de Febimbo, para que cumplan con los criterios de confidencialidad integridad y disponibilidad.

La confidencialidad de la información es una prioridad de Febimbo y por tanto es responsabilidad de todos los Empleados asegurar que no se lleven a cabo actividades contrarias a la naturaleza y espíritu de cada una de estas políticas.

El diseño del SGSI para Febimbo nació por necesidad, ya que la empresa está creciendo cada vez más y mejorando su infraestructura IT, por lo tanto, la información que se maneja en diferentes programas es lo más importante, el SGSI permitirá proteger con más controles y políticas la información, se implementar reglas y una buena rutina, para asegurarse de que la información funciona de manera correcta y estará protegida.

Ya para terminar el diseño del SGSI de Febimbo introducirá los primeros pasos y procesos que evaluaran la importancia de la información en los diversos procesos de la empresa; también al grupo de trabajo se explicara sobre el funcionamiento de las distintas tecnologías de la información y la comunicación mediante reuniones y presentaciones.

1 PLANTEMIENTO DEL PROBLEMA

En esta nueva era tecnológica, muchos aspectos de la seguridad de la información son de vital importancia, tanto para grandes como pequeñas empresas, porque ante tantas vulnerabilidades se debe proteger la información de intrusos o ataques que no se esperan, deben proteger lo más valioso de toda organización que es la información.

Al diseñar el SGSI, la compañía podrá detectar y establecer la mejor manera para realizar procedimientos de IT y así tener un mejor manejo de su información.

Por esta razón las empresas quieren garantizar la información con normas que permitan generar adecuadas políticas y procedimientos, que se pueden implementar en cualquier organización.

La protección de los recursos de información con los que cuenta Febimbo, no son suficientes, ya que no cuentan con ningún estudio que pueda validar la seguridad y someterse a situación de perdida de información que pueda afectar la empresa.

En el momento Febimbo tiene una infraestructura tecnológica que ha sufrido algunos cambios por el tema de la pandemia o Covid-19, que ha fortalecido el área de IT y han podido dar continuidad al negocio.

Como tal Febimbo no cuenta con una política de seguridad de información que permita controlar y procesar la información, por ello se debe implementar el SGSI para poder mitigar los riesgos que puedan afectar la seguridad de la información.

Aquí también se evidencia a los usuarios que por falta del SGSI en la compañía, esta se expone a muchas amenazas en la red que puede afectar o perjudicar a la organización.

1.1 FORMULACIÓN DEL PROBLEMA

¿Cómo garantizará el diseño de un sistema de gestión de seguridad de la información basado en ISO 27001:2013 la disponibilidad y protección de la información en el fondo de empleados Febimbo?

2 JUSTIFICACIÓN

Hoy en las organizaciones y empresas se necesita disponer de una estrategia o táctica que plantee un proyecto con el cual se debe defender la seguridad de la información, una de las estrategias creadas para que tengan algunos lineamientos y controles, que permitan mitigar o reducir los peligros que suponen una potencial amenaza contra la información.

Los riesgos provocados por la indebida manipulación de las tecnologías presentes en Febimbo, sean de forma premeditada o sin alguna intensión, son algunas de las fuentes que ponen en riesgo la continuidad del negocio; de tal forma que, un SGSI se especifiquen políticas y controles que logran mantener la confidencialidad, integridad y disponibilidad de la información, con esto resultara más sencillo actuar frente a cualquier evento fortuito que afecte la continuidad de la compañía, debido a que se contara con herramientas para actuar frente a estas amenazas.

Igualmente, cabe resaltar que un SGSI para el fondo de empleados febimbo, ayudara a reconocer los recursos tecnológicos presentes, los cuales, permiten el constante movimiento de información, teniendo presente todos los procesos de IT que desarrollen las diversas zonas empresariales; además de identificar riesgos asociados a cada activo.

Igualmente, el SGSI creará confianza entre los asociados de febimbo, para que cuando tengan nuevos ingresos, poder ofrecer que su información este segura, por lo tanto, cada cliente tendrá la plena seguridad de que los datos entregados cuentan con confidencialidad.

Al diseñar el SGSI bajo la norma ISO/IEC 27001:2013, generará firmes lineamientos a las exigencias de seguridad de IT, lo que llevará a Febimbo a mejorar la competitividad y crear confianza entre sus posibles y futuros asociados.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de seguridad de información para el fondo de empleados Febimbo, basado en la norma ISO 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Caracterizar la situación actual del fondo de empleados Febimbo, lo que permitirá conocer los procesos y procedimientos que allí se realizan.

- Identificar los activos de información que existen en el fondo de empleados Febimbo, para revisar los temas aplicables para el diseño del sistema de seguridad de información.

- Proponer los controles principales según la norma ISO 27001:2013 para garantizar la disponibilidad e integridad de la información.

- Formular las políticas de seguridad de la información que se pueden aplicar a Febimbo y que contribuyan a disminuir los riesgos identificados.

4 MARCO REFERENCIAL

4.1 ANTECEDENTES

Para desarrollar este plan es importante investigar las fuentes bibliográficas, especialmente para los proyectos que interactúen con el uso del SGSI, utilizando las normas ISO 27001:2013 y los proyectos desarrollados e implementados en los fondos de empleados.

Las siguientes referencias concuerdan con la necesidad de crear un SGSI, ya que es ampliamente aceptada para proteger la información y cumplir con los marcos de políticas nacionales bajo la norma ISO 27001:2013.

ISO 27001: 2013 SISTEMA DE SEGURIDAD DE LA INFORMACIÓN Planificación del diseño para los empleados de Febimbo en IT, proporciona la visión y permite que se haga realidad. Criterios de proceso para continuar utilizando el SGSI a fin de identificar peligros, detectarlos y mitigar estas amenazas.

El diseño de un proyecto aplicado con el propósito de administrar el caso actual Febimbo, interactuando con el SGSI; A través de observaciones y entrevistas, con esta información lograda, ayudará a conocer el estado de UT, lo que permitirá alcanzar algunas metas propuestas en este plan y esto será un referente para aplicarlo en proyectos más adelante.

También se mencionó el plan provisional o “SGSI basado en la norma ISO IEC 27001 PARA USOMET LTDA”[4], este de la ciudad de IBAGUÉ realizado en 2016, en la que demostró que el SGSI puede desarrollar una evaluación única en su tipo para identificar peligros y el efecto de la acción sin crear un producto; La identificación de peligros se realiza mediante la metodología MAGERIT, con el fin de brindar en última instancia la retroalimentación y las correspondientes recomendaciones a la gerencia sobre las medidas de control necesarias y evitar por las infracciones regulatorias tener siempre presente la disponibilidad y confidencialidad de la información.

Es importante especificar la opción DISEÑO Y COMPONENTES PARA SISTEMAS DE GESTIÓN DE SEGURIDAD DIRECTRICES PARA SISTEMAS DE INFORMACIÓN Basado en ISO IEC 27001: 2005 quien recomendó el uso de un SGSI en 2015:

Para diseñar un SGSI es fundamental comprender plenamente las fortalezas de una organización y las amenazas a las que se enfrenta en todo momento. Por lo

[4] (DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27001 PARA LA EMPRESA USOMET LTDA. EN LA CIUDAD DE IBAGUÉ. (s. f.). En unad.edu.co. https://repository.unad.edu.co/bitstream/handle/10596/12038/19307458.pdf?sequence=1&isAllowed=y

tanto, en esta situación se utilizará MAGERIT para enfocarse en idealizar el proceso además de tener una iniciativa clara sore los peligros que se pueden tomar y también se establecen garantías para ser utilizadas en caso de que surja algún peligro.

4.2 MARCO TEÓRICO

4.2.1 SGSI (sistema de Gestión de Seguridad de la Información)

Debido a que la información es el activo más importante y que cualquier empresa procesa, modifica y almacena para poder generar y extraer informes de los cuales poder tomar decisiones estratégicas sobre el crecimiento, esta debe protegerse por encima de todo. De ahí que este activo se convierta de gran valor y requiera cuidarla especialmente, aún más cuando la información pertenece a más personas o terceros. Por lo tanto, la protección debe tener las normas internacionales más altas y aplicables que puedan regulan la disponibilidad, integridad y confidencialidad de toda información.

La empresa está diseñando y colocando en marcha el SGSI, ya que es de gran importancia para cualquier organización, ya que permite identificar las amenazas o falencias y riesgos en los que se pueden exponer los recursos de información, para así poder crear controles y lineamientos que permitan cumplir las actividades de las organizaciones sin colocar en riesgo los recursos de comunicación e información.

“Por lo tanto, un SGSI es un conjunto de políticas, procedimientos y pautas junto con sus recursos y actividades asociados que son administrados colectivamente por una organización para proteger sus activos de información esenciales”[5]

El SGSI se basa en prácticas que durante los años han mostrado excelentes en las empresas y mejoras de la estabilidad de sus activos de información y que permiten realizarlo por medio de medidas tanto físicas como lógicas a grado de estabilidad y de esta forma poder identificar amenazas y asegurar la continuidad del negocio.

Con este sistema que se basa en la gestión de información, se garantizaría lo siguiente:

[5] Alvarado, C. (2022, 5 octubre). Sistema de gestión de seguridad de la información: qué es y sus etapas. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

- **Confidencialidad**: es prevenir que se divulgue la información a personas o dispositivos que no están autorizados, es como si otra organización quiera ver la información y esta no cuente con los permisos necesarios y así no pueda utilizar ni manipular la información.[6]

- **Integridad**: es la función de proteger los datos que no fueron modificados a partir de su construcción sin autorización, este objetivo es primordial una vez que se está llevando a cabo trámites bancarios por Internet, ya que, toda compañía tendrá que asegurar que ningún intruso logre capturar y cambiar los datos en tránsito, bajo esta cualidad se asegura que la información esté precisa, sin modificaciones inapropiadas.[7]

- **Disponibilidad**: es como cuando se necesita información o elementos que sean requeridos, todo con la autorización pertinente, "La disponibilidad, junto a la confidencialidad, la integridad y la autenticación son los aspectos fundamentales de la seguridad de la información, y en la que están basados la inmensa mayoría de soluciones y recursos digitales que se usan en las compañías día tras día."[8]

4.2.2 ISO/IEC 27001:2013

Este estándar nació de la necesidad de asegurar y gestionar la estabilidad de la información que es acceso y salida de varios procesos de las empresas.

"ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2." [9]

Esta norma requiere algunos objetivos para cumplir el SGSI, todo esto con controles necesarios para dar cumplimiento a la norma, estos son:

- Entablar un marco metodológico para un SGSI.

---

[6] Morales, O. B. (s. f.). Comité de ética en investigación. Sitio Web del Comité de ética en investigación. https://www.incmnsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

[7] Santander, B. (s. f.). Integridad. Banco Santander. https://www.bancosantander.es/glosario/integridad-seguridad-online#:~:text=La%20integridad%20de%20los%20datos%20o%20de%20la%20informaci%C3%B3n%20garantiza,de%20forma%20accidental%20o%20intencionada.

[8] DocuSign, C. de. (2021, 17 agosto). Disponibilidad de la información: ¿Por qué es importante contar con opciones seguras? DocuSign. https://www.docusign.mx/blog/disponibilidad-de-la-informacion

[9] Qué es la norma ISO 27001 y para qué sirve. (2020, 17 diciembre). EALDE Business School. https://www.ealde.es/iso-27001-para-que-sirve/

- La adopción de controles proporcionales a los peligros notados.
- La documentación de políticas, métodos, controles y procedimiento de riegos.
- Identificación y asignación de responsabilidades al grado conveniente.
- Formalización, seguimiento y revisión de los controles y peligros, de manera sistemática (periódica) y metodológica.
- Generación y preservación de pruebas.
- Procedimiento de los incidentes de estabilidad.
- Revisión y optimización continúa del SGSI.
- Administración de Peligros
- Uso de métricas para evaluar efectividad y eficiencia de los controles y del propio SGSI.

"Todo esto requiere algunos métodos y requerimientos de la norma ISO/IEC 27001, bajo el ciclo Deming: Planificar, Hacer, Verificar, Actuar, (PHVA)."[10]

Todo esto se aplica a cualquier empresa, sin importar sea grande o pequeña o cualquier tipo de actividad, todo se puede lograr para permitir un grado de confianza a los clientes y proveedores, ya que el tratamiento de datos u activos, son lo más importante para la organización.

4.2.3 CICLO DEMING EN NORMA ISO/IEC 27001:2013

El estándar ha estipulado que al implementar un SGSI siempre comienza desde un estado inicial y se desarrolla bajo este estado y genera mejoras continuas en fases que se denominan colectivamente modelo PDCA o ciclo Deming.

"El modelo PDCA o "Planificar-Hacer-Verificar-Actuar" (Plan-Do-Check-Act, de sus siglas en inglés), tiene una serie de fases y acciones que permiten establecer un modelo de indicadores y métricas comparables en el tiempo, de manera que se pueda cuantificar el avance en la mejora de la organización." [11]

En esta etapa se planea el SGSI, debido a que se conforman las metas, con el inventario de activos y se acomoda todo al plan, todo lo mencionado con un grado de peligros y activos de información.

Con este estándar se garantizaría lo siguiente:

- **Hacer:** con los controles podrán mitigar las amenazas y poder implementar el SGSI.

[10] Toro, R. (2015, 4 junio). ISO 27001: Ciclo de Deming. PMG SSI - ISO 27001. https://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/

[11] Seguridad Informatica. (2018). En silo.tips. https://silo.tips/download/seguridad-privadanet

- **Verificar:** se realizan las validaciones pertinentes para que se cumplan los objetivos del SGSI, con esto se detectan errores y soluciones para que el sistema tenga continuidad.

- **Actuar**: Aquí las fallas serán solucionadas, todo esto para que la organización pueda controlar la actividad o proponer auditorías internas, que permitan evidenciar algún riesgo y poder mejorarlo.

Figura 1 - CICLO DEMING

Fuente: CRISAZA

“El mejoramiento continuo es aceptar que las cosas se pueden hacer mejor hoy que ayer, y que mañana podrán realizarse mejor de lo que hoy se han hecho. El ciclo presenta cuatro etapas que se desarrollan de manera secuencial, iniciando por cualquiera de ellas y repitiéndose de manera indefinida. Esta repetición indefinida es la que produce el mejoramiento continuo en la organización.

Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). El ciclo PHVA, es de gran utilidad para estructurar y ejecutar planes de mejora de calidad a cualquier nivel ejecutivo u operativo."[12]

4.2.4 METODOLOGÍA MAGERIT

Figura 2 - METODOLOGÍA MAGERIT

Fuente: TITHINK

"MAGERIT significa (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología de análisis y gestión de riesgos específicamente diseñada para los sistemas de información"[13]. Fue desarrollado por el Centro Criptológico Nacional de España (CCN) y es ampliamente utilizado por organismos públicos y empresas privadas.

Su objetivo es proporcionar un enfoque integral y sistemático para la identificación, análisis, evaluación, tratamiento y seguimiento de los riesgos relacionados con los sistemas de información.

---

[12] FILOSOFIA WILLIAM EDWARD DEMING. (2012, septiembre). maestrosdelacalidadop100111. http://maestrosdelacalidadop100111.blogspot.com/2012/09/filosofia-william-edward-deming.html

[13] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (2006). En pilar-tools. https://www.pilar-tools.com/doc/magerit/v2/meth-es-v11.pdf

La metodología tiene en cuenta las características y requisitos específicos de los sistemas de información y su entorno, tales como la confidencialidad, integridad, disponibilidad y trazabilidad de la información.

Esta consta de tres fases principales: planificación, análisis y tratamiento.
En la fase de planificación se define el alcance del análisis, se establecen los objetivos y criterios para la gestión de riesgos y se identifican los recursos necesarios para el análisis, aquí se verá como en la fase de análisis, los riesgos son identificados y evaluados en términos de su probabilidad e impacto en el sistema de información.

En la fase de tratamiento, los riesgos son tratados mediante la implementación de medidas de mitigación de riesgos o la transferencia del riesgo a terceros.
Esta es una metodología útil para las organizaciones que necesitan evaluar y gestionar los riesgos asociados a sus sistemas de información. Al aplicar MAGERIT, las organizaciones pueden identificar y priorizar los riesgos más importantes y desarrollar un plan de gestión de riesgos que se adapte a sus necesidades y requisitos específicos.

Su principal característica es dividir los conjuntos de información en diferentes grupos para cubrir los riesgos en cada uno de estos grupos; con esto podrán iniciar el desarrollo del sistema SGSI, para poder centrarse en los riesgos y que esto no cause algún problema en el negocio, esto también esta alineado con la norma ISO y no habrá problemas al poder certificarse.

"Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas." [14]

[14] 429 Error | ESET. (2013, 14 mayo). https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Figura 3 - MAGERIT TRATAMIENTO DEL RIESGO

Fuente: TITHINK

Con esta metodología todas las empresas que están iniciando la implementación del SGSI tendrán todo de manera más organizada, todo esto permite validar los riesgos que puedan causar la caída o falla del negocio, además de que está en línea con la norma ISO/IEC 27001.

4.3 MARCO CONCEPTUAL

Información: "desde el punto de vista de la ciencia de la computación, la información, es un conocimiento explícito extraído por seres vivos o sistemas expertos como resultado de interacción con el entorno o percepciones sensibles del mismo entorno. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del que posee dicha información con su entorno."[15]

Vulnerabilidad: son las debilidades que puede tener un objeto de información, que permiten la intrusión de amenazas, estas debilidades pueden surgir por una configuración o instalación incorrecta.[16]

Amenaza: en el contexto de las computadoras, una amenaza es cualquier cosa que comprometa la integridad, la confidencialidad y la disponibilidad de la información; tales amenazas incluyen incendios, inundaciones, disturbios,

[15] Información - OCHA Colombia Wiki. (s. f.). https://wiki.salahumanitaria.co/wiki/Informaci%C3%B3n

[16] Jiménez, M. M. (s. f.). Vulnerabilidades que afectan la seguridad de la información. https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

disturbios y delitos.[17]

Activo: son los elementos de valor para las empresas ya que las operaciones dependen de ellos, los activos incluyen los recursos tecnológicos, humanos y materiales.

Ataque: es el método utilizado para intentar divulgar o modificar los sistemas de información con el fin de controlarlos sin autorización, los ataques aprovechan las fallas o debilidades en los recursos de información.

Política: son estándares o lineamientos propuestos por empresas o instituciones para prevenir amenazas, estos lineamientos suelen ser estrictos y deben ser puestos en práctica por los empleados.

Impacto: alcance del impacto en los activos si una vulnerabilidad está amenazada.

Riesgo: es la posibilidad de que una amenaza se presente a una entidad o empresa y cause un desastre, lo que puede causar depende del grado de vulnerabilidad.

Seguridad de la información: es preservar la seguridad y confidencialidad de la información, todo esto gracias a que su integridad sea intacta y se tenga disponibilidad, autenticidad y fiabilidad.

Seguridad informática: "la seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático."[18]

4.4 MARCO HISTÓRICO

"EL FONDO DE EMPLEADOS DE BIMBO DE COLOMBIA S.A. "FEBIMBO", basa su razón de ser en los servicios ofrecidos a sus asociados y su grupo familiar, para resolver necesidades económicas, de capacitación, educación y calamidad, brindando facilidades para el acceso a los beneficios, basada en la contribución de los aportes sociales y ahorros permanentes de sus asociados."[19]

4.4.1 Reseña histórica

[17] Amenazas y vulnerabilidades de la seguridad informática. (s. f.). Scribd. https://es.scribd.com/document/474841443/Amenazas-y-vulnerabilidades-de-la-seguridad-informatica

[18] Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Información. (2021, 3 marzo). LISA Institute. https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

[19,17,18,19] Nosotros. (s. f.). https://www.febimbo.com/nuestra.html

"Constituido en octubre 24 de 1997, registrado ante la Cámara y Comercio y con personería jurídica 976721, bajo la supervisión de la Superintendencia de la Economía Solidaria, fue concebido con el propósito de unir esfuerzos para solucionar eventuales problemas económicos, con el ánimo de Fomentar el ahorro y propiciar el Progreso Familiar."[20]

4.4.2 Misión

"Somos una Empresa de Economía Solidaria de Ahorro y Crédito, financiera y administrativamente sólida, dedicada a satisfacer las necesidades de nuestros asociados y sus familias, ofreciéndoles beneficios servicios encaminados al mejoramiento continuo de su calidad de vida."[21]

4.4.3 Visión

"Lograr para el año 2021 FEBIMBO ser el mejor y mayor respaldo a nivel de desarrollo y calidad de vida de nuestros asociados, basado en la confiabilidad y solidaridad; soportado en el ahorro y crédito mediante la innovación constante, dinámica y futurista."[22]

4.4.4 Objetivos

"Febimbo tendrá como objetivos generales mejorar la calidad de vida, fomentar el ahorro de sus asociados con miras a generar recursos destinados especialmente a la satisfacción de sus necesidades de crédito; a la inversión en proyectos de desarrollo empresarial, así como actividades comerciales, industriales y de servicios que contribuyan al mejoramiento económico, social y cultural de sus asociados y sus familiares. Igualmente fomentará los lazos de respeto, solidaridad, compañerismo entre los mismos, y desarrollará la integración social y económica, para lo cual estrechará sus relaciones con otras entidades del sector solidario."[23]

4.4.5 Valores

"**Solidaridad:** Buscar el bien común de nuestros asociados, sus familias y nuestro entorno.

Transparencia: Actuamos de manera clara, confiable y oportuna

Equidad: Respeto y reconocimiento de que todos nuestros asociados tendrán los mismos derechos, deberes y oportunidades.
Responsabilidad Social: Es el actuar frente a nuestros clientes, asociados de negocio y el medio ambiente.

---

[23] Nosotros. (s. f.). https://www.febimbo.com/nuestra.html

Rentabilidad: Obtener resultados sociales y económicos en procura del crecimiento sostenible.

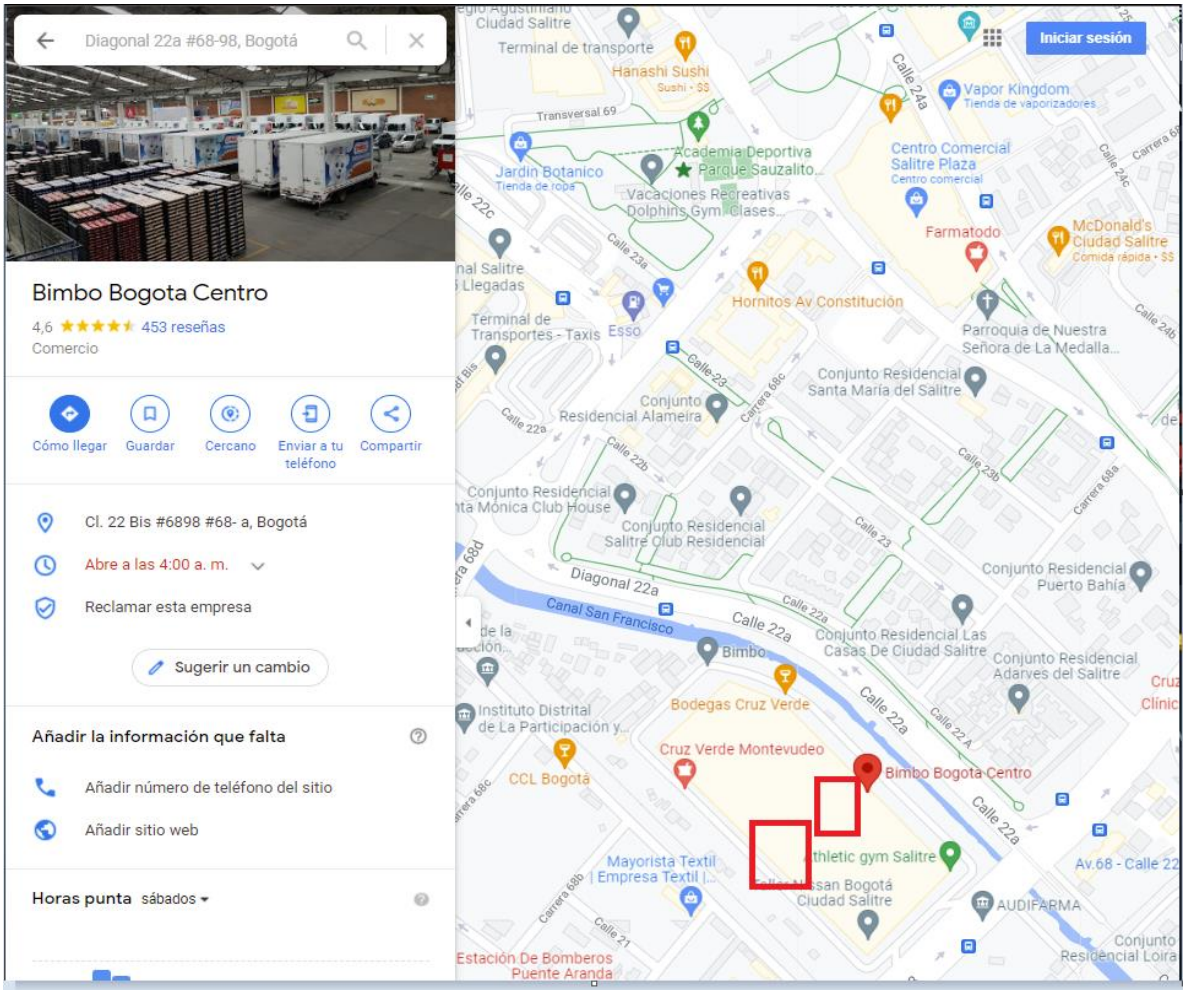
Servicio: Pasión por lo que hacemos."[24]

4.4.6 Domicilio y ámbito territorial

El domicilio principal de Febimbo es en la ciudad de Bogotá, república de Colombia, tiene operaciones en todo el territorio nacional.

Actualmente su dirección física donde realizan las operaciones es Diagonal 22A # 68-98 barrio Montevideo.

Figura 4 - Ubicación geográfica



Fuente: Propia

[24] Idem

El fondo de empleados Febimbo desarrolla varios programas de beneficio para un mejor desarrollo económico de las familias de los asociados, fomentando el servicio y ofreciendo las siguientes modalidades:

Ahorro Permanente: Suma periódica obligatoria que todo Asociado se compromete a entregar de manera permanente desde el momento de su Asociación: Sólo se reintegra cuando el asociado se desvincule de Febimbo. Juntos Aportes y ahorro permanentes dan base para la aprobación del cupo para créditos. Están afectados desde su origen a favor de Febimbo, como Garantía de las obligaciones que el Asociado contraiga con Febimbo.

Ahorro Programado: Línea de ahorro donde se establece un período de tiempo y el asociado ahorra de forma quincenal, dicho período de tiempo es de 3, 6 o 9 meses con una tasa del 5%, 7% y 9% según el período de ahorro programado, una vez finalizado el tiempo pactado se reintegra el ahorro más sus rendimientos, se hace un descuento quincenal mediante nómina y se tendrá en cuenta la capacidad de pago, que no exceda el 50% del salario.
CDTA: Es un certificado de depósito de ahorro a término, el cual ofrece una tasa de interés muy representativa respecto al mercado.[25]

Requisitos Asociación: Estar vinculado laboralmente de manera directa con bimbo Diligenciar el formato de asociación, Adjuntar fotocopia de la cédula de ciudadanía, Diligenciar la ficha de actualización de datos Juntos Aportes y ahorro permanentes dan base para la aprobación del cupo para créditos. Están afectados desde su origen a favor de Febimbo, como Garantía de las obligaciones que el Asociado contraiga con Febimbo.

Líneas de consumo: Líneas de crédito con intereses desde el 0.5%.

- Libre inversión.
- Suministros.
- Mercancías.
- Vehículo.

Beneficios: Constituyen una serie de servicios sin costo alguno, a los cuales el asociado tiene derecho por pertenecer a Febimbo.

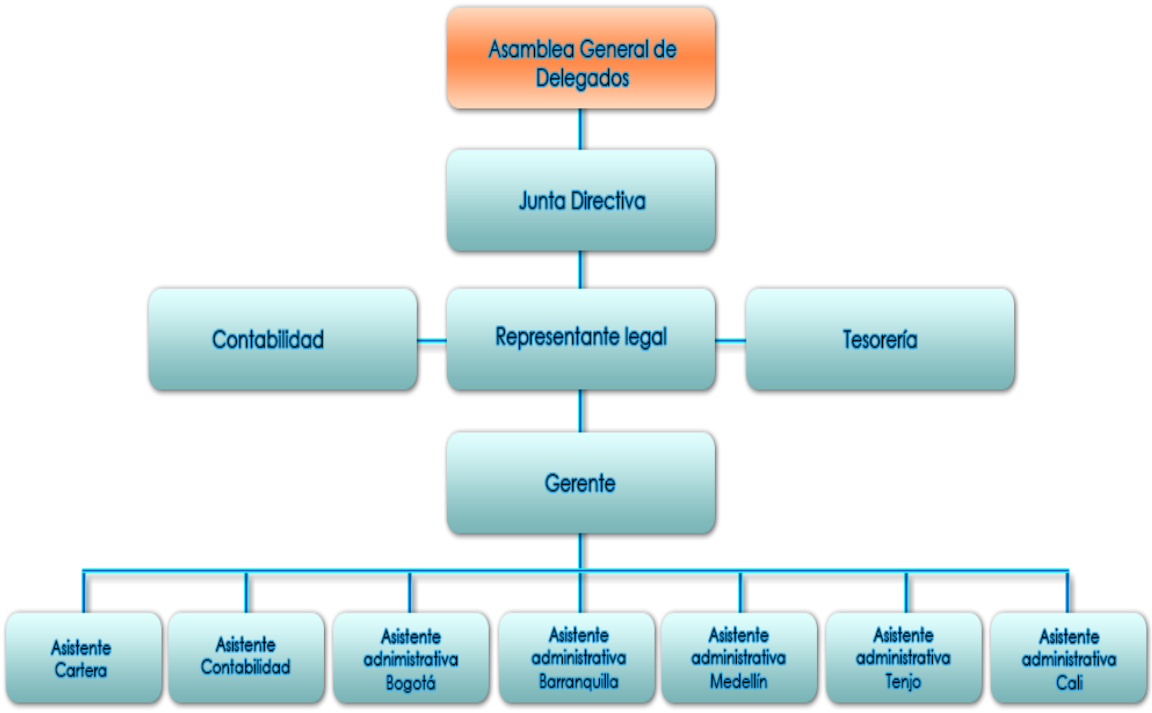
- Auxilio de nacimiento.
- Auxilio por salud.
- Auxilio por calamidad.
- Póliza de cartera, cubre el saldo de los créditos que tenga el asociado en el momento de su fallecimiento.
- Campañas de capacitación para los asociados.
- Campañas de salud.
- Eventos en fechas comerciales, cumpleaños de los asociados, Halloween, navidad, ferias de tecnología y del hogar.

[25] Servicios. (s. f.). https://www.febimbo.com/servicio.html

Líneas Sociales: Líneas de crédito con intereses desde el 0.5%.

- Educación.
- Salud y familia.
- Calamidad doméstica.
- Mejora vivienda.
- Apoyo a microempresarios.

Figura 5 - Organigrama FEBIMBO



Fuente: FEBIMBO

4.5 MARCO LEGAL

La implementación de las tecnologías de la información y medios de comunicación han traído diversos dividendos en las operaciones de las empresas, no obstante, han desarrollado problemas de seguridad donde la información es el activo más quebrantado o violado, ya que estas actividades son generadas por hackers o ladrones informáticos.

Por esto se ha implementado leyes y normas en seguridad para ofrecer un soporte jurídico a las organizaciones las cuales se describen a continuación.

Ley 1266: "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones."[26]

Ley 1273: "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."[27]

Ley 527: "por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."[28]

Ley Estatutaria 1581 De 2012: "La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones 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; así como el derecho a la información consagrado en el artículo 20 de la misma."[29]

[26] Ley 1266 de 2008 - Gestor Normativo. (2021, 5 noviembre). Función Publica. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

[27] Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (s. f.). http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[28] Ley 527 de 1999 - Gestor Normativo. (2021, 19 mayo). Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4276

[29] Ley Habeas Data - Protección de Datos | Asoenergia. (s. f.). https://asoenergia.com/es/node/119

5 DISEÑO METODOLÓGICO

Para llevar a cabo el proyecto, se aplicará las teorías de investigación, luego se utilizarán métodos cualitativos y cuantitativos, donde se validarán diferentes temas de la norma ISO / IEC 27001: 2013 y la metodología de riesgos, a través de diversos análisis de esta. Se integrará con datos cuantificados y tomados de aportes y soluciones de mejora.

De los enfoques cualitativos y cuantitativos se obtendrán datos que permitirá aclarar la importancia de resguardar la información y poder generar dinámicas óptimas, donde las operaciones realizadas tengan un alto grado de confianza en el procesamiento y almacenamiento de información.

El proyecto se desarrollará a través de períodos o etapas que apuntan a la consecución de objetivos específicos. Los cuales se verán a continuación:

Para la primera fase se analizará la situación actual del fondo de empleados de Febimbo, permitiendo conocer los procesos y trámites que allí se llevan a cabo, este análisis se realizará aplicando un riesgo metodología de gestión, que le permitirá comprender vulnerabilidades, amenazas y riesgos.

En la segunda fase se investigarán y clasificarán los activos de información a disposición del fondo de empleados de Febimbo, junto con esta actividad se conocerá el estado físico y funcional.

En la tercera fase se establecen los controles según la norma ISO / IEC 27001: 2013, necesarios para el diseño del sistema, esta se extrajo del diagnóstico realizado a través del análisis de los riesgos.

En la cuarta fase se diseñó la propuesta de políticas de seguridad, acorde a las necesidades de la empresa para mitigar los riesgos.

Adicional se utilizarán algunas técnicas para recolectar información como la entrevista, lista de chequeo, observación con las cuales se podrá realizar el proyecto.

6 DESARROLLO DE OBJETIVOS

6.1 OBJETIVO 1: CARACTERIZAR LA SITUACIÓN ACTUAL DEL FONDO DE EMPLEADOS FEBIMBO, LO QUE PERMITIRÁ CONOCER LOS PROCESOS Y PROCEDIMIENTOS QUE ALLÍ SE REALIZAN.

6.1.1 INTRODUCCIÓN

Aquí se conocerán los procesos y procedimientos que tiene el fondo de empelados Febimbo, su historia y servicios.

6.1.2 Área sistemas

6.1.2.1 Misión

El sector de IT tiene la tarea de aprovechar todas las iniciativas existentes y producir nuevas oportunidades que conduzcan al surgimiento del fondo de empleados Febimbo, todo esto a través de la implementación de tecnologías apropiadas que permita optimizar los procesos de IT en la organización.

6.1.2.2 Objetivos

- Proponer nuevas tecnologías en IT que ayuden a la organización a mejorar.
- Diseñar planes de mantenimiento preventivo y ofrecer un servicio de soporte técnico de calidad.

6.1.2.3 Estructura del área sistemas

Como tal el área de sistemas del fondo de empelados Febimbo es un tercero, el cual brinda todo lo relacionado a soporte y asistencia en el área de IT, y se acoge a los lineamientos que solicita el gerente o personal de la compañía.

6.1.3 Infraestructura IT

En la siguiente figura se mostrará como está la infraestructura tecnológica que dispone el fondo de empleados Febimbo.

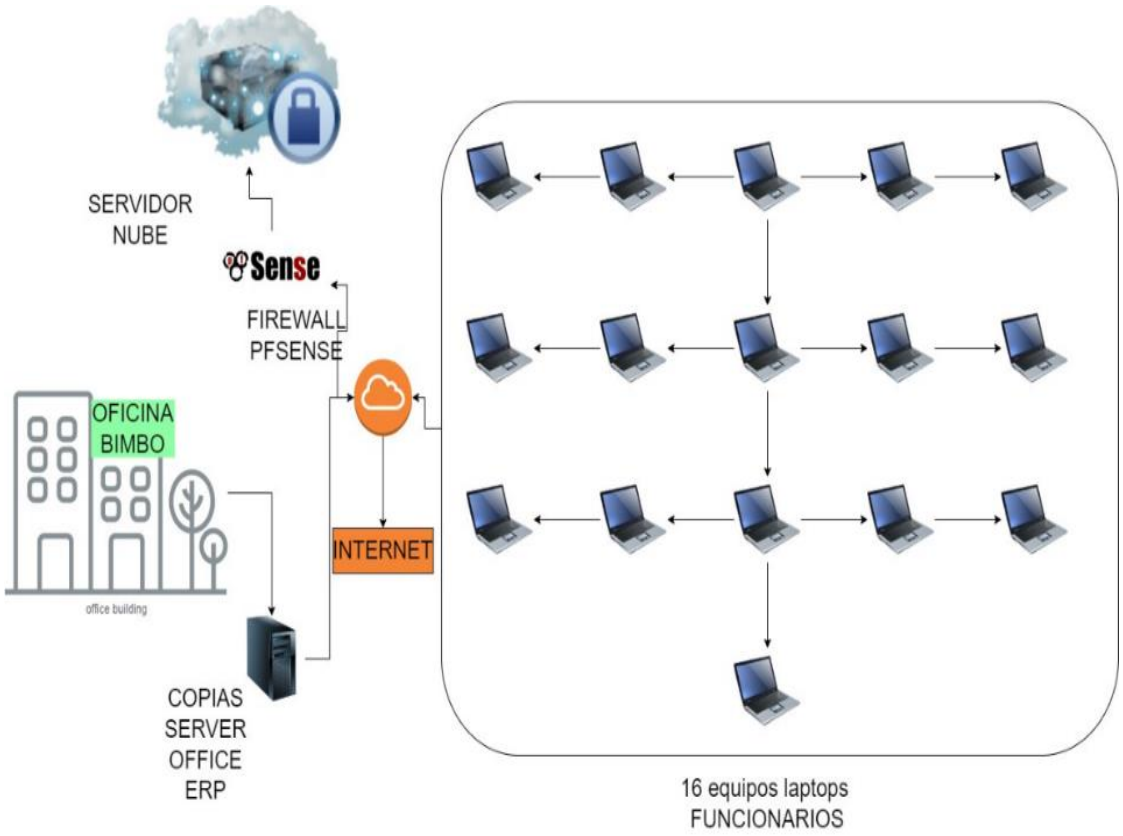
Se tienen varias sedes en Colombia, Bogotá centro, Sur y norte, se tienen en Tenjo, Cali, Medellín, Barranquilla, todos están trabajando con sus portátiles en la red de Bimbo y en casa, no se tiene infraestructura de redes, ya que aquí funciona el fondo de empleados de BIMBO y no es posible agregar nada en sus sedes, con temas de redes ni enlaces, por ende cada empleado tiene su portátil, se conectan a internet, se tiene un servidor en la nube, con el cual para ingresar primero se debe conectar a una VPN ((Virtual Private Network) crea una

conexión segura entre el usuario e internet. Ofrece una capa adicional de privacidad y anonimato para que puedas:) está VPN en un servidor y utiliza la aplicación PFSENSE para administrarlo y luego el servidor en la nube, luego se tiene el programa SAPIENS que es todo el ERP de la organización, el cual se valida y se desarrolla todo lo del fondo.

Todo el tema de información y archivos se administra en OneDrive con el paquete de Office 365 para empresas, se tiene antivirus licenciado y bloqueo de puertos USB (Un dispositivo USB, también conocido como dispositivo flash o dispositivo de memoria, es un dispositivo pequeño y portátil que se conecta al puerto USB de su computadora. Los dispositivos USB se utilizan comúnmente para almacenamiento, respaldo de datos y transferencia de archivos entre dispositivos) para que los empleados no puedan filtrar información de los equipos, también se usa BitLocker para asegurar la información, adicional otros temas de seguridad implementados.

Por eso en la Figura 6 se evidencia cómo se conectan los 16 equipos a la infraestructura que se conectan a internet, luego se conectan a una VPN que es una IP en el servidor virtual y luego el PFSENSE valida que el usuario este permitido y ya tendría acceso al programa Sapiens.

Figura 6 - Infraestructura IT



Fuente: Febimbo

6.1.3.1 Política del uso internet

La conexión a la red de internet en las oficinas es provista a los usuarios de Febimbo exclusivamente para las ocupaciones en relación con las necesidades del cargo y funcionalidades desempeñadas, por temas de enfermedad pandémica cada cliente tiene el internet de su hogar y móvil y tienen la posibilidad de tener el mismo cuidado y responsabilidad que en la oficina.
Los usuarios del servicio de navegación en Internet, al admitir el servicio permanecen asumiendo que:

- Los usuarios serán sujetos a monitoreo en sus equipos portátiles, ya que se debe utilizar el equipo y dispositivos para solo temas laborales, adicional no pueden ingresar a páginas no autorizadas.
- No se puede descargar ni instalar programas sin autorización.
- El uso de Internet tanto en la oficina y en la casa, es responsabilidad de cada usuario.
- El papel de IT está facultado para bloquear todos esos sitios de Internet que considere que no son compatibles con las tareas.
- En caso de existir excepciones por razones debidamente justificadas, tendrá que exponer la solicitud por medio de correo al gerente del Fondo de empleados Febimbo con copia al encargado de IT, exponiendo las razones para su análisis y aceptación.
- Se prohíbe ingresar a páginas XXX, bajar videos o música o participar en juegos de entretenimiento online.
- No usar los servicios de radio y TV por medio de Internet.
- No ingresar a páginas de redes sociales a lo largo de la jornada laboral.
- La descarga de archivos de internet debería ser con fines laborales y de manera razonable para no perturbar la banda ancha del Internet.

6.1.4 Sistemas de información

6.1.4.1 SAPIENS

Sapiens software flexible adaptado a las normas internacionales, facturación electrónica y demás normas legales vigentes. Software para el Sector solidario, colegios y sector empresarial, módulos totalmente integrados.

Principales Módulos de SAPIENS

- Documentos
- Contabilidad
- Cuentas por cobrar
- Cuentas por pagar
- Nomina
- Parafiscales
- Planillas
- Pagos magnéticos

6.1.5 Procesos que se tienen actualmente

Se tienen varios procesos internos los cuales se verán a continuación.

Aquí se garantizará que los proceso en Febimbo sirvan como facilitadores tecnológicos en el área de IT, cumpliendo las normas y políticas actuales.

En la tabla 1, se mostrará como es el proceso y procedimiento interno de gestión de usuarios desde el área de IT para la empresa FEBIMBO.

Tabla 1 - Proceso Interno de gestión usuarios

TAREA	EXPLICACION	RESPONSABLE	REGISTRO	FORMATO
Informar la creación, modificación o retiro de usuario	Validar el requerimiento o solicitud al área de IT, para la creación, retiro o modificación de usuarios.	GERENTE O RRHH	EMAIL	N/A
Crear EMAIL y cuentas asociadas	Crear la cuenta de email, con primer nombre y apellido o como lo disponga la gerencia Ejemplo: samuel. bartolito Las cuentas asociadas al nuevo usuario son: - Usuario VPN - Usuario Office - Usuario servidor NUBE - Usuario escritorio remoto - Usuario Sapiens - Usuario portátil	Área IT	EMAIL	N/A
Retirar usuarios	Recibir información de inactividad o retiro de empleados	GERENTE O RRHH	EMAIL	N/A

Fuente: FEBIMBO

En la tabla 2, se mostrará como se realiza el proceso y procedimiento de incidencias reportadas al área de IT para la empresa FEBIMBO.

Tabla 2 - Proceso gestión incidentes

TAREA	EXPLICACION	RESPONSABLE	REGISTRO	FORMATO
Informar incidencia	Usuarios informan al área de sistemas la incidencia	EMPLEADOS FEBIMBO	EMAIL, LLAMADA, WHATSAPP	OS-IT-001 Solicitud soporte técnico
Registrar incidencia	Registrar incidencia en el seguimiento de tiques	Área IT	EMAIL, LLAMADA, WHATSAPP	CI-IT-001 Seguimiento de tiques
Analizar incidencia	Realizar análisis de la incidencia	Área IT	N/A	N/A
Diagnostico incidencia	Realizar diagnóstico de la incidencia	Área IT	N/A	N/A
Solucionar incidencia	Solucionar la incidencia	Área IT	N/A	N/A

Fuente: Febimbo

Adicionalmente se mostrará como se realiza el proceso y procedimiento, para ejecutar el cronograma de mantenimiento de equipos 2 veces al año, esto suele suceder de junio a agosto o de enero a marzo, así para cumplir el proceso.

En la siguiente tabla 3, se mostrará como se programa el mantenimiento de equipos de IT.

Tabla 3 - Proceso mantenimiento equipos

TAREA	EXPLICACION	RESPONSABLE	REGISTRO	FORMATO
Elaborar cronograma mantenimientos	Elaborar cronograma de mantenimientos 2 veces al año	Área IT	Excel	N/A
Programar mantenimiento	Programar mantenimiento por correo agendando citas	Área IT	EMAIL	CM-IT-001 Cronograma mantenimiento
Ejecutar mantenimiento	Ejecutar mantenimiento	Área IT	N/A	N/A
Llenar formato mantenimiento	Llenar formato de mantenimiento y firma por el empleado y área de IT	Área IT	N/A	FSM-IT-001 Formato de Software y Mantenimiento

Fuente: FEBIMBO

6.2 OBJETIVO 2: IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN QUE EXISTEN EN EL FONDO DE EMPLEADOS FEBIMBO, PARA REVISAR LOS TEMAS APLICABLES PARA EL DISEÑO DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN.

6.2.1 Desarrollo del proyecto

Para el desarrollo de este proyecto se cuenta con el apoyo de la gerencia, los cuales actúan en conjunto con los diferentes niveles de la empresa, para la autorización y desarrollo efectivo de cada uno de los objetivos propuestos en este proyecto.

6.2.2 Alcance del proyecto

Para el desarrollo y cumplimiento de este proyecto se llevarán a cabo las siguientes actividades:

- Conceptualizar los activos de información que se tienen presentes en la Cooperativa y plantear medidas para su protección, bajo la norma ISO 27001 de 2013.
- Identificar vulnerabilidades, amenazas y los riesgos a los que están expuestos los activos de información y que puedan afectar la continuidad del negocio.
- Establecer controles necesarios que puedan garantizar la disponibilidad y confidencialidad de la información.
- Realizar el inventario de activos de información con los que cuenta la empresa.

6.2.3 Análisis del riesgo

El desarrollo del plan se basó en la metodología MAGERIT, la cual se convirtió en uno de los instrumentos primordiales para evaluar los peligros y amenazas que vulneren la seguridad, disponibilidad y confidencialidad de los activos de información. Para proteger la información de los riesgos y amenazas, se realiza un inventario de activos de información teniendo en cuenta la metodología entes mencionada, la cual está diseñada para cualquier empresa, sin importar su actividad económica; partiendo de esta, se realizaron las siguientes actividades:

- Identificación de activos de información con sus amenazas y vulnerabilidades.
- Determinar cada uno de los controles de seguridad.
- Valoración de a impacto y riesgo.

Para el desarrollo del proyecto y con el fin de determinar la metodología, se realiza un estudio comparativo entre las más representativas, entre las que se encuentran las siguientes:

- OCTAVE
- MAGERIT
- MEHARI

En la siguiente tabla 4 se evidencia un cuadro comparativo de metodologías y normas.

Tabla 4 - Cuadro comparativo de metodologías y normas

Metodología	Características	Conceptos	Fases	Ventajas	Desventajas
OCTAVE	Fue desarrollada en EE. UU., fue creada para recolectar y analizar información con el fin de desarrollar una estrategia de protección y mitigación de riesgos, basados en los riesgos operacionales de seguridad organizacional.	Construcción de perfiles de amenazas, basados en los activos. Identificación de infraestructura y vulnerabilidades. Desarrollo de estrategias de seguridad. Desarrollo de planes.	Visón de la organización. Visón de tecnología. Planificación de medidas y reducción de riesgos.	Es una metodología autodirigida. Comprende los procesos y análisis de gestión del riesgo. Se considera de las más completas.	No toma la cuenta el repudio de la información como principal objetivo de seguridad. Usa muchos documentos anexos para el análisis de los riesgos. Requiere de profundos conocimientos técnicos.
MAGERIT	Creado por el Consejo Superior de Administración Electrónica de España. Está orientada a los sistemas de información. Está enfocada e a los siguiente s objetivos: Sistematizar y analizar riesgos.	Escalas de valores cualitativos y cuantitativo. Indisponibilidad dad del servicio. Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia.	Análisis de riesgos. Caracterización de las amenazas. Caracterización de las salvaguardas.	Se le considera con un alcance completo, tanto en el análisis como en la gestión de riesgos. Posee un extenso archivo de inventarios en lo referente a Recursos de Información, amenazas y tipo de Activos.	El hecho de tener que traducir de forma directa todas las valoraciones en valores económicos hace que la aplicación de esta metodología sea realmente costosa. No involucra a los procesos, recursos ni

	Descubrir y planificar medidas para controlar los riesgos .			Permite un análisis completo cualitativo y cuantitativo.	vulnerabilidades como elementos del modelo a seguir.
MEHARI	Método para la evaluación y gestión de riesgos según requerimientos de ISO/IEC 27005:2008. Comprende bases de datos de conocimiento, con manuales y guías que describen los diferentes módulos (amenazas, riesgos, vulnerabilidades).	Diagnóstico De Seguridad. Análisis de Los Intereses Implicados por la Seguridad.	Establecimiento del contexto Tipología y lista de activos principales. Análisis de activos. Daños potenciales lista de posibles escenarios de riesgos. Análisis de amenazas eventos de iniciación, actores, condiciones específicas	Usa un modelo de análisis de riesgos cualitativo y cuantitativo.	Sólo toma en cuenta los principios de confidencialidad, integridad y disponibilidad de la información como objetivos de seguridad. La recomendación de los controles no la incluye dentro del análisis de riesgos sino en la gestión de los riesgos.

Fuente: PMG

Con base en la comparación que se realizó anteriormente, se decidió utilizar la metodología MAGERIT bajo las comparaciones previas que resaltaron la calidad de cada método en el desarrollo del proyecto.

Otro de los puntos claves por los cueles se decide escoger la metodología MAGERIT, es que dispone de tablas de frecuencia para el análisis cualitativo y cuantitativo.

La metodología MAGERIT está ajustada al estándar ISO/IEC 27001:2013 para garantizar que se generen controles en una variedad de activos identificados con altos niveles de riesgo una vez que se completa el análisis de riesgo.

6.1.3 Análisis y gestión del riesgo

Con base en la metodología MAGERIT se llevan a cabo las fases anteriores y se consiguen los objetivos propuestos para el desarrollo de este proyecto.

6.1.4 Activos de información

Durante el desarrollo del proyecto se identificaron activos estrechamente relacionados con los datos procesados, almacenados y de salida que podrían ser utilizados por la cooperativa. Los activos se observan directamente como datos relevantes en el sistema contable de la empresa Febimbo.

La clasificación de los activos de información se realiza de acuerdo con las sugerencias de la metodología MAGERIT. La metodología MAGERIT propone identificar cada activo de información para su posterior análisis mediante una nomenclatura.

La Tabla 5 se evidencia la clasificación de los activos de información por tipos de activos.

Tabla 5 - Tipos de activos

Nomenclatura	**Nombre**
[D]	Datos
[S]	Servicios
[SW]	Software de aplicaciones
[HW]	Hardware
[COM]	Redes de comunicación
[MEDIA]	Soportes de información
[L]	Instalaciones
[P]	Personal

Fuente: Propia

Los activos de información que forman parte del análisis interactúan con los procesos considerados de afiliación, crédito financiero, ingreso de fondos, afiliación y gestión técnica, por ser las actividades primordiales de cumplimiento de la misión dentro de la organización. Además de los servicios principales para los empleados de Febimbo, por lo tanto, proteger el buen funcionamiento de los activos en las áreas de secretaría, cartera, contabilidad, finanzas y sistemas donde se realizan los procesos anteriores es fundamental para la calidad del servicio.

Cada uno de los activos de información de Febimbo se encuentra dentro del grupo correspondiente según sea su función, logrando así que cada activo de información cuente con una nomenclatura, la cual es especifica por la metodología MAGERIT.

Para nombrar los activos de información, se relacionan los activos con los que cuenta la empresa, en la siguiente tabla 6 se evidencia.

Tabla 6 - Identificación de activos

COD	Nombre	Nomenclatura	Descripción	Cantidad
[D]	Datos	[BD]	Base de datos en la nube.	1
		[Files]	Archivo general histórico de gestión administrativa, políticas, acuerdos, actas.	1
		[Int]	Archivo principal de información asociados, proveedores, convenios, comunicados, circulares.	1
[S]	Servicios	[Www]	Navegación - Internet.	1
		[File]	Almacenamiento en la nube de BD.	1
		[Servimp]	Impresión y scanner en red.	1
		[Sub]	Sapiens	1
		[Dbms]	Sistema gestión BD en la nube.	1

[Sw]	Software Aplicaciones	[Office]	Office 365	16
		[Os]	Windows 10 Pro	14
		[Browser]	Google Chrome	NA
[Media]	Soportes de información	[disk]	Disco Externo	2
		[san]	Almacenamiento En Red	1
		[USB]	Almacenamiento Externo Baja Capacidad	1
[L]	Instalaciones	[Infra]	Planta Física Febimbo	1
[P]	Personal	[ui]	Personal Interno Administrativos.	15
		[ue]	Personal Externo (IT)	3

Fuente: Propia

6.1.4 Valoración de Activos de Información

Para realizar la valoración de los activos de información de Febimbo se utilizan algunas medidas cualitativas, la cuales permiten realizar cálculos matemáticos simples, los cuales generan un valor que mide la criticidad de los activos de información en el cumplimiento de los objetivos de la organización.

En la siguiente tabla 7, se evidencia la valoración de los activos.

Tabla 7 - Valoración de Activos

Calificación		**Definiciones**
Muy alto	=10	Indispensable mantener la confidencialidad, integridad, disponibilidad del activo de información.
Alto	> 8 <10	Conservar la confidencialidad, integridad y disponibilidad del activo.
Medio	>3 y <5	Es transcendental mantener la confidencialidad, integridad o disponibilidad del activo.
Bajo	>0 y <2	Se debe Mantener la confidencialidad, integridad y disponibilidad del activo en la medida de lo posible.
Muy Bajo	=0	No es necesario mantener la confidencialidad, integridad y disponibilidad del activo de información.

Fuente: Propia

En la valoración que se evidencia en la tabla 8, se aplicaran dimensiones asociadas a cada uno de los activos de información de la empresa, que son los siguientes:

- [D] disponibilidad
- [I] integridad
- [C] confidencialidad
- [A] autenticidad
- [T] trazabilidad

Con el fin de realizar la valoración de cada uno de los activos y dependiendo de sus diferentes dimensiones se deben realizar algunas preguntas para abordar las dimensiones a evaluar cómo se evidencia en la tabla 8.

Tabla 8 - Preguntas para valorar las dimensiones

Dimensiones	Pregunta	Descripción
Disponibilidad [D]	¿Qué puede pasar si el activo de información no se encuentra disponible?	Tendrá un valor **MUY ALTO** ya que afectaría considerablemente la continuidad de la de las actividades de la empresa.
Integridad [I]	¿Qué relevancia tiene el activo si es alterado?	Podría tener un valor MUY **ALTO** si al modificarlo afecta el funcionamiento de la empresa, o si al modificarlo o alterarlo no afecta el funcionamiento de la empresa; tendría un valor **BAJO**.
Confidencialidad [C]	¿Qué relevancia tendría el activo de información si es conocido o manipulado por personal no autorizado o externo a la empresa?	Al exponer el activo de información públicamente, podría tener un valor **MUY ALTO**, ya que afectaría notoriamente la funcionalidad de la empresa.
Autenticidad [A]	¿Qué consecuencias traería para la empresa si no es controlado el acceso al activo?	Si no se puede controlar el acceso al activo de información, podría tener un valor **MUY ALTO**, ya que afectaría notoriamente el funcionamiento de la empresa.
Trazabilidad [T]	¿Como afectaría el funcionamiento de la empresa si el activo de información no cuenta con constancia de uso?	Tendría un valor muy alto si no existe constancia de uso y no se pueda controlar

Fuente: Propia

Teniendo la escala sobre la cual se trabajará para determinar el valor de los activos de información de la empresa, se procede a realizar el análisis cualitativo y cuantitativo, como se evidencia en la tabla 9.

Tabla 9 - Valoración de activos por dimensión

Nombre del activo	Nomenclatura del activo	Descripción	Cantidad	Valor cualitativo	Valor cuantitativo
Datos	[BD]	Base de datos en la nube	1	10	Muy alto
	[Files]	Archivo general histórico de gestión administrativa, políticas, acuerdos, actas.	1	10	Muy alto
	[Int]	Archivo principal de información asociados, proveedores, convenios, comunicados, circulares.	1	10	Muy alto
Servicios	[Www]	Navegación -Internet	1	10	Muy alto
	[File]	Almacenamiento en la nube de BD	1	10	Muy alto
	[Servimp]	Impresión y scanner en red	1	2	Bajo
Software de aplicaciones	[Sub]	Sapiens	1	10	Muy alto
	[Dbms]	Sistema gestión BD en la nube	1	10	Muy alto
	[Office]	OFFICE 365	16	8	Muy alto
	[Os]	WINDOWS 10 PRO	14	10	Muy alto
	[Browser]	Google Chrome	1	8	Alto
Soportes de información	[disk]	Disco externo	2	8	Alto
	[san]	Almacenamiento en red	1	8	Alto
	[USB]	almacenamiento externo baja capacidad	1	5	Medio
Instalaciones	[Infra]	Planta física FEBIMBO	1	10	Muy alto
Personal	[ui]	Personal interno administrativos	15	8	Alto
	[ue]	Personal externo (IT)	3	8	Alto

Fuente: Propia

6.3 PROPONER LOS CONTROLES PRINCIPALES SEGÚN LA NORMA ISO 27001:2013 PARA GARANTIZAR LA DISPONIBILIDAD E INTEGRIDAD DE LA INFORMACIÓN.

6.3.1 Plan de tratamiento de riesgos

Con la información recolectada se definió y evaluó cada uno de los activos de información sobre los que existen amenazas y riesgos potenciales.

Con este análisis se generaron controles con el fin de optimizar el impacto para cada uno de los activos de información donde el nivel de riesgo es muy alto, dichos controles están relacionados en la norma ISO 27001 en su versión 2013 y alineados con la guía de buenas prácticas ISO/IEC 27002:2013.

Eliminar: bajo este tratamiento se quiere eliminar totalmente el impacto, esto puede darse ya sea eliminando el activo o procesos que generar un alto grado de riesgo.

Reducir: son medidas basadas en actividades técnicas u organizativas que permiten mitigar el riesgo, entre estas los planes de contingencia, adquisición de elementos para reforzar la protección a los activos etc.

Asumir: no habrá medidas frente a un riesgo, esto será aplicable teniendo en cuenta que el activo no sufra degradación considerable que pueda afectar la continuidad del negocio.

En la siguiente tabla 10, se muestra cómo está el nivel de riesgo.

Tabla 10 - Nivel del riesgo

Nivel del riesgo	
10-20	10-20
8-10	8-10
3-7	3-7
1-2	1-2

Fuente: Propia

En la tabla 11, se evidencia un plan de tratamiento de riesgo para cada uno de los activos de información de Febimbo con mayor riesgo.

Tabla 11 - Tabla matriz de valoración riesgo cualitativamente

Nombre Del Activo De Información	**Amenazas**	**Vulnerabilidades**	**Valor Del Riesgo**	**Tratamiento Del Riesgo**	**Control Según La Norma ISO 27002**
Base De Datos En La Nube	[A.25] Robo De Información	Claves De Acceso Inseguras	Muy Alto	Verificar Las Políticas De Seguridad De Información.	Tratamiento Del Riesgo De Acuerdo Con Las Políticas De Seguridad De La Información.
Archivo Principal De Información Asociados, Proveedores, Convenios, Comunicados, Circulares Políticas, Actas, Acuerdos.	[N.1] Fuego	Insistencia De Elementos Que Controlen La Temperatura Al Interior De La Bodega Donde Se Almacena La Documentación	Muy Alto	Generar Medidas Con El Fin De Identificar Posibles Incendios, Como Alarmas De Detención De Humo	Protección Contra Amenazas Externas Y Ambientales
Navegación Internet	[I.8] Fallas En El Servicio De Internet	No Existe Un Prestador De Servicio Alterno	Muy Alto	Se Debe De GENERAL UN Plan De Contingencia Ante Una Eventual Caída Del Servicio	Planeación De Continuidad De La Seguridad De La Información
	[I.6] Corte Del Suministro Eléctrico	No Se Cuenta Con Un Respaldo De Energía En Caso De Fallas	Alto	Adaptar Un Sistema Eléctrico De Acuerdo Con Las Necesidades De La Entidad	Instalaciones De Suministros
Almacenamiento En La Nube De BD Impresión Y Scanner En Red	[I.9] Interrupción De Servicios Y/O Suministros	Carencia De Monitorización De Los Servicios Prestados Por El Proveedor	Alto	Contar Con Mecanismos De Comunicación De Peticiones, Quejas Y Reclamos Para Resolver	Supervisión Y Revisión De Los Servicios Prestados Por Los Proveedores

				Una Eventual Caída De Los Servicios.	
	[A.7] Uso No Previsto	Falta De Políticas Para El Uso De Escáner E Impresoras	Medio	Generar Políticas Que Regulen El Uso Eficiente Del Activo	Uso Aceptable De Los Activos
Sapiens	[I.8] Fallas En El Servicio	No Hay Monitoreo Del Servicio	Alto	Realizar Pruebas Que Permitan Identificar Vulnerabilidades	Gestión De Vulnerabilidades
OFFICE 365	[E.21] Error De Mantenimiento O Actualización De Software	No Se Cuenta Con Soportes De Los Mantenimientos Realizados Al Software	Medio	Definir Necesidades Para Actualizaciones	Instalación De Software En Sistemas De Producción
WINDOWS 10 PRO	A.22] Manipulación De Programas	No Se Cuenta Con Políticas Y Perfiles Para Acceder Al Sistema	Alto	Implementar La Política Para El Control De Acceso	Política De Control De Acceso
Google Chrome	[E.20] Vulnerabilidades De Los Programas	Software Obsoletos	Medio	Definición De Necesidades Para La Actualización De Paquetes De Software	Instalación De Software En Sistemas De Producción
Disco Externo	[A.25] Robo De Información	Falta De Políticas Para El USO DE Los Activos De Información	Alto	Generar Políticas Para La Regulación Del Uso Eficiente Del Activo	Uso Aceptable De Los Equipos
Personal Interno Administrativos	[E.1] Errores De Los Usuarios	Desconocimiento De Las Políticas De Seguridad De	Medio	Es Necesario Que Cada Una De Las Políticas Que Se Implementen Sean Conocidas Y Socializadas Con Todo El Personal	Educación, Capacitación En Seguridad De La Información

Fuente: Propia

6.3.2 Cumplimiento Norma ISO/IEC 27001:2013.

Con base en el análisis de riesgos se continúa revisando con relación a la implementación de la norma ISO/IEC 27001, con que cuentan los procesos de afiliación, crédito, financiero, ingreso de fondos, afiliaciones y gestión tecnológica de las áreas de secretaría, cartera, tesorería y sistemas respectivamente; para obtener dicho análisis se generó la matriz de aplicabilidad mediante el uso del anexo A de la Norma ISO/IEC 27001:2013 donde se especifica si cumple o no con los controles de los diferentes dominios de la norma.

A continuación, se registra el nivel de cumplimiento de los diferentes controles según la norma ISO/IEC 27001:2013, mediante una respuesta que puede ser SI o NO de acuerdo con si se cumple con dicho control; el dominio 6, Aspectos Organizativos, se tiene la siguiente tabla 12.

Tabla 12 - Nivel de cumplimiento

Controles				Cumple		%
Dominio	Control	Descripción del control	Pregunta	SI	No	cumplimiento
Política de seguridad	Política de seguridad de la información	Se debe crear una política de seguridad de la información, aprobada por la dirección, publicada y socializada con todos sus empleados	¿FEBIMBO cuenta con una política de seguridad de la información, documentada e implementada?	x		80%
	Actualización de las políticas de seguridad de la información	Las políticas de seguridad de la información se deben de actualizar mínimo una vez al año o antes si ocurren cambios significativos dentro de la empresa	¿se realiza revisión periódica de las políticas de seguridad de la información?	x		
	Investigación de antecedentes disciplinarios	Se deberían realizar revisiones de los antecedentes disciplinarios de cada una de las	¿se realiza verificación de antecedentes disciplinarios de los empleados?	x		90%

Seguridad de los recursos humanos		personas que ingresan a la empresa				
	Términos y condiciones	Como parte del proceso de contratación y las obligaciones contractuales los empleados deberán firmar y aceptar términos y condiciones estipulados en cada uno de los contratos por la empresa FEBIMBO, en los que se establecen términos y condiciones de ambas partes esto con el fin de proteger la seguridad en la información	¿En cada uno de los contratos celebrados entre ambas partes se determinan las obligaciones del trabajo, así como también las de seguridad de la información?	x		
Gestión de activos	Realizar inventario de activos de información con los que cuenta la empresa	Cada uno de los activos de información se deben inventariar y clasificar según su criticidad	¿Los activos de información se encuentran inventariados y clasificados?		x	80%
	Uso de los activos de información	Se debe documentar e implementar las regulaciones necesarias para el buen uso de los activos de información	¿Se tienen normas estipuladas para el uso adecuado de los activos de información?		x	
	Entrega de los activos de información asignados para el cumplimiento de las actividades	Todo el personal contratado por FEBIMBO, deben devolver las óptimas condiciones los activos de	¿una vez finalizado el contrato laboral, el empleado hace entrega de los activos de información?		x	

		información asignados durante la ejecución del contrato				
Control de acceso	Política de control de acceso	Se debe documentar y divulgar una política para el control de acceso, basados en las necesidades de la seguridad de la empresa y los activos de información	¿se cuenta con una política para el control de acceso a los activos de información de FEBIMBO	x		100%
		Se debería proveer a los usuarios de los accesos a redes y los servicios de red para los que han sido expresamente autorizados a utilizar.	¿se restringe el acceso o a las redes y servicios a los cuales no están autorizado el ingreso?	x		
	Gestión de información confidencial de autenticación de usuarios	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlada	¿Se garantiza que se mantiene la confidencialidad de la información de acceso?	x		
	Retiro de accesos	Se deben de retira los derechos de acceso, todos los empleados que hayan finalizado su contrato laboral.	¿Se retiran los accesos al momento de finalizar el contrato laboral?	x		
	Doble autenticación	Se debe de realizar la activación de	¿Se cuenta con doble autenticación			

		doble autenticación para el control de acceso de los usuarios a las cuentas de: Office 365	en cada uno de los usuarios?			
	Gestión de contraseñas de los usuarios	Las contraseñas de accesos de los usuarios deben de ser seguras y de calidad	¿las contraseñas son fuertes y robustas?	x		
Seguridad física y ambiental	Control de acceso físico	Los accesos a las instalaciones de la empresa,	¿se cuenta con controles para evitar el acceso	x		98%
		debe de estar protegida mediante controles de acceso, con el fin de garantizar el acceso solo al personal autorizado	de personas no autorizadas?			
	Seguridad en el cableado	Los cables eléctricos deben de estar protegidos contra posibles daños	¿se protege adecuadamente el cableado eléctrico?	x		
	Seguridad en los equipos	Debería de realizarse mantenimiento preventivo y correctivo de los equipos mínimo 2 veces al año	¿todos los equipos reciben mantenimiento preventivo y correctivo dos veces al año, de acuerdo con el plan de mantenimiento?	x		
	Retiro de activos fuera de las instalaciones de la empresa	Los equipos y/o activos de información no deberían retirarse de la empresa sin previa autorización de la alta gerencia	¿Se cuenta con un control para el retiro del activo de información fuera de la empresa?	x		

	Política de puesto de trabajo despejado y bloqueo de pantalla de los equipos en desuso	Se debe adoptar una política de puesto de trabajo limpio y política de bloqueo de equipos que no se estén utilizando	¿Se cuenta con política de escritorio limpio y pantallas apagadas?		x	
Seguridad operativa	Gestión de cambios	Se deben controlar los cambios que afectan a la seguridad de la información, procesos de negocio, las instalaciones y sistemas de procesamiento de información.	¿Ante un eventual cambio sobre los activos se genera controles?		x	70%
	Gestión de capacidades	Monitorear y ajustar el uso de cada uno de los recursos y proyectar las necesidades requisitos y gestión de capacidades en el futuro	¿Se tienen documentado e implementado el plan de continuidad del negocio?	x		
	Protección contra código malicioso	Se deben implementar controles para detener y controlar y recuperar afecciones de programa maligno.	¿Se tienen implementado un sistema de detención contra códigos maliciosos?		x	
	Copias de seguridad	Se deben de realizar copias de seguridad de la información, de software, imágenes del sistema con relación a la política de	¿se cuenta con el sistema de copias de seguridad de la información?	x		

		respaldo de Backup				
	Registro de actividad	Se debe de proteger contra posibles alteraciones o accesos no autorizados a los sistemas de información	¿se cuenta con control de accesos para prevenir cambios o accesos no autorizados?	x		
	Gestión de vulnerabilidades s	Se debe de obtener información de las vulnerabilidades de los sistemas de información de manera oportuna, con el finde evaluar el grado de exposición y tomar las medidas necesarias	¿se realiza una identificación de vulnerabilidades de los sistemas de información?		x	
	Auditorías a los sistemas de información	Se deben de planificar y acodar requisitos y actividades de auditorías donde se involucren los sistemas de información con el objetivo de minimizar las interrupciones a los procesos de la empresa	¿se realizan auditorías a los sistemas de información?		x	
Seguridad operativa	Gestión de seguridad en las redes	Se deben de administrar y controlar los accesos a las redes con el fin de proteger la información en sistemas y aplicaciones	¿la empresa cuenta con un control y administración de la red?	x		85%
Adquisición, desarrollo y	Seguridad en los procesos	Se debe de establecer y	¿la empresa establece	x		90%

mantenimiento de los sistemas de información		aplicar reglas para el desarrollo de Software	normas para la seguridad de la información en el desarrollo de Software			
	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Las aplicaciones críticas con las que cuenta la empresa deberán ser revisadas con el fin de verificar que no se hay han efectuado impactos adversos en la seguridad de la empresa	¿la empresa revisa en buen funcionamiento en las aplicaciones después del cambio en los sistemas?	x		
	Pruebas de aceptación	Se deben de realizar pruebas para la aceptación de la implementación de nuevos sistemas de información y/o actualizaciones de nuevas versiones	Las nuevas versiones o actualizaciones de software están sujetas a un proceso de actualización	x		
Gestión de incidentes de seguridad d la información	Responsabilidades y procedimientos	Se deben de establecer responsabilidades y procedimientos de gestión con el finde garantizar una respuesta eficiente a los incidentes de seguridad de la información ocurridos dentro de la empresa	¿la empresa cuenta con un procedimiento ara la atención de incidentes de seguridad de la información?		x	50%
	Notificación de los eventos de seguridad de la información	Los eventos de seguridad de la información ocurridos deben de ser reportados lo antes posibles con el fin de	¿se reportan todos los incidentes de seguridad de la información ocurridos dentro de la empresa?	x		

		mitigar su impacto y tomar las medidas de prevención necesarias para evitar nuevos incidentes				
	Identificación de puntos débiles en temas de seguridad de la información	Se deben de realizar pruebas de Hacking Ethical con el fin de identificar puertos abiertos	¿se realizan pruebas de Hacking Ethical mínimo una vez al año?		x	
	Respuesta ante incidentes de seguridad	Se debe de responder oportunamente ante incidentes de seguridad de la información, con base en los procedimientos estipulados	¿se da respuesta y solución inmediata cuando se presentan incidentes de seguridad?	x		
	Aprendizaje o lecciones aprendidas de los incidentes de seguridad	De debe de utilizar el conocimiento adquirido durante el análisis de los incidentes de seguridad de la información para reducir el impacto de futuros incidentes	¿bajo la solución de incidentes de seguridad se generan procesos de aprendizaje para solución de futuros incidentes y mejoras en la seguridad?	x		
Continuidad del negocio	Planificación y continuidad de la seguridad de la información	La empresa debe de implementar lineamientos para la seguridad de la información y gestión durante situaciones adversas o crisis de desastres	¿Dentro del plan de continuidad del negocio se tienen integrado la política de seguridad de la información?		x	60%
	Implementación de la política de continuidad de la seguridad de la información	La empresa debe de documentar e implementar los procesos procedimiento y	¿se dispone de un plan con medidas para gestionar la continuidad de	x		

		controles para garantizar el mantenimiento de la seguridad de la información cuando se presenten situaciones adversas	la seguridad de la información dentro de la empresa?			
Cumplimiento	Identificación de decretos, leyes y normas aplicables	se debe de tener una matriz de requisitos legales aplicables a la empresa	¿e cuenta con una matriz de requisitos legales actualizada y ajustada a la empresa?		x	80%
	Protección de documentación de la empresa	Los soportes de documentación deberán de ser protegidos contra perdidas, incendios, robo de acuerdo con los requisitos legales	¿Se cuenta con controles necesarios para proteger los documentos según los requisitos legales?	x		
	Protección de datos y privacidad de la información	Se debe de garantizar la privacidad de la protección de la información personal de acuerdo con la legislación	¿se da cumplimiento a la legislación vigente en materia de protección de datos personales?	x		
	Cumplimiento de las políticas y normas de seguridad	La alta gerencia debe de revisar el cumplimiento de las políticas, normas, procesos y procedimientos dentro de la empresa	¿la alta gerencia revisa el cumplimiento de todas las políticas y normas de seguridad dentro de la empresa?	x		

Fuente: Propia

Durante la realización de la matriz de cumplimiento a los diferentes controles, se genera la siguiente tabla 13, la cual muestra el grado de cumplimiento en cada dominio, con base en la norma ISO/IEC 27001:2013.

Tabla 13 - Cumplimiento en cada uno de los dominios

Dominio	Calificación Actual	Calificación Objetiva
Política de seguridad	80%	100%
Seguridad de los recursos humanos	90%	100%
Gestión de activos	80%	100%
Control de acceso	100%	100%
Seguridad física y ambiental	98%	100%
Seguridad operativa	70%	100%
Adquisición, desarrollo y mantenimiento de los sistemas de información	90%	100%
Gestión de incidentes de seguridad d la información	50%	100%
Continuidad del negocio	60%	100%
Cumplimiento	80%	100%

Fuente: Propia

Con el fin de tener mejor comprensión del nivel de cumplimiento y la brecha que tiene en la actualidad Febimbo, con relación al nivel de cumplimiento en cada uno de sus dominios, se realiza la figura 7, en esta se encontrara el modelo MSPI ("El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital."[30]) propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones.

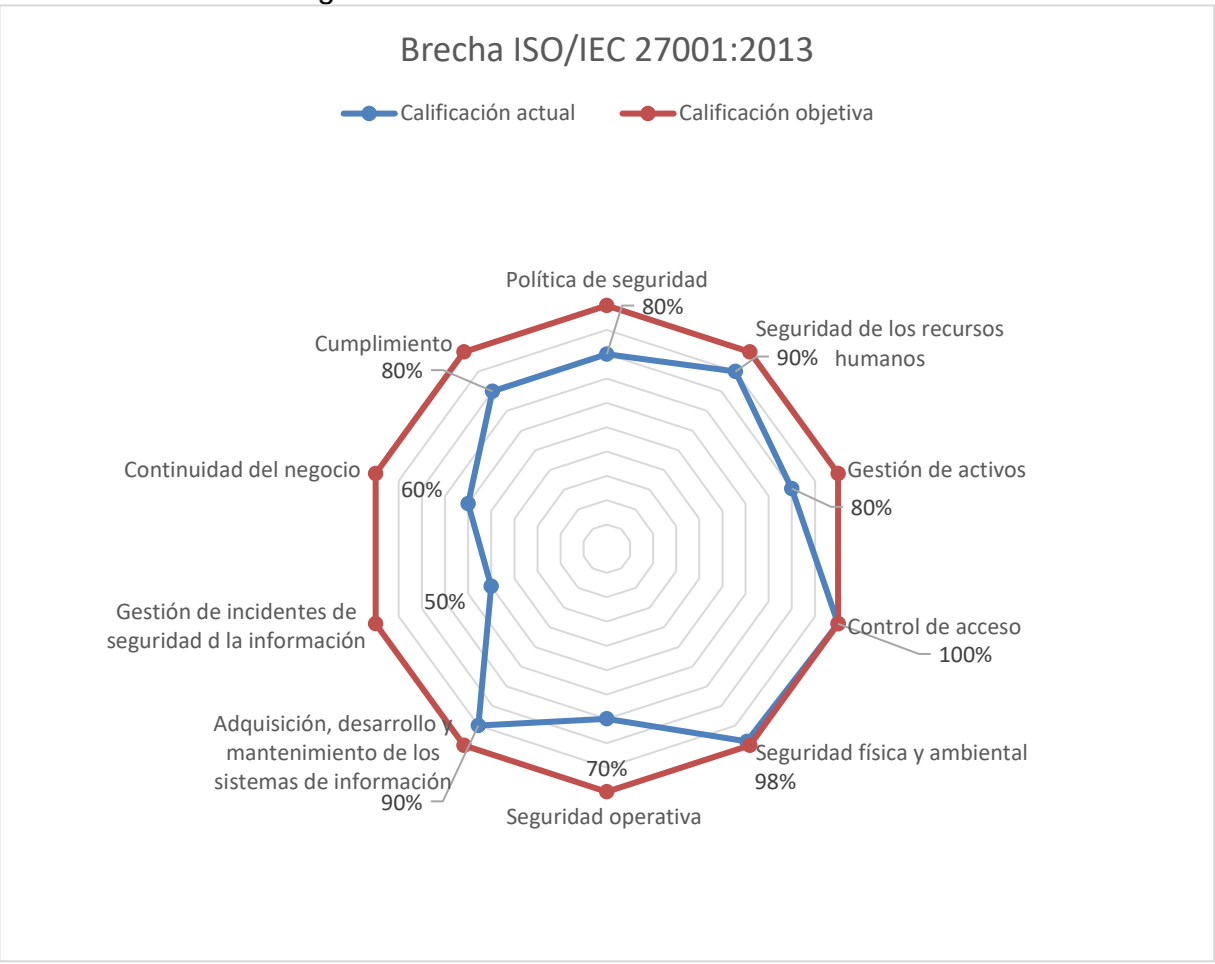
[30] MSPI. (s. f.). https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Como se observa en la figura 7, los dominios cuentan con un grado medio de ejecución. Los dominios en los cuales se debería tomar en consideración para su implementación y mejora son los siguientes:

- Gestión de incidentes de seguridad de la información
- Continuidad del negocio
- Seguridad operativa

Entre estos dominios es de gran importancia la política de gestión de incidentes de seguridad de la información.

Figura 7 - Brecha ISO/IEC 27001:2013



Fuente: Propia

6.4 FORMULAR LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN QUE SE PUEDEN APLICAR A FEBIMBO Y QUE CONTRIBUYAN A DISMINUIR LOS RIESGOS IDENTIFICADOS.

6.4.1 Introducción

La Políticas de Seguridad y privacidad de la información de Febimbo, representa la protección de los activos de información, tales como: software, hardware, información, características de procesos, procedimientos e instrucciones, con el fin de enseñar a todos los empleados sobre el uso adecuado de estos activos , para asegurar el cumplimiento de los estándares de disponibilidad, integridad y confidencialidad de la información que fluye a través de procesos apoyados en tecnologías de la información.

6.4.2 Objetivos

Las políticas definidas por Febimbo, tiene como finalidad lo siguiente:

- Velar por la integridad, confidencialidad y disponibilidad de los activos de información.
- Cumplir con lineamientos de Febimbo, para mantener un uso adecuado de los activos de información.
- Involucre a la alta dirección y proporcióneles las herramientas que necesitan para mantener actualizados sus sistemas de gestión de la seguridad de la información.
- Prevención de incidentes de seguridad que afectan los activos de información.
- Minimizar el riesgo, definiendo procedimientos alineados con el plan de respuesta al riesgo.
- Fomentar la seguridad de la información de los empleados.

6.4.3 Alcance

Las políticas de seguridad de la información, definidas, se aplican a todos los procesos tanto externos como internos, con el objetivo de garantizar un nivel de seguridad óptimo en los activos de información, de la empresa Febimbo.

6.4.4 Política de seguridad

Las políticas de seguridad de la información mencionadas a continuación tienen como objetivo ayudar a la alta gerencia a mejorar sus planes con relación a la protección de los activos de información acogiéndose a la legislación vigente.

6.4.5 Conformación del comité de SGSI

Con el fin de da garantizar la ejecución de las diversas actividades de apoyo a la seguridad de la información, se debe de conformar un comité para validar el SGSI, para dar cumplimiento a cada uno de los objetivos del sistema y así realizar la mejora continua.

Las políticas se actualizarán en un plazo no mayor a dos meses. Las reuniones que realiza el comité se programan con anticipación, y las decisiones tomadas se reflejan en actas firmadas por cada participante, y se lleva un registro de asistencia y aceptación de acuerdos.

El comité del SGSI deberá de estar conformado de la siguiente manera:

- Presidente del SGSI.
- Representante del área financiera.
- Representante del área jurídica.
- Representante del área IT.

El comité del SGSI, tendrá las siguientes funciones:

- Evaluar el nivel de cumplimiento de la norma ISO/IEC 27001:2013.
- Definir las políticas del SGSI y sus objetivos.
- Identificar los riesgos de seguridad de la información.
- Generar planes de acción para mitigar los riesgos de seguridad de la información.
- Capacitar a todo el personal en temas de seguridad de la información.
- Dar a conocer la creación del comité y sus funciones.

En todas las actividades ejecutadas por Febimbo, el comité del SGSI, encabezado por el presidente del comité, deberá tener en cuenta la seguridad de la información identificando amenazas, vulnerabilidades y riesgos, con el fin de abordar los controles necesarios que preserven la confidencialidad, integridad y disponibilidad de los activos de información.

6.4.6 Gestión de activos de información

Febimbo debe garantizar que cada uno de los activos de información que se encuentran en las instalaciones físicas, se encuentren identificados y registrados dentro del inventario; en el cual se deben de registrar los datos más relevantes de cada activo de información. La actualización del inventario de activos se debe de realizar una vez al año o partiendo de las necesidades de la empresa, este inventario debe de estar a cargo de la persona encargada del área de IT.

6.4.7 Clasificación de activos de información

Los activos de información se clasificarán de acuerdo con la importancia de FEBIMBO, con base en:

- [D] Disponibilidad
- [I] Integridad
- [C] Confidencialidad

Los activos de información de Febimbo se evaluarán partiendo de cada una de las variables expuestas anteriormente, asignando un valor cualitativo. De acuerdo con la clasificación definida se deberá etiquetar cada activo de información de manera física, donde se estipule el nivel e importancia del activo, dicho etiquetado deberá reconocerse fácilmente.

6.4.8 Propiedad de los activos

Cada uno de Los activos de información que hacen parte del inventario definido por el área de IT de FEBIMBO, deben estar asignados a un funcionario, el cual será el responsable de dicho activo de información.

- El usuario responsable del activo de información deberá de estar relacionado en el formato dispuesto para esta actividad, el cual debe de cumplir con lo siguiente para el cuidado del activo de información:

- Verificar que, dentro del inventario, en el cual se relacionan los activos asignados hagan parte de este.

- Garantizar que no haya fuga de información del activo asignado, con base en la clasificación e importancia del activo.

- Proteger el activo de información durante su uso y cuando no se esté utilizando.

6.4.9 Uso de los activos de información

Durante las labores ejecutadas por los funcionarios de Febimbo y que dentro de esas actividades esté relacionado el uso de activos de información; estos no deben de ser utilizados para actividades diferentes a las estipuladas dentro del contrato laboral. Por ello se plantean las siguientes reglas:

- **Uso de internet:** Solo será utilizado con fines laborales; el funcionario que utilice este servicio para fines personales asumirá el riesgo asociado y será sancionado por la empresa
- **Uso de impresoras y escáner:** solo estará permitido imprimir o escanear aquellos documentos que hagan parte de las funciones asignadas y para Febimbo.
- **Uso de teléfono fijo y/o celular asignado:** será para comunicación de carácter corporativo.
- **Dispositivos de almacenamiento externo:** solo se podrá almacenar información relacionada con las actividades laborales para las que fue contratado.

6.4.10 Devolución de activos de información

Al momento de terminar la vinculación laboral o cambio de cargo, todos los empleados de Febimbo deben de realizar la devolución de cada uno de los activos de información asignados al momento de la vinculación laboral.

El área de IT tendrá la obligación de verificar la entrega de los elementos asignados y generará un certificado de lo recibido, con el cual se le informará al área de gerencia para generar paz y salvo correspondiente.

Si en dicha entrega alguno de los elementos de IT, estuviera dañado perdido o intencionalmente, se deberá generar el respectivo cobro al funcionario, desde el área encargada.

6.4.11 Trabajo en casa

Cuando los funcionarios por diferentes situaciones no puedan asistir a las instalaciones de Febimbo, para desarrollar sus funciones pero les es posible ejecutar estas en modalidad de teletrabajo, el funcionario deberá enviar una petición previa a gerencia, área encargada de aprobar y autorizar el manejo del activo en modalidad de teletrabajo, una vez se cuente con la autorización, el área de IT deberá preparar los elementos necesarios en cuanto a elementos de tecnología para que el funcionario pueda realizar normalmente las actividades en modalidad de teletrabajo. El funcionario que esté desarrollando la actividad en la modalidad de teletrabajo no deberá realizar ninguna modificación de los elementos entregados.

6.4.12 Seguridad

Todos los funcionarios de Febimbo deben tener conocimiento de los riesgos asociados a las actividades para las que fueron contratados, de igual forma las amenazas de los activos de información que tienen a su cargo, deberán tener conocimiento de cada una de las políticas establecidas en este documento.

6.4.13 Control de acceso

Todo el personal contratado por Febimbo, deberá de acatar las normas con el acceso a los activos de información, estos son generados para validar que todos los empleados cuenten con los permisos y accesos entregados.

6.4.14 Políticas de control para acceso lógico

Para el desarrollo de cada una de las actividades del personal, tendrán acceso a información necesaria, dependiendo del perfil y cargo para el cual fueron contratados por Febimbo, los cuales se han definido en el manual de procesos.

Para el acceso de los funcionarios a los activos e información, se debe crear un usuario y contraseña, estos datos serán únicos y estarán gestionadas por el área de IT y entregadas al momento de la contratación

Al momento de tener el primer acceso al sistema de información, el usuario deberá realizar el cambio de contraseña, el cual deben de tener mínimo 12 caracteres, de los cuales mínimo deben ser carácter especial, mayúsculas, minúsculas, letras o números etc. El cambio de contraseñas se debe de realizar mínimo cada 3 meses o 90 días.

El área de IT de Febimbo, realizará un control del acceso para cada sistema de información y sistema operativo, con lo que deberá auditar los eventos de inicio de cada sesión, esto para analizar los registros y verificar anomalías o acciones de accesos no autorizados.

Al momento de terminación del contrato o cambio de cargo, el área de IT deberá desvincular los datos del usuario asignados y generar nuevos datos de acceso, con base en el nuevo cargo a ocupar.

Para el acceso a redes y servicios, se tendrán en cuenta las siguientes consideraciones:

- IT es el encargado de brindar en servicio a cada funcionario, dependiendo de las necesidades del usuario y las labores a ejecutar.

- No está permitido usar la conexión de internet para ingresar a páginas de pornografía, terrorismo, drogas, juegos y descarga de aplicaciones que puedan violar la seguridad de la información de la empresa Febimbo.

- No está permitido la instalación de ningún software, solo los permitidos por Febimbo y el área de IT.

Para el acceso a escritorio remoto se tendrá en cuenta lo siguiente:

- Las conexiones remotas serán realizadas por medio de VPN.

- Si el acceso se realizara desde afuera de las oficinas, el área de sistemas deberá configurar el equipo asignado para conectarse por medio de la VPN, esto se debe de realizar con previa autorización del área gerencial.

6.4.15 Seguridad Física

- El acceso a las instalaciones de la oficina de Febimbo, es únicamente para los funcionarios de cada una de las áreas.

- El acceso de personal externo deberá de ser acompañado por personal de Febimbo.

6.4.16 Seguridad en los equipos

Cada uno de los equipos de almacenamiento y aquellos que soportan la comunicación, se ubicaran de manera adecuada para que sean protegidos de manipulación física no autorizada y robo.

El cableado de energía eléctrica debe de estar protegido mediante canaletas para evitar su deterioro e incidentes del personal que se encuentra en las instalaciones de la empresa.

Con el fin de mantener el correcto funcionamiento de los equipos de cómputo, se deben de realizar dos jornadas de mantenimiento preventivo al año, las cuales deben de ser realizadas por el grupo de IT. Toda actividad de mantenimiento se debe de registrar en el formato de historial de mantenimiento y debe de anexarse a la hoja de vida de cada uno de los equipos.

Los equipos que requieran de mantenimiento por fuera de las instalaciones de Febimbo, se debe de contar con previa autorización por parte de la gerencia y el área de IT.

Los documentos que se encuentren en el escritorio de los equipos de cada funcionario deben resguardarse en un lugar seguro, ya sea temporal o por finalización de la jornada laboral.

Todos los equipos de cómputo deben de estar configurados para que se bloqueen en el momento que dejen de ser usados por los funcionarios.

6.4.17 Seguridad operativa

Todo procedimiento realizado a la infraestructura tecnológica debe deberá ser controlado y documentado por el área de IT.

6.4.17.1 Responsabilidades y procedimientos de operación

Cada uno de los procedimientos que se realicen a los recursos tecnológicos deberán estar documentados de la siguiente manera:

- Realización de Backus.
- Actualización de software.
- Actualización de hardware.
- Administración de servicios.
- Mantenimiento de equipos de cómputo y de elementos de redes.

Los cambios ejecutados a la infraestructura tecnológica deben de contar con autorización por Gerencia, a quien el comité de SGSI le informara mediante reunión sobre las actividades a realizar, y los riesgos que conlleva dicha acción; estas deberán tener un registro donde se relacione lo siguiente:

- Quien autorizo el cambio.
- Persona que realizara el procedimiento del cambio.
- Descripción de las labores a ejecutarse.
- Fecha y hora a realizar los cambios.

El coordinador del área de IT deberá de realizar las pruebas necesarias para corroborar la funcionalidad de los activos de información intervenidos, con el fin de evitar indisponibilidad de estos.

Código malicioso: Se debe de garantizar que todos los equipos estén protegidos y que cuenten con antivirus, antispam, y antispyware, los cuales deben de contar con su respectiva licencia y configuración para la prevención de códigos maliciosos.

Febimbo debe de garantizar que, dentro del presupuesto anual, sean destinados los recursos necesarios para compra de y software antivirus.

Copias de seguridad: Se debe de garantizar que la información que generen las diferentes áreas de la empresa, este respaldada por medio de copias de seguridad que garanticen la reposición de la información en caso de pérdida del equipo, daño o cualquier eventualidad.

El coordinador del área de IT debe de realizar actividades de respaldo de información, mediante copias de seguridad de cada una de las áreas de la empresa. Las labores de copias de seguridad deben de ser realizadas en el horario definido, teniendo en cuenta los horarios laborales de la empresa.

Control de instalación de Software: la instalación o eliminación de software debe de estar a cargo del área de sistemas, los cuales evaluaran según la necesidad.

Cada uno de los cambios realizados para la instalación de software, deben de ser registrados y anexados a las hojas de vida de los equipos, con el fin de evidenciar el historial y seguimiento, de igual forma se debe de mantener repositorios de software de la versión anterior por la que fue reemplazada o eliminada.

Gestión de Vulnerabilidades técnicas: se debe validar con un proveedor las vulnerabilidades técnicas del activo de información, mediante realización de pruebas, ataques simulados y escaneos de vulnerabilidades, cada una de estas actividades deberá de estar a cargo de IT.

Con base en las pruebas realizadas para la identificación de vulnerabilidades, se debe de documentar para darlas a conocer al comité de SGSI, de igual forma de debe de generar un plan de acción para corregir los hallazgos minimizando el nivel de riesgo e impacto.

Auditoria en los sistemas de información: Se debe realizar auditorías a cada sistema de información de la compañía, dichas auditorias deberán ser programadas por el coordinador del área de IT y ejecutadas por un ente o proveedor externo a la empresa; en estas auditorías se pretende conocer lo siguiente:

- Cumplimiento de la normatividad, cumplimiento de cada una de las políticas del sistema de información que permitan minimizar las amenazas y vulnerabilidades.
- Accesos correctos.
- Verificar procesos y procedimientos.
- Estabilidad de los sistemas de información.
- Mejoras futuras.

6.4.18 Seguridad en las telecomunicaciones

Mensajes de correo electrónico: Cada una de las áreas de la empresa cuenta con una cuenta de correo electrónico institucional, por tal motivo se prohíbe el uso de correos personales para envió o recepción de correos.

El correo institucional deberá de ser usado para el cumplimiento de cada una de las actividades para las que fue contratado, por lo que está prohibido el uso para fines personales.

Cada una de las cuentas de correo electrónico de Febimbo están limitadas a 50 Gigas de capacidad de almacenamiento, por tal motivo cada uno de los funcionarios deberán validar que información es importante y cual se puede

eliminar, adicional se pueden crear archivos PST (“es un formato de archivo propietario abierto que se utiliza para almacenar copias de mensajes, eventos de calendario y otros elementos dentro del software de Microsoft , como Microsoft Exchange Client , Windows Messaging y Microsoft Outlook.”[31]) para el tema de respaldos de la información en el correo.

Confidencialidad: Con el fin de que la información de Febimbo se mantenga de manera confidencial, cada uno se los funcionarios contratados deberán de firmar dentro de su contrato laboral los términos y condiciones en el que se estipula que la información que se utilizara en el cumplimiento de sus funciones no podrá ser divulgada o transferida a personas u empresas externas.

6.4.19 Seguridad de los sistemas de información

Cada uno de los sistemas de información actuales y los nuevos que se implementen en Febimbo deberán ser analizados, en consecuencia, el proveedor del software deberá especificar las características de seguridad del software, tales como:

- Requisitos de autentificación.
- Privilegios de usuarios.
- Registro de actividades en el sistema de información.
- Supervisión y monitoreo del sistema de información.
- Controles de seguridad.
- Cifrado del sistema de información.
-

Las actualizaciones o cambios realizados a los sistemas de información que sean por adquisición, actualización y nuevas funcionalidades, estos deben validarse por parte de IT, estos cambios deben de ser verificados con el fin de identificar impactos adversos en las aplicaciones.

6.4.20 Recursos compartidos

El uso de carpetas compartidas en OneDrive es una práctica útil de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de confidencialidad, integridad y disponibilidad de la información, por lo tanto, su uso y aplicación es controlado, solo se permite compartir información a miembros de la organización.

Por lo expuesto anteriormente, se definen los siguientes lineamientos para el uso seguro

- El coordinador de soporte IT establece e implementa, en los casos aprobados por la dirección, la configuración de acceso a la carpeta compartida OneDrive.

[31] Wikipedia contributors. (2023, 22 marzo). Personal Storage Table. Wikipedia. https://en.wikipedia.org/wiki/Personal_Storage_Table

- Los usuarios a quienes se les autoriza el recurso compartido serán los responsables por las acciones y los accesos sobre la información contenida en dicha carpeta.

6.4.21 Incidentes de seguridad

Todos los incidentes de seguridad de la información ocurridos en Febimbo deben de ser reportados por el funcionario al que se le presento el suceso, el cual debe de ser reportado mediante un correo electrónico y enviado al coordinador del grupo de IT, el reporte debe de ir acompañado de capturas de pantalla, fotos o videos

El coordinador del área de IT deberá realizar el registro del incidente, el formato de reporte de incidentes de seguridad digital, el cual, debe de reposar como evidencia.

Cada uno de los incidentes de seguridad ocurrido en Febimbo, deben de ser valorados, con el fin de conocer su impacto y sobre esa valoración se generan los respectivos controles; de igual forma como se debe detallar las acciones inmediatas que se realizan para mitigar el incidente de seguridad de la información.

Después de cada incidente de seguridad presentado en Febimbo, el área de IT deberá realizar la respectiva retroalimentación a todo el grupo de trabajo, con el fin de que se tome conciencia y evitar futuros sucesos.

6.4.22 Continuidad del negocio

Febimbo debe implementar el plan de continuidad del negocio, enfocado a aspectos de seguridad de la información, de tal manera que durante y después de eventos que impidan el normal funcionamiento de las actividades en las diferentes áreas, se debe generar una respuesta oportuna en la recuperación de los servicios informáticos esenciales de IT como servidores o información valiosa para la organización.

En los lineamientos establecidos en el plan de continuidad de seguridad de la información, se deben de ejecutar simulacros y pruebas que garanticen la efectividad de las medidas establecidas en el plan, adicional se debe de realizar una revisión anual a cada una de las estrategias de recuperación oportuna de los servicios informáticos.

El plan de continuidad de seguridad de la información deberá ser socializado a cada una de las áreas de la organización; de igual manera cada uno de los simulacros realizados, deben de involucrar a todo el personal, con el finde generar capacidad de respuesta en caso de que ocurra un incidente de seguridad de la información en la empresa.

6.4.23 Cumplimiento de requisitos legales

Con el fin de evitar el incumplimiento a cada uno de los requisitos legales (políticas, normas, legislaciones) se debe de realizar una identificación dé cada uno de los requisitos legales y una vez identificados, deben de ser documentados, para esta labor se contará con el apoyo del área jurídica, la cual deberá de asesorar al comité de SGSI con el fin de definir normas y leyes, entre las cuales se encuentras las siguientes:

- Tratamiento de datos personales.
- Protección de la información y de los datos.
- Derechos de autor.
- Delitos informáticos.

Febimbo cuenta con la política de tratamiento de datos personales, la cual, deberá ser integrada en los procesos de capacitación y sensibilización sobre seguridad de la información.

Para verificar el cumplimiento y evolución del sistema de gestión de seguridad de la información en cuanto a controles, políticas, procesos y procedimientos se deberá ejecutar auditorías internas, estas permitirán analizar si el SGSI está alineado a los objetivos misionales de Febimbo, con el objetivo de ajustar el sistema a las necesidades y cambios organizacionales, esta auditoria será llevada por el comité de SGSI quien generará un informe que será revisado por la gerencia para determinar acciones correctivas.

CONCLUSIONES

Con los resultados obtenidos de este estudio, se puede evidenciar varias conclusiones; En primer lugar, para la administración de los recursos tecnológicos de la empresa Febimbo es fundamental tener en cuenta los controles y políticas diseñadas dentro del SGSI, garantizando así; la seguridad de la información de cada uno de los procesos desarrollados. Es de gran importancia también mencionar que cada una de las políticas realizadas durante este proyecto, fueron generadas con base en las necesidades, procesos y características de la empresa Febimbo, lo cual fue indispensable para generar una operación eficiente del SGSI.

Desarrollando este SGSI se trabajó con cada área, desde el gerente y pasando por cada persona, todo esto para tener un mejor control en la organización, para poder mejorar los procesos. Esto también influye en que la norma legal sobre almacenamiento de datos y de información, aumenta la seguridad de la organización y mejora la confianza para Febimbo con los usuarios.

Con el informe de los activos de información y el análisis de cada uno de los riesgos realizados en Febimbo, se determinó cada uno de aquellos activos de información que son más críticos dentro de la empresa y que puedan desencadenar un alto impacto; con lo anterior se determina un plan de tratamiento de riesgos con el fin de minimizar el impacto y adicional, brindar información de gran importancia de cada uno de los activos de información para la ejecución de las diferentes actividades ejecutadas al interior de la empresa para el cumplimiento de la misión. Se valido el objetivo con la caracterización actual del fondo de empleados en el área de IT, todo esto para conocer los procesos y procedimientos y como se mejoran al diseñar la gestión de usuarios, como se mejora su proceso de incidentes y problemas, además de cómo se pueden mejorar la infraestructura de la compañía.

También se identificó el segundo objetivo con algo importante que es los activos de información con los que cuenta la compañía, todo esto para diseñar y aplicar el SGSI, encontrando vulnerabilidades y amenazas en la organización y validando los riegos con los que cuenta, todo esto para mitigarlos y tener los controles necesarios con algunas metodologías importantes, colocando nomenclaturas a los activos he identificado los activos, además de valorar los activos por dimensión.

En su tercer objetivo, algunos controles a la norma ISO 27001:2013, todo esto para garantizar la disponibilidad de la información, tratando los riesgos de manera adecuada cualitativamente y constatando su nivel de seguridad, también las políticas en general que se evidencian como un mapa de calor, donde se describe la brecha en la que está la organización y a donde quieren llegar para aumentar así su seguridad de la información.

También se evidencia como el cuarto objetivo ayudará a establecer nuevas políticas de seguridad de información y disminuirá los riesgos encontrados, algunos de los más importantes fueron las responsabilidades en la operación, definiendo como los sistemas de Backup de información deben tener un control anual en todo lo que se realiza en la organización de Febimbo.

RECOMENDACIONES

El diseño del SGSI fue de gran importancia para mejorar la seguridad de la información lo cual permite que los procesos desarrollados al interior de la empresa generen un alto grado de confianza al personal tanto externo como interno que labora en la empresa, no obstante, este paso debe de ir más allá, ya que se debe de realizas las respectivas revisiones y actualizaciones al SGSI con el fin de que se mantenga en el tiempo.

De igual manera, se recomienda que cada uno de los análisis de los riesgos que se realicen; se involucren los nuevos recursos tecnológicos, los cuales, ya hacen parte de la organización y que si no se da un uso adecuado pueden afectar la integridad, confidencialidad y disponibilidad de la información.

Se recomienda establecer un proceso de auditoría externa con el propósito de obtener diferentes puntos de vista, acerca del funcionamiento y cumplimiento del SGSI. De igual manera, se recomienda que el comité de SGSI, genere actualizaciones y revisiones, con el fin de que se puedan identificar nuevas necesidades y cambios, tanto en los activos de información, así como en cargos y/o funciones.

Se debe llevar a cabo auditorías anuales, todo esto para tener planes de acción, adicional es necesario invertir anualmente un presupuesto con la gerencia y área financiera, para mejorar la seguridad e implementar mejoras en la organización. La gerencia administrativa o junta deben validar los planes de acción a tomar o que se requieran para poder luego del diseño, realizar la implementación del SGSI para Febimbo.

Es importante monitorear y mejorar continuamente el sistema, evaluar continuamente el sistema de seguridad de la información implementado para asegurarse de que se está cumpliendo con los objetivos de seguridad. También se deben realizar mejoras continuas para adaptar el sistema a los cambios tecnológicos y a los nuevos riesgos que puedan surgir.

Se recomienda también certificar el sistema, para demostrar que el sistema de seguridad de la información del fondo de empleados cumple con los estándares internacionales, se puede certificar el sistema según la norma ISO 27001:2013, lo que permite demostrar a los afiliados y demás interesados que se está tomando en serio la seguridad de la información.

Ya para terminar se pueden realizar temas de sensibilización, destinadas a indicar a los usuarios el compromiso que se debe tener con la organización y aprender las amenazas de seguridad que podrían afectar la información de los usuarios y trabajadores de Febimbo.

BIBLIOGRAFÍA

CAMILO RODRÍGUEZ ISAZA. Ciclo de Deming PDCA – Planear, Hacer, Verificar, (10 agosto de 2022) Disponible en:. (https://crisaza.com/guia-de-scrum/el-empirismo-y-los-pilares-de-scrum/ciclo-de-deming-pdca-planear-hacer-verificar-actuar-camilo-rodriguez-isaza/)

CASESAR. Ataque informático. Recuperado 16 de octubre de 2021, Disponible en: (https://www.caser.es/glosario-seguros/comercio/ataque-informatico)

COLABORADORES DE WIKIPEDIA. Información. Wikipedia, la enciclopedia libre, (2022c, octubre 24) disponible en: https://es.wikipedia.org/wiki/Informaci%C3%B3n

CRUZ, H. Metodología OCTAVE para el análisis de riesgos en SGSI. PMG SSI - ISO 27001., (2022, 24 agosto). disponible en: https://www.pmg-ssi.com/2021/09/metodologia-octave-para-el-analisis-de-riesgos-en-sgsi/

DE LA IGLESIA, E. D. Tipos de vulnerabilidades en ciberseguridad. campus ciberseguridad. (22 junio de 2022)., disponible en: https://www.campusciberseguridad.com/blog/item/118-tipos-de-vulnerabilidades-en-ciberseguridad#:%7E:text=Una%20vulnerabilidad%20es%20una%20debilidad,sus%20correspondientes%20tipos%20de%20vulnerabilidades.

DEPARTAMENTO DE SEGURIDAD INFORMÁTICA. Departamento de Seguridad Informática: 10 octubre de 2022 Disponible en (http://www.seguridadinformatica.unlu.edu.ar/?q=node/12 página web)

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN BAJO LA NORMA ISO 27001:2013 en la E.P.S Asmet Salud. (20, junio de 2022). Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/27057/%20%09jfreyesa.pdf?sequence=1&isAllowed=y

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI BAJO LA NORMA ISO/IEC 27001:2013 para la empresa “en Línea Financiera” de la ciudad de Cali – Colombia. (8 de agosto de 2022,). disponible en: https://repository.unad.edu.co/bitstream/handle/10596/11907/76041068.pdf?sequence=1&isAllowed=y

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE SISTEMA DE LA EMPRESA RYMCO S.A BAJO LA NORMA ISO IEC/27001:2013. (2022c, octubre 24) disponible en :https://repository.unad.edu.co/handle/10596/3987

FEBIMBO, (octubre 28) disponible en: https://www.Febimbo.com/servicio.html

FIGUEROA CUBILLOS Carolina. Diseño de un sistema de gestión de seguridad de la información para el colegio Germán Arciniegas i.e.d., bajo la norma técnica colombiana NTC ISO/IEC 27001:2013. Bogotá 2019. 105 p. (Trabajo de grado para optar al título de especialista en seguridad). Universidad nacional abierta y a distancia UNAD. Escuela de ciencias básicas tecnología e ingeniería informática.

Gestión de Riesgos Magerit. (2006). Tithink. https://www.tithink.com/publicacion/MAGERIT.pdf

HURTADO PÉREZ Andrés Julián. Diseño del sistema de gestión de seguridad de la información - SGSI- para los procesos críticos de la cooperativa favor basado en la norma iso 27001:2013.. Bogotá. 239 p. (Trabajo de grado). Universidad piloto de Colombia. Facultad de ingeniería

*OFICINA ASESORA DE PLANEACIÓN Y CONTROL. subsistema de seguridad de la información (sgsi) (*Recuperado 28 de octubre de 2022), disponible en http://planeacion.udistrital.edu.co:8080/sigud/s/sgsi

SGSI. Mitología de implantación. (2022, 29 octubre). disponible en https://metologiadeimplantacion.blogspot.com/

TECNOLOGIAS DE LA INFORMACIÓN, Seguridad en sistemas de información (8 de agosto de 2022) octubre 24) disponible en: https://www.tecnologias-informacion.com/seguridad.html

WELIVESECURITY. MAGERIT: Metodología práctica para gestionar riesgos. [página web]. (14, mayo, 2013). [Consultado el 10, agosto, 2022]. Disponible en Internet: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

ANEXOS

Anexo 1 - Carta aprobación

V0.1

Bogotá, 15 de octubre de 2021

Señor:
RICHARD NIETO CARRILLO
GERENTE

Asunto: Autorización para la ejecución del proyecto titulado: DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL FONDO DE EMPLEADOS FEBIMBO EN EL ÁREA DE TECNOLOGÍA.

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a FEBIMBO, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA EL FONDO DE EMPLEADOS FEBIMBO EN EL ÁREA DE TECNOLOGÍA el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

Fuente: Propia

Anexo 2 - Descripción de funciones u Contrato

El CONTRATISTA en su calidad de trabajador independiente, se obliga para con El CONTRATANTE a ejecutar los trabajos y demás actividades propias del servicio contratado, el cual debe realizar de conformidad con las condiciones y cláusulas del presente documento y que consistirá en: Prestar el soporte técnico IT y medios tecnológicos, mediante outsourcing informático con el fin de lograr un uso de los medios tecnológicos más eficientes, estables y seguros. SEGUNDA. - DURACIÓN O PLAZO: La ejecución del presente contrato será de contados a partir de XX y se renovará automáticamente anualmente. TERCERA. - PRECIO: XXX CUARTA. - FORMA DE PAGO: El valor del contrato será cancelado así: Se pagará mensualmente, los primero 15 días de cada mes QUINTA.- OBLIGACIONES: El CONTRATANTE deberá facilitar acceso a la información y elementos que sean necesarios, de manera oportuna, para la debida ejecución del objeto del contrato, y, estará obligado a cumplir con lo estipulado en las demás cláusulas y condiciones previstas en este documento. El CONTRATISTA deberá cumplir en forma eficiente y oportuna los trabajos encomendados y aquellas obligaciones que se generen de acuerdo con la naturaleza del servicio, además se compromete a afiliarse a una empresa promotora de salud EPS, y cotizar igualmente al sistema de seguridad social en pensiones tal como lo indica el art.15 de le ley 100 de 1993, para lo cual se dará un término de ..... días contados a partir de la fecha de iniciación del contrato. De no hacerlo en el término fijado el contrato se dará por terminado SEXTA. - SUPERVICION: El CONTRATANTE o su representante supervisará la ejecución del servicio encomendado, y podrá formular las observaciones del caso, para ser analizadas juntamente con El CONTRATISTA. SEPTIMA. - TERMINACIÓN. El presente contrato terminara por acuerdo entre las partes y unilateralmente por el incumplimiento de las obligaciones derivadas del contrato. OCTAVA. - INDEPENDENCIA: El CONTRATISTA actuará por su cuenta, con autonomía y sin que exista relación laboral, ni subordinación con El CONTRATANTE. Sus derechos se limitarán por la naturaleza del contrato, a exigir el cumplimiento de las obligaciones del CONTRATANTE y el pago oportuno de su remuneración fijada en este documento. NOVENA. - CESIÓN: El CONTRATISTA no podrá ceder parcial ni totalmente la ejecución del presente contrato a un tercero, sin la previa, expresa y escrita autorización del CONTRATANTE. DÉCIMA. -DOMICILIO: Para todos los efectos legales, se fija como domicilio contractual a la ciudad de Bogotá.

Anexo 3 - Cronograma actividades

1. CRONOGRAMA DE ACTIVIDADES												
ACTIVIDAD	***MES 1***	***MES 2***	***MES 3***	***MES 4***	***MES 5***	***MES 6***	***MES 7***	***MES 8***	***MES 9***	***MES 10***	***MES 11***	***MES 12***
Levantamiento información de sistemas	*X*											
Definir requerimientos de sistemas		*X*										
Identificar procesos de sistemas			*X*									
Identificar eventos de sistemas				*X*								
Diseñar el modelo de riesgos de sistemas					*X*							
Diseñar la evaluación de riesgos de sistemas						*X*						
Diseñar la valoración de riesgos							*X*					
Diseñar el tratamiento de riesgos de sistemas								*X*				
Diseñar la matriz de controles el tratamiento de									*X*			

riesgos de sistemas												
Validar la Norma ISO/IEC 27.001 y el ciclo de Deming										*X*		
Validar metodología MAGERIT											*X*	
Diseñar anexos y procedimientos para implementar el SGSI												*X*

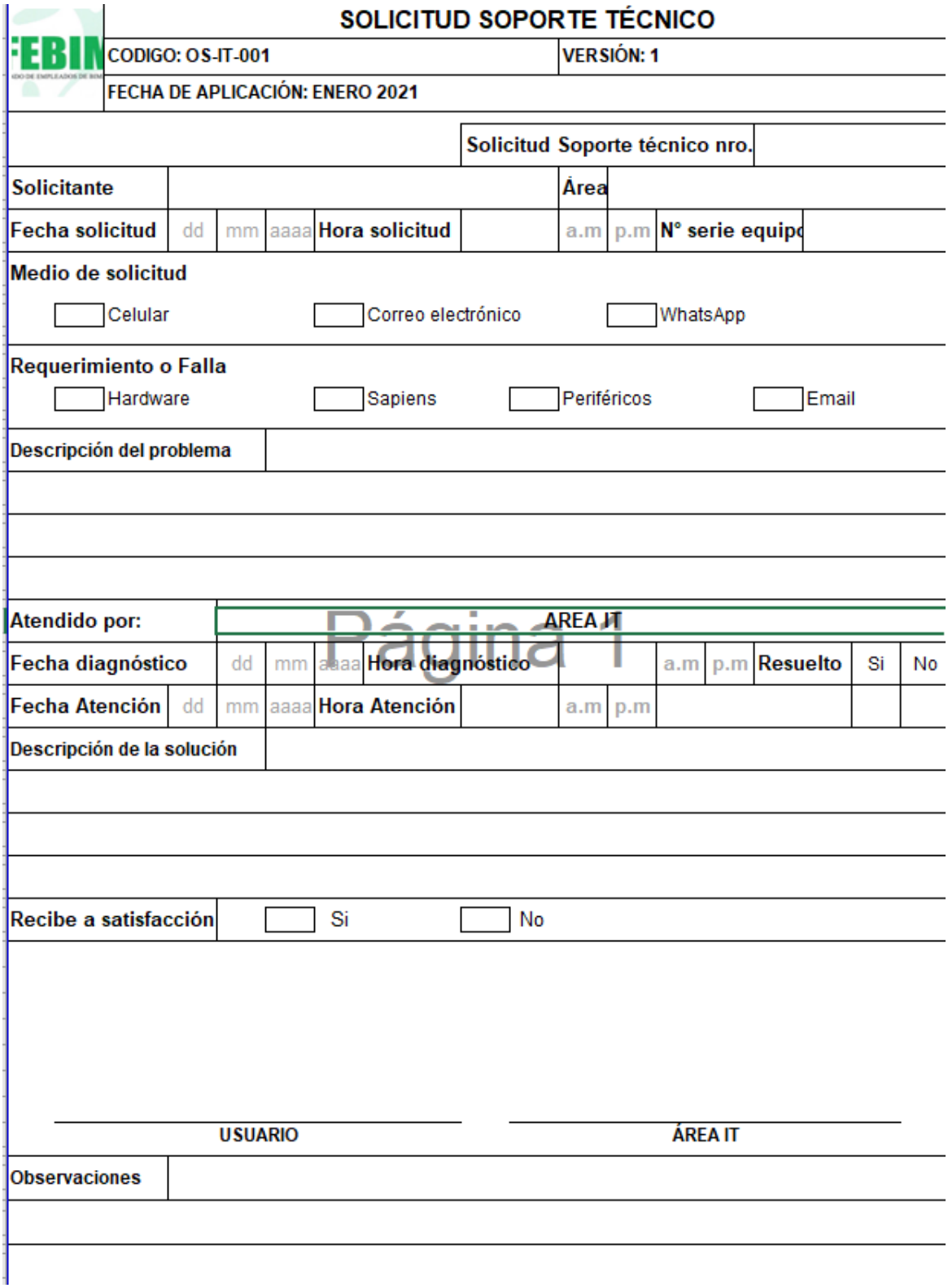
Fuente: Propia

Anexo 4 - Recursos necesarios

RECURSO	***DESCRIPCIÓN***	***PRESUPUESTO***
Equipo Humano	*Especialista En Seguridad informática, Quien Elabora El Proyecto*	*Sin Gatos*
Equipos y Software	*Laptop O Computador*	*Sin Gatos*
Viajes y Salidas de Campo	*Levantar Información, Implementar El Sistema Y Capacitar Al Usuario*	*Sin Gatos*
Materiales y suministros	*Memoria USB, Google En La Nube, Disco Duro*	*Sin Gatos*
Bibliografía	-	-
TOTAL		

Fuente: Propia

Anexo 5 - OS-IT-001 Solicitud Soporte técnico



SOLICITUD SOPORTE TÉCNICO

CODIGO: OS-IT-001	VERSIÓN: 1
FECHA DE APLICACIÓN: ENERO 2021	

Solicitud Soporte técnico nro.

Solicitante						Área			
Fecha solicitud	dd	mm	aaaa	Hora solicitud		a.m	p.m	N° serie equipo	

Medio de solicitud

☐ Celular ☐ Correo electrónico ☐ WhatsApp

Requerimiento o Falla

☐ Hardware ☐ Sapiens ☐ Periféricos ☐ Email

Descripción del problema	

Atendido por:	AREA IT										
Fecha diagnóstico	dd	mm	aaaa	Hora diagnóstico		a.m	p.m	Resuelto	Si	No	
Fecha Atención	dd	mm	aaaa	Hora Atención		a.m	p.m				

Descripción de la solución	

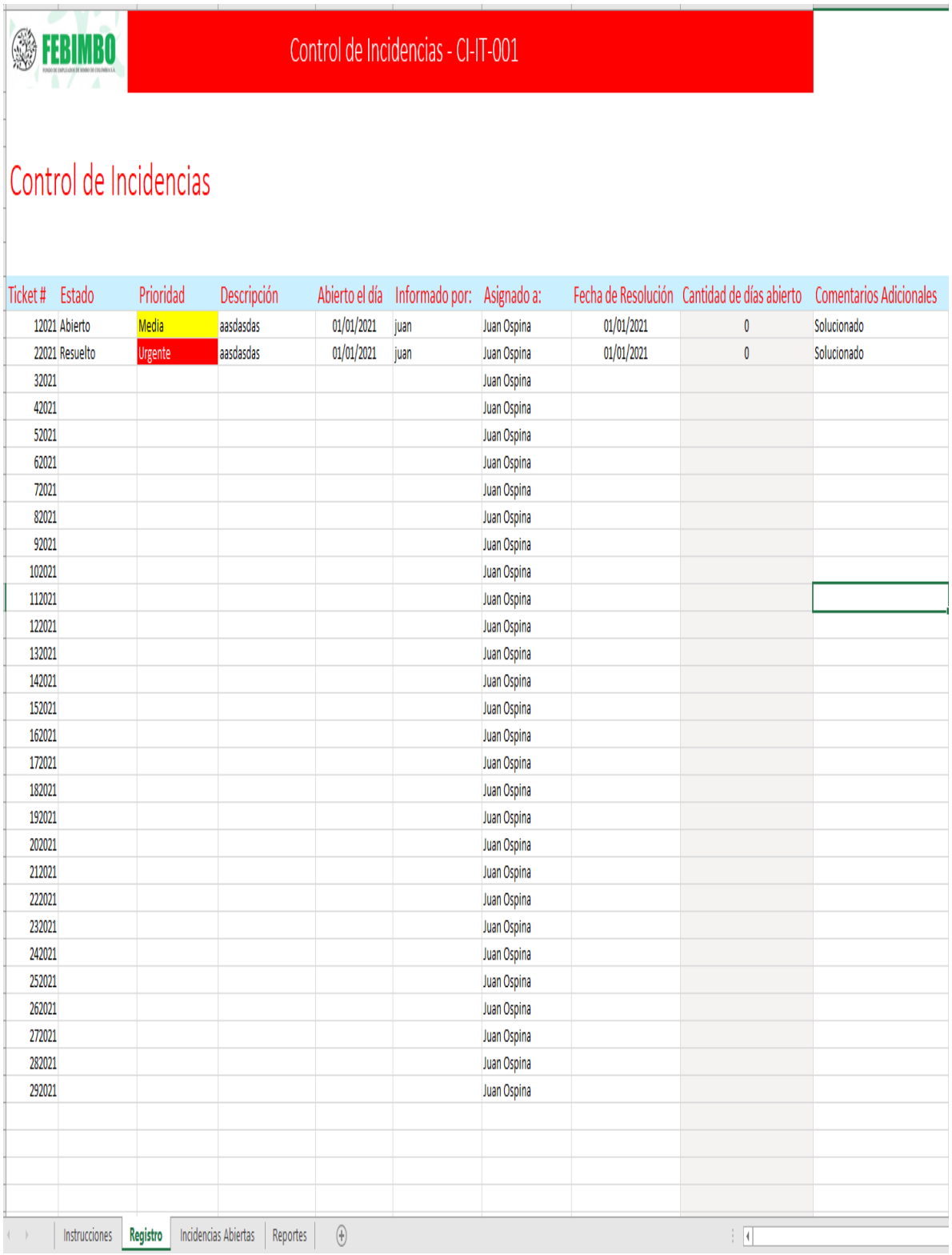
Recibe a satisfacción ☐ Si ☐ No

USUARIO ÁREA IT

Observaciones	

Fuente: Propia

Anexo 6 - CI-IT-001 Seguimiento Tickets



FEBIMBO

Control de Incidencias - CI-IT-001

Control de Incidencias

Ticket #	Estado	Prioridad	Descripción	Abierto el día	Informado por:	Asignado a:	Fecha de Resolución	Cantidad de días abierto	Comentarios Adicionales
12021	Abierto	Media	aasdasdas	01/01/2021	juan	Juan Ospina	01/01/2021	0	Solucionado
22021	Resuelto	Urgente	aasdasdas	01/01/2021	juan	Juan Ospina	01/01/2021	0	Solucionado
32021						Juan Ospina			
42021						Juan Ospina			
52021						Juan Ospina			
62021						Juan Ospina			
72021						Juan Ospina			
82021						Juan Ospina			
92021						Juan Ospina			
102021						Juan Ospina			
112021						Juan Ospina			
122021						Juan Ospina			
132021						Juan Ospina			
142021						Juan Ospina			
152021						Juan Ospina			
162021						Juan Ospina			
172021						Juan Ospina			
182021						Juan Ospina			
192021						Juan Ospina			
202021						Juan Ospina			
212021						Juan Ospina			
222021						Juan Ospina			
232021						Juan Ospina			
242021						Juan Ospina			
252021						Juan Ospina			
262021						Juan Ospina			
272021						Juan Ospina			
282021						Juan Ospina			
292021						Juan Ospina			

Instrucciones | Registro | Incidencias Abiertas | Reportes

Fuente: Propia

Anexo 7 - CM-IT-001 Cronograma Mantenimiento

FEBIMBO

CRONOGRAMA MANTENIMIENTO - CM-IT-001

USUARIO	FECHA	HORA	OBSERVACIONES	REALIZADO

Fuente: Propia

Anexo 8 - FSM-IT-001 Formato de software y mantenimiento

FEBIMBO

FSM-IT-001 - Formato de Software y Mantenimiento

DATOS DEL COLABORADOR					
Nombre		Cargo		Usuario de Red	
Correo		Area		Fecha de revision	

HARDWARE				
TIPO	NOMBRE EQUIPO	MARCA	MODELO	SERIAL
DESKTOP ☐ LAPTOP ☐				
PROCESADOR	MEMORIA RAM (GB)	CAPACIDAD DE DISCO (GB)	TECLADO SERIAL	MOUSE SERIAL
MONITOR	CARGADOR	BASE REFRIGERANTE	TELEFONO SERIAL	IP TELEFONO

SOFTWARE					
Software estándar corporativo		Software Especial Instalado		Software Eliminado	
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐
	☐		☐		☐

OBSERVACIONES	
DATOS FIRMA	
RECIBE	ÁREA IT
Nombre:	Nombre:

Fuente: Propia