DISEÑO DE UN SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001:2013 PARA LA COMPAÑÍA ESSENSALE S.A.S.

CESAR DANIEL RINCON BRITO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

DISEÑO DE UN SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001:2013 PARA LA COMPAÑÍA ESSENSALE S.A.S.

CESAR DANIEL RINCON BRITO

PROYECTO APLICADO COMO REQUISITO ACADÉMICO PARA OBTENER EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de Proyecto:

JOHNN EDUARD CRIOLLO SALAMANCA

EDUARD MANTILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2020

Nota de aceptación

Firma presidente del Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 20 de diciembre de 2020

DEDICATORIA

Quiero ofrecer el desarrollo de este proyecto y agradecimiento:

A la Universidad Nacional Abierta y a Distancia UNAD y a cada uno de los docentes que han contribuido al desarrollo de este proyecto.

A la compañía Essensale S.A.S que ha adoptado las normas de este proyecto para el beneficio y desarrollo de la misma.

.

A todos ellos, les agradezco y les dedico este proyecto.

AGRADECIMIENTOS

A: Los docentes Juan José Cruz Garzón, Luis Fernando Zambrano, Johnn Eduard Criollo Salamanca y Eduard Mantilla, por apoyar y asesorar el diseño, orientación y desarrollo del presente compromiso.

A: Compañeros y docentes de las diferentes asignaturas cursadas durante el desarrollo de la especialización.

A: Todas aquellas personas que, aunque no aludo en estas gratitudes, de alguna u otra manera permitieron la ejecución de este trabajo.

Muchas Gracias

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ATAQUE: Acceso no autorizado a un activo, con el fin de destruir, sabotear u obtener información[1].

CEH: Certificación para el análisis de vulnerabilidades en los sistemas de información.

Conformidad: cumplir con los diferentes tipos de requisitos creados por alguna entidad[2].

DESASTRE: Evento desventurado, desagradable[3].

DIGITAL: almacenamiento, procesamiento, o presentación información a nivel de bits[4].

DISPOSITIVO: Objeto o mecanismo para desarrollar actividades especiales[5].

ERP: Enterprise Resource Planning, conjunto de módulos relacionados entres si para la toma de decisiones[6].

---

[1] RAE. Real Academia Española. [Sitio web], [Consulta: 20 de noviembre 2020]. Disponible en: https://dle.rae.es/ataque.

[2] EC-Council. Certified Ethical Hacker (CEH). [Sitio web], [Consulta: 10 octubre 2018]. Disponible en: www.eccouncil.org.

[3] RAE. Real Academia Española. [Sitio web]. [Consulta: 15 de noviembre 2020]. Disponible en: https://dle.rae.es/desastre.

[4] RAE. Real Academia Española. [Sitio web]. [Consulta: 15 de noviembre 2020]. Disponible en Internet: < https://dle.rae.es/digital>.

[5] Oracle. Oracle Colombia. [Sitio web]. [Consulta: 18 de agosto 2019]. Disponible en: https://www.oracle.com/co/erp/what-is-erp/.

[6] RAE. Real Academia Española. [Sitio web]. [Consulta: 15 de noviembre 2020]. Disponible en: https://dle.rae.es/infraestructura.

INFRAESTRUCTURA: Conjunto de elementos necesarios para el funcionamiento de las operaciones[7].

SISTEMA: Conjunto de reglas relacionadas entre sí de forma racional[8].

SALVAGUARDA: Almacenar datos sin pérdidas con la opción de recuperarlos en cualquier momento[9].

PARETO: Utilidad para la toma de decisiones basado en graficas organizadas con información de mayor a menor dependiendo de su magnitud, creado por Vilfredo Pareto que dice: El 80% de los problemas se pueden solucionar, si se eliminan el 20% de las causas que los originan[10].

POLÍTICA: Conjunto de actividades para la toma de decisiones[11].

---

[7] RAE. Real Academia Española. [Sitio web], [Consulta: 15 de noviembre 2020]. Disponible en: https://dle.rae.es/infraestructura.

[8] RAE. Real Academia Española. [Sitio web], [Consulta: 15 de noviembre 2020]. Disponible en: https://dle.rae.es/sistema.

[9] RAE. Real Academia Española. [Sitio web], [Consulta: 15 de noviembre 2020]. Disponible en: https://dle.rae.es/salvaguarda.

[10] ANDRES LEUDO GARCIA Y CARLOS ALBERTO YEPES CARTAGENA. Identificación de las técnicas para la recuperación de proyectos en crisis. [En línea]. Trabajo de grado presentado como requisito para optar el título de especialista en gestión integral de proyectos, Universidad San Buenaventura, 2016. [Consultado 5 de noviembre 2019]. Disponible en: http://bibliotecadigital.usbcali.edu.co/bitstream/10819/3711/1/Identificacion_tecnicas_recuperacion_leudo_2016.pdf.

[11] RAE. Real Academia Española. [Sitio web], [Consulta: 15 de noviembre 2020]. Disponible en: https://dle.rae.es/politica.

GSI: Sistema de gestión de seguridad de la información[12].

TRAZABILIDAD: Identifica el origen y las etapas en el proceso de desarrollo, producción y salida[13].

---

[12] MINTIC. Ministerio de Tecnologías de la Información y Comunicaciones. [Sitio web], [Consulta: 10 de noviembre 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/w3-article-5482.html.

[13] RAE. Real Academia Española. [Sitio web], [Consulta: 20 de noviembre 2020]. Disponible en: https://dle.rae.es/trazabilidad.

RESUMEN

El presente proyecto tiene como finalidad mejorar el tratamiento de la información, los activos y personal de la compañía ESSENSALE S.A.S ubicada en Santiago de Cali, para tener respuesta rápida a posibles desastres naturales, acciones mal intencionadas de acceso abusivo o compromiso de los sistemas de información de la compañía.
Se desarrollará un sistema de gestión de seguridad de la información estableciendo diferentes políticas para proteger los activos de ESSENSALE S.A.S.

La metodología aplicada para el diseño del SGSI seleccionada fue el sistema PHVA (Planear, Hacer, Verificar, Actuar), la cual se basa en procesos que permiten establecer, implementar, mantener y lograr la mejora continua de un sistema de gestión de información[14].

Palabras clave: activos, amenazas, desastres, disponibilidad, información, integridad, PHVA, políticas, riesgos, salvaguardas, seguridad, ISO 27001, SGSI.

---

[14] ISO 9001. Ciclo PHVA. [Sitio web], [Consulta: 10 de noviembre 2020]. Disponible en: https://www.nueva-iso-9001-2015.com/2019/05/ciclo-phva-en-iso-9001/.

ABSTRACT

The purpose of this project is to improve the treatment of information, assets and personnel of the company ESSENSALE SAS located in Santiago de Cali, to have a rapid response to possible natural disasters, malicious actions of abusive access or compromise of information systems of the company.

An information security management system will be developed establishing different policies to protect the assets of ESSENSALE S.A.S.

The methodology applied for the design of the selected ISMS was the PHVA system (Plan, Do, Verify, Act), which is based on processes that allow establishing, implementing, maintaining and achieving continuous improvement of an information management system.

The Essensale SAS perfumery and cosmetics company based in Santiago de Cali included in the 500 most important companies in Valle del Cauca has as a project for its clients to offer information about their sales, forecasts, statistics, orders and online payments, it has a Siesa ERP system and databases hosted at its own headquarters.

The company is independent from protecting the information since all its servers are physically located in its facilities, and allowing access to its clients from abroad forces it to acquire methods so that the information always remains safe and reliable.

Keywords: assets, availability, disasters, information, integrity, ISMS, ISO 27001, PDCA, policies, risks, safeguards, security, threats,

INTRODUCCIÓN

La seguridad de la información en las compañías es esencial debido a que se encuentran en una era digital donde se trabaja en gran porcentaje la manipulación de datos mediante dispositivos electrónicos.

La empresa Essensale S.A.S de perfumería y cosmética con sede en Santiago de Cali incluida en las 500 empresas más importantes del Valle del cauca tiene como proyecto para sus clientes ofrecer información acerca de sus ventas, pronósticos, estadísticas, pedidos y pagos en línea, cuenta con un sistema ERP de Siesa y bases de datos alojadas en su propia sede.

La sociedad es independiente de proteger la información ya que todos sus servidores se encuentran físicamente en sus instalaciones, y permitir el acceso a sus clientes desde el exterior la obligan a adquirir métodos para que la información siempre permanezca segura y sea confiable.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La empresa ESSENSALE S.A.S de perfumería y cosmética en su constante crecimiento ha presentado diferentes opiniones acerca de sus productos por parte de sus clientes en sus 13 años de operación.

En los últimos años ha incrementado su oferta de productos para satisfacer los gustos de los clientes, mejorar su imagen y belleza, estos productos requieren de un control especial, ya que son productos químicos que pueden afectar la salud de las personas que lo utilicen por lo cual la compañía ESSENSALE S.A.S busca mejorar su servicio, para ello implementó las soluciones del proveedor tecnológico SIESA, controlando la información desde servidores locales para las bases de datos y servidores de aplicaciones, que se exponen por medio de internet y su red local en conjunto con un nuevo sistema ERP, aplicaciones hechas a la medida por su equipo de desarrollo, y que son manipuladas por diferentes colaboradores de la compañía, para dar soluciones a todos los inconvenientes que sean reportados, siempre tratando de mantener y mejorar para seguir avanzando y consolidarse como una de las compañías más importantes a nivel nacional[15].

---

[15] SIESA. SIESA Enterprise Resource Planning. [Sitio web], [Consulta: 5 de Febrero 2018]. Disponible en: https://www.siesa.com.

Logrando el perfilamiento de cada una de las tiendas Senthia, conociendo la demanda, el inventario optimo, el Pareto, horas de mayor venta, el tipo y perfil de cada consumidor, número de clientes atendidos, estacionalidad de la tienda.

Para esta iniciativa se definió un responsable y las herramientas tecnológicas a utilizar. (INTRANET, ERP, CRM).

En esta creciente exponencial que ha venido presentando se adquirió gran cantidad de dispositivos tecnológicos para el desarrollo de sus actividades, diferentes equipos como computadores de escritorio, computadores portátiles, servidores, routers y desarrollo de aplicaciones, no obstante la compañía es independiente de proteger la información ya que todos sus servidores se encuentran físicamente en sus instalaciones, y permitir el acceso a sus franquiciados desde el exterior como también a sus colaboradores la obligan a adquirir métodos para que la información siempre permanezca segura y sea confiable.

Este documento pretende dar a conocer cómo desarrollar un SGSI para mejorar los servicios que ofrece la compañía ESSENSALE S.A.S en cuanto al manejo de incidencias, tipificación, asignación y controles, realizando un seguimiento, documentar, y generar reportes para futuros problemas y dar solución oportuna.

La compañía tiene como objetivo consolidar la Información en una sola plataforma tecnológica para tener un control adecuado de la cadena de valor, garantizando tener información actualizada y de fácil acceso a todos los procesos estratégicos de la organización, así mismo se busca tener Integridad y estabilidad en la información de los puntos de venta permitiendo trabajar en línea y en desconectado.

ETAPAS:

1. Negociación y contratación de servicios con proveedor ERP.
2. Alineación de requerimientos del ERP con plan estratégico
3. Diagnostico levantamiento de requisitos, adquisición de HW para automatización de Cadena de Valor, selección y liberación de grupo de trabajo.
4. Capacitación, ambientación, diseño y desarrollo.
5. Pruebas piloto, carga de inventarios iniciales, y corte al nuevo sistema.

La compañía cuenta con un único canal de acceso a la información de clientes y colaboradores para mejorar la comunicación y los tiempos de respuesta de los procesos que actualmente se hacen por diferentes medios, alinear los procesos y reportes automatizables del objetivo estratégico A4 en una sola plataforma para facilitar seguimiento de cumplimiento de metas.

ETAPAS:

1. Levantamiento de reportes y procesos automatizables del plan estratégico (Pedidos, Rolling Forcast, etc.), contratación de nuevo ingeniero de desarrollo.
2. Implementación de adecuaciones tecnológicas para soportar el proyecto, adquisición de hosting/dominio para extranet, adquisición de equipos de red y plataformas de administración de red para mejorar seguridad y desempeño de red local en escenario sin Hosting en Data center o negociación con data center.
3. Desarrollo de aplicaciones planeadas según plan estratégico.
4. Pruebas piloto, solución de fallas, y lanzamiento de la plataforma a franquiciados.

Durante el desarrollo de este proyecto se contó con la aprobación de los representantes legales y el gerente de tecnología para llevar a cabo todos los procedimientos que expone un SGSI.

1.2 FORMULACIÓN

¿En qué medida mejoraría la seguridad de la información el diseño de un sistema de gestión de seguridad de la información aplicando la norma internacional ISO/IEC 27001:2013 para la compañía ESSENSALE S.A.S.?

1.3 DESCRIPCIÓN

El presente documento de proyecto de grado tiene como objetivo principal presentar el diseño de un Sistema de Gestión de Seguridad de la Información para la compañía Essensale S.A.S con el fin de acompañar a la incorporación del estándar ISO 27001:2013

para la seguridad de la información en el manejo de sus procesos para su buen funcionamiento y toma de decisiones, contrarrestando los problemas que se puedan generar al implementar las nuevas tecnologías en todas sus sucursales y clientes.

Se ha podido apreciar en la última década que el desarrollo tecnológico crece a diario de una forma exponencial, las compañías se ven obligadas a mejorar su infraestructura tecnológica donde también podemos evidenciar que la gran mayoría de personas están conectadas de alguna forma con diferentes tipos de tecnología haciendo que se tomen ciertas medidas para que la información llegue a su destino de una forma segura y cumpla con su objetivo.

En este plano se hace necesario que el conocimiento y los aportes a la ciencia resuelvan las necesidades de la sociedad, donde los usuarios pueden encontrarse con diferentes problemas que puedan afectar el funcionamiento de sus máquinas en todos los campos, sea en su red local LAN, red inalámbrica WLAN, su dispositivo móvil (Smartphone) por medio de aplicaciones que accedan a su información aprovechando las vulnerabilidades, ataques a sus contraseñas, suplantación de identidad, pérdida de datos y otros[17].

---

[17] CISCO. Redes Inalámbricas. [Sitio web], [Consulta: 7 de marzo 2018]. Disponible en: https://www.cisco.com/c/es_co/products/wireless/index.html.

2. JUSTIFICACIÓN

Para la empresa ESSENSALE S.A.S los franquiciados son clientes de mayor importancia, ya que son los mayores inversionistas en la compañía, actualmente cuenta con más de 40 franquiciados, y 90 tiendas propias a nivel nacional, las tiendas propias y franquicias consultan la información de la central conectándose a la Internet por medio de conexiones seguras, en ella los cliente realizan sus pedidos y consultan información, como también todas las ventas realizadas a diario, estos datos son cargado en tiempo real, siendo una información también muy importante para la toma de decisiones de los clientes.

Algunos parámetros en las configuraciones ofrecidas en el ERP vienen siendo utilizadas, pueden generar un fallo ya que son datos conocidos por diferentes personas, como también las aplicaciones que contienen contraseñas preestablecidas en las base de datos, que actualmente son utilizadas por empleados internos, estas puede permanecer en los equipos donde cualquiera puede acceder a ellos o al ser cambiados por otros equipos la información puede salir de la compañía y ser accedida desde el exterior.

Debido a que su proveedor tecnológico no ofrece en su contrato el tema de la seguridad de la información es necesario implementar normas internacionales como la ISO 27001:2013, y desarrollar aplicaciones para contrarrestar el acceso a usuarios no autorizados, estas aplicaciones ofrecen a la compañía reportes de posibles ataques para mejorar sus diseños y desarrollos, como también un control interno y externo de sus empleados o franquiciados.

La seguridad de la información cuando esta ha sido implementada y certificada, al ser ofrecida a los cliente va a dar una mejor imagen y garantía en el uso del software o hardware utilizado en la empresa Essensale, dando al cliente confianza a la hora de realizar contratos y adquirir las nuevas tecnologías que se van implementando para manejar los datos por esta razón, es necesario que se establezcan políticas y objetivos de seguridad con un sistema de gestión de seguridad que administre de forma correcta la información.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información aplicando la norma internacional ISO/IEC 27001:2013 para la compañía Essensale S.A.S.

3.2 OBJETIVO ESPECÍFICOS

1. Realizar el levantamiento de información y clasificación de los activos de la compañía ESSENSALE S.A.S de acuerdo a la Norma ISO/IEC 27001:2013.
2. Identificar las vulnerabilidades y amenazas de seguridad expuestas en la compañía ESSENSALE S.A.S basado en la metodología de análisis y evaluación de riesgos informáticos MAGERIT.
3. Emplear el análisis de riesgos basados en los procesos desarrollando la norma internacional ISO/IEC 27001:2013 para establecer una serie de estrategias y controles oportunos que protejan la información.
4. Determinar los objetivos de control más inmediatos sobre norma ISO/IEC 27001:2013 aplicables a la compañía ESSENSALE S.A.S.
5. Ejecutar pruebas de penetración en el sistema de la compañía ESSENSALE S.A.S para hallar debilidades en materia de seguridad.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO.

4.1.1 ISO/IEC 27001:2013.

Es el estándar difundido oficialmente para la gestión de la seguridad de la información, las organizaciones al implementar este estándar pueden identificar los riesgos de seguridad y asignar controles en el lugar para tratarlos, obteniendo confianza en el cliente de que su información confidencial está asegurada, no caerá en manos de terceros y crecer como empresa.

Para establecer, supervisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información el estándar establece los siguientes pasos:

- Identificación de requerimientos de seguridad.
- Evaluación sobre las amenazas de los activos de información.
- Identificación de vulnerabilidad.
- Análisis de impacto potencial de incidentes.
- Evaluación de los riesgos.
- Aplicación, mantenimiento y mejoras de controles del sistema de información.

4.1.2 METODOLOGÍA DE SEGURIDAD.

Abarca la auditoría de seguridad y las vulnerabilidades en el sistema que pueden ser explotadas con éxito por los atacantes. En esta fase se evalúa la seguridad de un sistema de información o red simulando un ataque para encontrar vulnerabilidades que un atacante podría explotar. Los resultados de este test se documentan en un reporte para la toma de decisiones en la compañía.

4.1.3 TEST DE PENETRACIÓN.

El test de penetración realizado en una compañía o ambiente controlado resuelve los siguientes elementos.

- Reducir el gasto en la seguridad de tecnologías de información al identificar vulnerabilidades.

- Obtener certificaciones.
- Prevenir futuros ataques.
- Evaluar la eficacia de los dispositivos de red.
- Realizar técnicas avanzadas y ataques para identificar la inyección de SQL, las secuencias de comandos Cross Site Scripting (XSS), LFI, RFI en aplicaciones web.
- Realizar un informe profesional y aceptado que logre la aceptación administrativa y técnica.
- Escribir códigos de explotación para acceder a un sistema o aplicación vulnerable.
- Explotar vulnerabilidades en sistemas operativos como Windows, Linux.

4.1.4 TIPOS DE TEST DE PENETRACIÓN.

Los tipos de test de penetración se dividen en tres modalidades que son llamadas Blackbox, Whitebox, y Greybox.

- Black Box: No se tiene acceso o un conocimiento de la compañía.
- White Box: Conocimiento completo de la infraestructura.
- Grey Box: Conocimiento limitado de la infraestructura.

4.1.5 FASES DE TEST DE PENETRACION:

Consta de tres fases, pre ataque, ataque y post ataque

PRE-ATAQUE

- Planeación y preparación.
- Metodología designada.
- Información de red de trabajo.

ATAQUE

- Perímetro de penetración.
- Selección de objetivos.
- Escalamiento de privilegios.
- Ejecución e implantación.

POST-ATAQUE

- Reporte
- Limpieza
- Destrucción de artefactos

4.1.6 PENTESTING PÁGINAS WEB.

En este tipo de análisis el "pentester" utiliza una página web para encontrar vulnerabilidades, por lo general en el código fuente, o descargar su información para posteriormente ser analizada, *(CEH V9, Módulo 1)* al encontrar fallos el atacante puede modificar la página web, redireccionarla o acceder a las bases de datos, los ataques más conocidos son de tipo XSS, SQLINJECTION, captura de sesiones, o cookies. Existen diferentes aplicaciones para recolectar información como HTTRACK o encontrar fallos como BURPSUITE o SQLMAP.

4.1.7 PENTESTING EN REDES LAN.

En esta área se realizan diferentes ataques basados en redes locales, donde el "pentester" primero hace una recolección de información, encontrando puertos, clientes, servidores, usuarios de sistema, credenciales con contraseñas débiles, realizar ataques de MITM (Hombre en el medio), SPOOFING (suplantación), acceso a bases de datos o máquinas de usuarios utilizando fallos que no han sido actualizados por su sistema operativo, algunas aplicaciones para realizar esta verificación son: "NMAP, NETDISCOVER, METASPLOIT, CRUNCH, SEARCHSPLOIT, ARMITAGE, DRIFNET, MITM PROXY Y WIRESHARK"[18].

4.1.8 PENTESTING EN REDES WLAN.

El pentester realiza diferentes tipos de ataques al router que presta el servicio de WIFI, primero recolecta información acerca del punto de acceso, utilizando diferentes aplicaciones para probar la seguridad en las contraseñas *(CEH Certified Ethical Hacker Bundle, Third Edition, Junio 24, 2017 de Matt Walker)*, tales como el pin WPS para ser crackeado y obtener la contraseña de red inalámbrica, si su seguridad es efectiva, realiza un ataque por diccionario con un patrones de letras o números, finalmente realiza un ataque de phishing donde el pentester bloquea el router, precediendo a crear otro punto

de acceso idéntico a la red inalámbrica y un servidor para recibir la información ingresada por el cliente, algunas de las aplicaciones más comunes para realizar este ataque son: CRUNCH, JHON, WIFITE, PIXIEWPS, REAVER , AIRCRACK, MANA WIRELESS TOOLKIT, WIFIPHISHER[18].

4.1.9 PENTESTING BASES DE DATOS.

Un pentester realiza ataques a las bases de datos, por web con aplicaciones como SQLMAP o SQLNINJA, donde el pentester puede realizar ataques de tipo inyección, alterando la información en las bases de datos, otros ataques son la fuerza bruta a contraseñas.

4.1.10 SEGURIDAD INFORMÁTICA.

La norma ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener la seguridad de un sistema de información en el contexto de la organización.

4.1.11 REPORTE DE VULNERABILIDADES IDENTIFICADAS.

El reporte debe contener todo lo encontrado que puedan crear un gran impacto en la seguridad, así no haya sido explotado.

Algunos de los dispositivos que entran en este reporte son:

- Configuraciones en el firewall que permitan accesos no autorizados
- Obtención de credenciales mediante aplicaciones web.

4.1.12 RETENCIÓN DE EVIDENCIA.

Se considera toda la información que soporta el test de penetración, se debe seguir un sistema para procesar la información de forma segura y almacenar la evidencia.

4.1.13. HERRAMIENTAS PARA REPORTES DE TEST DE PENETRACION.

La intención es proporcionar la herramienta que pueda ser utilizada por los pentester para rápidamente determinar la profundidad de las pruebas y la calidad de los informes basado en el acuerdo contractual entre la organización y el experto en la materia.

4.1.14 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI).

Un SGSI es la abreviatura para sistema de gestión de seguridad de la información, representado en ingles con la abreviatura ISMS que hace referencia a Información Security Management System.

En el contexto de este documento se refiere a información al conjunto de datos de forma ordenada para el control de procesos y que tiene valor en una compañía. La Seguridad de la Información es muy amplia, por lo que no es sólo aplicar técnicas sino llevar una alta responsabilidad con la dirección de la compañía.

Los riesgos al realizar las diferentes transacciones son hoy en día más delicados en lo que concierne a la Seguridad de la Información. El abanico de vulnerabilidades de este tipo de riesgo es extenso, en colaboración con el comportamiento y manipulación, el recelo al cambio, la cultura empresarial, el modo de comunicarse y otros.

---

[18]. Kali Linux, Kali Linux Tools Listing (2017), Herramientas incluidas en el sistema operativo para análisis de vulnerabilidades. [Sitio web], [Consulta: 8 de febrero 2018]. Disponible en Internet: https://tools.kali.org/tools-listing.

4.1.15 SEGURIDAD DE LA INFORMACIÓN.

El propósito de la seguridad de la información es proteger la información no permitiendo el acceso no autorizado, la divulgación, el uso o la interrupción de la misma.
Según la norma ISO/IEC 27001:2013, radica en la preservación de su confidencialidad, integridad y disponibilidad, como también los mecanismos utilizados en su tratamiento.

4.1.16 CONFIDENCIALIDAD.

La información no está disponible para terceros ni es revelada a cualquier tipo de terceros como personas u organizaciones.

4.1.17 INTEGRIDAD.

Se controla la información verificando que los datos sean válidos y ordenados en cada uno de los métodos para tratarla.

4.1.18 DISPONIBILIDAD.

Garantizar al usuario que la información ofrecida por la compañía sea presentada en el momento requerido.

4.1.19 CICLO PHVA.

Permite monitorear y establecer el proceso de planeación de un sistema de gestión, con el modelo P.H.V.A. (planear, hacer, verificar y actuar) se logra planear, tomar decisiones, analizar y definir acciones de resultados obtenidos.
En el ciclo PHVA se mencionan 4 fases que consisten en:

- Planear: En esta fase se establecen las metas y los métodos.
- Hacer: Se realiza la recolección de la información.
- Verificar: Se procede a evaluar los resultados y se toman acciones a problemas sin resolver.
- Actuar: Se efectúan las acciones correctivas para el desarrollo de las metas.

4.1.20 MAGERIT.

Permite conocer que tanto están siendo poco valorados activos de alto valor. Detectar los riesgos al que están sometidos los activos de la compañía es importante para realizar una adecuada gestión.

MAGERIT está dividida en 4 fases:

- Planificación.
- Análisis e identificación de los riesgos.
- Gestión y Tratamiento de los riesgos.
- Definir las Salvaguardas.

La metodología MAGERIT permite realizar una cuantificación de los activos y calcular el valor de acuerdo al nivel de impacto que pueda ocasionar la perdida en la compañía si se materializa. La valoración de los activos puede realizarse de forma cuantitativa o cualitativa de acuerdo a la siguiente escala:

- Muy Alto (MA)
- Alto (A)
- Medio (M)
- Bajo (B)
- Muy bajo (MB)

Con MAGERIT se logra realizar una excelente gestión y análisis de riesgos, clasificando los activos, identificando los riesgos y las amenazas estableciendo un nivel de impacto donde se da soluciones implementando salvaguardas para contrarrestar los daños que se puedan ocasionar en cualquier momento.

4.1.21 SEGURIDAD DE RED.

La mayoría de los sistemas conectados en la actualidad a Internet son vulnerables a los usuarios que intentan conseguir acceso sin estar autorizados.

Los usuarios ajenos a la red de la compañía pueden intentar acceder directamente configurando una conexión ilegal que intercepte las comunicaciones de los usuarios válidos y autorizados de la red logrando obtener datos de forma remota.

Para contrarrestar estos ataques y protegerse de estos ataques existen los cortafuegos y el cifrado.

4.1.22 ADMINISTRACION DE SISTEMAS DE ARCHIVOS.

Los archivos residen en dispositivos físicos como son las unidades de disco duro, los CD-ROM o dispositivos de almacenamiento externo entre otros, estos archivos están organizados en un sistema de archivos. Para acceder a los archivos en un dispositivo, se asocia su sistema de archivos a un directorio especificado, lo que se conoce como montar un sistema de archivos. Los sistemas de archivo general se usan para hacer copias de seguridad o para incrustarlo dentro de paquetes para ser transferidos vía internet o ser descargados vía FTP

4.2 MARCO CONCEPTUAL

4.2.1 ACTIVO.

Conjunto de los bienes que posee una compañía, los cuales permiten que la actividad de la empresa se desarrolle y de los cuales se puede obtener beneficios y no solo económicos.

4.2.2 AMENAZA INFORMÁTICA.

Evento o persona que tiene la capacidad de causar daño a un sistema, puede presentarse como un robo, destrucción de información, divulgación de datos privados, caídas de sistema, etc.

4.2.3 IMPACTO.

Resultados de la ejecución de una amenaza que afectan el funcionamiento de los procesos de una compañía.

4.2.4 RIESGO.

Probabilidad que una de las amenazas se lleve a cabo y pueda impactar de forma negativa.

4.2.5 VULNERABILIDAD.

Punto crítico de un sistema con fallos que puede ser usado para realizar actividades maliciosas.

4.2.6 ATAQUE.

Acción que realiza una persona utilizando diferentes herramientas para causar daño a un sistema.

4.2.7 DESASTRE.

Evento que produce destrucción o daños en la infraestructura.

4.2.8 IDS (INTRUSION DETECTION SYSTEM).

“Un sistema de detección de intrusiones (IDS) examina la actividad del sistema o de la red para encontrar posibles intrusiones o ataques. Los sistemas de detección de intrusos están basados en la red o basado en el host; los vendedores solo están comenzando a integrar las dos tecnologías” (*ICSA labs, 2004, p. 14)*. un ejemplo de ids es SNORT.

4.2.9 IPS (INTRUSION PREVENTION SYSTEM).

Conocido como sistema de prevención de intrusos, son aplicaciones que controlan la red para evitar ataques o accesos no permitidos, estas aplicaciones se basan en configuraciones, políticas, firmas y filtrando o bloqueando actividades no comunes en la red inalámbrica o local, una aplicación IPS es Fragroute. (Todd Lammle, 2015, SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System)[19].

---

[19] BARRACUDA. Intrusion Prevention System. [Sitio web], [Consulta: 14 de abril 2018]. Disponible en: https://www.barracuda.com/glossary/intrusion-prevention-system.

4.2.10 ATAQUES WEB.

Acción que se ejecuta contra una aplicación que contiene errores de programación o configuración de servidores incorrecta.

4.2.11 FORMULACIÓN DE REDES SEGURAS.

Existe gran variedad para la implementación de una red segura, se debe contar con puntos básicos, como lo son el uso de firewalls, servidores proxy, credenciales con contraseñas seguras, realizar las actualizaciones del sistema operativo, aplicaciones para detección de anomalías, aplicar políticas en cuanto al uso de memorias, dispositivos externos, almacenamiento de información, contraseñas, descarga de archivos y responsabilidad en los usuarios.

4.2.12 ANÁLISIS DE BOTNETS.

Es una técnica para analizar el tráfico de la red, donde se hace un análisis de paquetes, direcciones ip, utilización de puertos, protocolos, para encontrar un comportamiento no habitual en el sistema, existen protocolos para realizar estos análisis como lo es el Netflow[2], que intenta identificar un patrón en la comunicación de los dispositivos que constituye la red, una aplicación para realizar ataques botnets de denegación de servicio es UFONET.

4.2.13 VPN.

“Una forma de abordar problemas de transmisión de datos es crear redes privadas y virtuales dentro de la estructura de Internet. Estas redes virtuales son creadas mediante el uso de túneles, autenticación y encriptación para proporcionar una línea arrendada virtual entre redes empresariales” *(Jon C. Snader. 2006, VPNs Illustrated: Tunnels, VPNs, and IPsec: Tunnels, VPNs, and IPsec 1st Edition, p.15).*

4.2.14 WEB TROJANS.

son programas maliciosos que aparecen sobre las pantallas de inicio de sesión para obtener credenciales privadas. Cuando un Web Trojan se instala en una máquina, el troyano espera de manera silenciosa a que un cliente o usuario visite un sitio web en

particular. Cuando el usuario visita el respectivo sitio, el Web Trojan ubica una ventana o capa de inicio de sesión falsa sobre la ventana de inicio de sesión real del sitio

4.2.15 CLICKJACKING.

Este tipo de ataque se basa en engañar al usuario por medio del navegador web en modo GUI interponiendo una capa transparente sobre hipervínculos que son pulsados sin que el usuario se percate de la acción.

4.2.16 XSS CROSS-SITE SCRIPTING.

Es un ataque contra otros clientes, este método se encuentra en los sitios web que contienen una mezcla de contenido, estilos y código.

4.2.17 CROSS-SITE REQUEST FORGERY (CSRF).

Este tipo de ataque consiste en forzar a un cliente a ejecutar acciones no deseadas en una aplicación web, este ataque se centra en los cambios de estado de las peticiones web sin obtener los datos ya que el atacante no puede visualizar la respuesta a las solitudes o peticiones.

4.2.18 CORTAFUEGOS.

Impide cualquier intento directo de acceso sin autorización.

4.2.19 CIFRADO.

Protege las transmisiones de usuarios remotos autorizados.

4.2.20 SHELL SEGURA.

Cifra cualquier comunicación entre le usuario remoto y un sistema de su red empleando dos claves: una clave pública y otra privada. La clave pública se usa para cifrar datos, mientras que la clave privada los descifra[20].

4.2.21 SERVIDOR.

Es un demonio que está ejecutándose simultáneamente a los demás programas, a la espera de peticiones para los servicios que ofrece para los usuarios de su sistema como también los usuarios remotos conectados a su sistema a través de una red[21].

---

[20] PETERSON, Richard. Linux Manual de referencia, Segunda Edición, Osborne McGraw-Hill, Aravaca Madrid, 2000, P.1086. ISBN: 0-07-212940-9

[21] BARRACUDA. Barracuda Essentials. [Sitio web]. [Consulta: 20 de febrero 2018]. Disponible en: https://www.barracuda.com/products/essentials.

4.3 MARCO CONTEXTUAL

4.3.1 PRESENTACIÓN DE LA EMPRESA –ESSENSALE S.A.S.

La empresa Essensale S.A.S dedicada al comercio al por menor de productos farmacéuticos y medicinales cosméticos y artículos de tocador en establecimientos especializados, con sede en Santiago de Cali incluida en las 500 empresas más importantes del Valle del cauca, contando con una amplia gama de productos que van desde el cuidado personal como la perfumería, cremas, splash, hasta elementos para el hogar como ambientadores y mejoras de interiores.

Essensale maneja la marca SENTHIA la cual es una marca contratipos de perfumería líder en Colombia, que reinventó en 2003 la cultura del perfume con un innovador concepto de cuidado personal**:** 'Hágalo usted mismo'**,** una visión en donde tú elaboras y elijes como quieres llevar tu fragancia[22].

La sede principal se encuentra ubicada en el norte de Cali, CALLE 41 6 16 COMPLEJO BODEGA LA ESMERALDA BOD 1, CALI, VALLE

ESSENSALE S.A.S. también cuenta a la fecha 45 franquiciados que funcionan a nivel nacional.

---

[22] SENTHIA. Nosotros – Mundo Senthia [En línea], Cali: Essensale [Consulta: 20 de febrero 2018]. Disponible en: https://www.senthia.com/nosotros/

Figura 1. Essensale Senthia

Fuente: Essensale, Senthia. (2018). Fotografía de Bodega principal. [Figura]. Recuperado de https://www.google.com/maps/

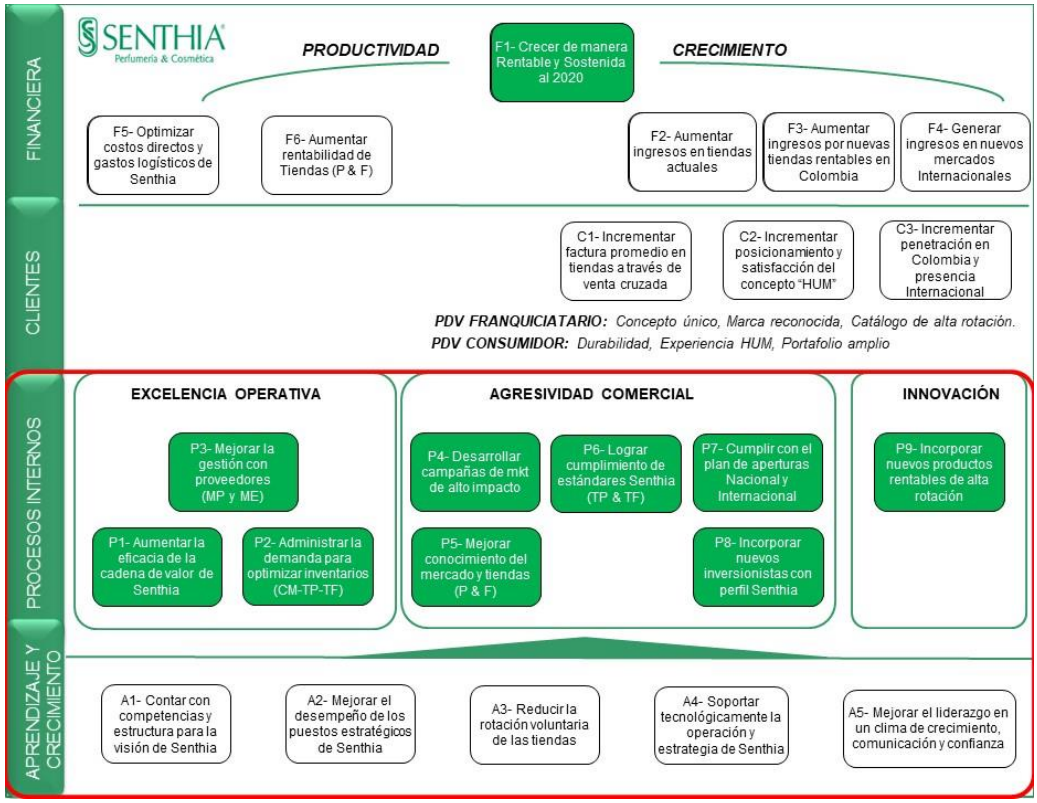
4.3.2 MISIÓN.

SENTHIA siempre está en la búsqueda de nuevas tendencias en perfumería y cuidado personal, con el fin que encuentres en cada visita una fórmula diferente que te acompañe en todo momento y en cualquier ocasión para que logres eso que tanto anhelas

4.3.3 VISIÓN.

Lograr establecer e incrementar desde el 2018 la presencia en 65 municipios colombianos a través de 197 puntos de venta.

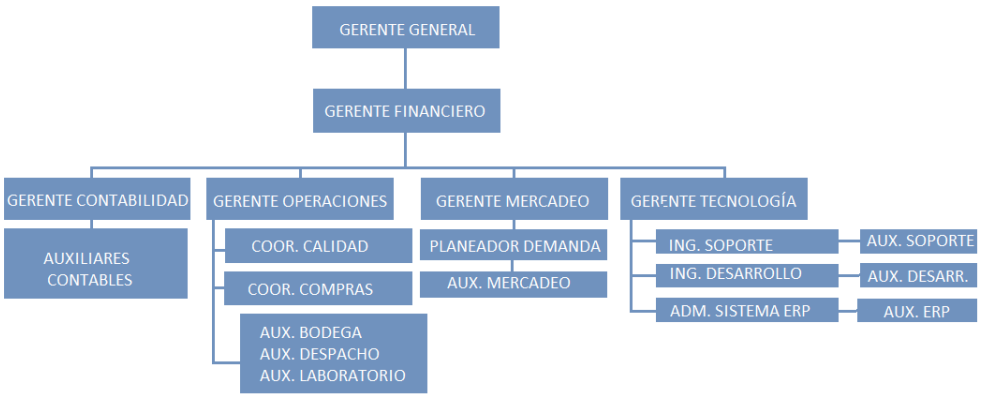
Figura 2. Iniciativas Estratégicas de Senthia para su visión 2021



Fuente: Archivo de SGC de Essensale S.A.S

4.3.4 ORGANIGRAMA.

Figura 3. Organigrama ESSENSALE S.A.S



Fuente. Archivo de SGC de Essensale S.A.S

4.3.5 ESTRUCTURA ORGANIZACIONAL.

La empresa ESSENSALE.S.A.S. está constituida por las siguientes áreas:

GERENTE GENERAL. Líder encargada de realizar todas las operaciones en el ámbito legal de la compañía como también velar por el buen el funcionamiento de las áreas recibiendo informes de gerencia.

AREA FINANCIERO. Constituido y liderado por el gerente financiero encargado de proyectar los movimientos de la compañía, cuenta con personal a cargo como auxiliares contables y financieros.

Diseña y Redefine la cadena de valor fortaleciendo la competitividad, representando diferencias operacionales, reduciendo los costos e incrementando la utilidad, a través de la Automatización de la línea de producción para el cumplimiento a la Demanda, desde la planeación estratégica hasta la alineación de la operación de cada uno de los procesos que intervienen.

Tiene como objetivo alinear la cadena de valor a las definiciones de la estrategia de Senthia al 2020 y automatizar las líneas de producción.

AREA GESTIÓN DE OPERACIONES. Gerente encargado de validar los productos a generar en el día, hacer estudios de rotación de ítems, traslados e informes de producción, contando con auxiliares de despacho y laboratorio para la realización de pedidos de inventario y un auxiliar para ingresar la información al sistema ERP.

Define el plan estratégico de compras e identificar las brechas de los proveedores con el fin de afianzar y fortalecer aquellos que están en capacidad de ser aliados en el cumplimiento del crecimiento de la organización.

Tiene como objetivo lograr reducción de costos, aumentando los ahorros, mejorando la rentabilidad, la posición competitiva de la compañía, así como la satisfacción del servicio al cliente.

Etapas:

- Conocer estado actual de los proveedores
- Buscar alternativas de mejora con el mercado actual
- Diseñar el programa de desarrollo de proveedores, creando mecanismos de definición y evaluación de objetivos con proveedores.

- Implementar el programa.

Formaliza la estructura de costos de producción y re - empaque que permita diseñar estrategias de reducción de costos, manteniendo la calidad del producto y priorizar en aquellos componentes que impacten en el costo de la operación. Adicionalmente clasificar aquellos gastos que hacen parte del costo de la operación para conocer realmente el costo de la operación.

AREA DE MERCADEO. El gerente de mercadeo Incrementa el conocimiento de la marca, nuevos productos, al igual que la interacción y participación de clientes y nuevos consumidores a través de estrategias de marketing con el fin de generar engagement, posicionamiento de marca y acción a la compra.

Alcance: Hombres y Mujeres de 25 – 34 años, trabajan o estudian se localizan principalmente en ciudades como Bogotá, Cali, Medellín y/o ciudades cercanas a las nombradas anteriormente, hablan principalmente el idioma español.

Alcance de medios: Medios digitales (redes sociales, Pagina web, Google, YouTube)

AREA DE TECNOLOGÍA. Consolida la Información en una sola Plataforma tecnológica para tener un y control adecuado de la cadena de valor, el coordinador de sistemas o de soporte garantiza tener información actualizada y de fácil acceso a todos los procesos estratégicos de la organización, así mismo se busca tener Integridad y estabilidad en la información de los puntos de venta permitiendo trabajar en línea y en desconectado.

ETAPAS:

1. Negociación y contratación de servicios con proveedor ERP.
2. Alineación de requerimientos del ERP con plan estratégico
3. Diagnostico levantamiento de requisitos, adquisición de HW para automatización de Cadena de Valor, selección y liberación de grupo de trabajo.
4. Capacitación, ambientación, diseño y desarrollo.
5. Pruebas piloto, carga de inventarios iniciales, y corte al nuevo sistema.

El ingeniero de desarrollo establece un único canal de acceso a la información de clientes y colaboradores para mejorar la comunicación y los tiempos de respuesta de los procesos que actualmente se hacen por diferentes medios, alinear los procesos y reportes automatizables del objetivo estratégico en una sola plataforma para facilitar seguimiento

de cumplimiento de metas.

ETAPAS:

1. Levantamiento de reportes y procesos automatizables del plan estratégico (Pedidos, Rolling Forcast, etc), contratación de nuevo ingeniero de desarrollo.
2. Implementación de adecuaciones tecnológicas para soportar el proyecto, adquisición de hosting/dominio para extranet, adquisición de equipos de red y plataformas de administración de red para mejorar seguridad y desempeño de red local en escenario sin Hosting en Data center o negociación con data center.
3. Desarrollo de aplicaciones planeadas según plan estratégico
4. Pruebas piloto, solución de fallas, y lanzamiento de la plataforma a franquiciados.

4.3.6 RECURSOS HUMANOS.

Una de las bases fundamentales para el éxito de un franquiciado SENTHIA y asesores, es su formación. Esta debe de abarcar todos y cada uno de los ámbitos de nuestro concepto de negocio.

El programa de formación comprende todos los aspectos necesarios para triunfar en el negocio SENTHIA, destacando principalmente materias relacionadas con nuestro concepto HUM, gestión comercial, lanzamiento de nuevos productos, técnicas de atención al cliente, gestión y administración de una tienda, imagen corporativa y manejo de la plataforma tecnológica.

ETAPAS:

1. Estructurar un currículo y el programa de capacitaciones o cursos que debe tener un franquiciado o asesor Senthia.
2. Selección y capacitación de formadores SENTHIA
3. Adecuación de plataforma tecnológica para evaluación y seguimiento de capacitaciones. (intranet)
4. Lanzamiento a franquiciados

4.4 MARCO LEGAL

Los profesionales practicantes de seguridad informática generalmente realizan crímenes donde se involucran computadoras en diferentes categorías. Dicho de una forma breve, un delito informático es un delito (o violación de una ley tipificada) que involucra una computadora. El delito podría ser contra la computadora, o la computadora podría haber sido utilizada para lograr el delito. Cada una de las categorías de delitos informáticos conforman el propósito de un ataque y su resultado predeterminado. Se considera que cualquier persona que viole una o más de sus políticas de seguridad es un atacante. Está persona utiliza diferentes técnicas para lograr un objetivo específico. Comprendiendo que el objetivo ayuda a aclarar los diferentes tipos de ataques, detrás del delito informático no hay otra razón que cometer otro delito y su única diferencia son las formas de realizarlo.

Algunos de los tipos de delitos informáticos se presentan a continuación:

Ataques militares y de inteligencia: obtener información secreta y restringida de la policía o fuentes de investigación militar y tecnológica.

- Ataques empresariales: obtener la información confidencial de una organización. Esta podría ser información que es crítica para el funcionamiento de la organización, como una fórmula secreta o información que podría dañar la reputación.
- Ataques financieros: se llevan a cabo para obtener ilegalmente dinero o servicios. Es el tipo de delito informático que más se escucha en las noticias. El objetivo de un ataque financiero podría ser robar números de tarjetas de crédito, aumentar el saldo en una cuenta bancaria o realizar llamadas telefónicas de larga distancia sin costo.
- Ataques terroristas: El propósito de un ataque terrorista es interrumpir la vida normal e inculcar miedo, se utiliza principalmente con fines políticos, religiosos o económicos.
- Ataques de odio: se llevan a cabo para dañar una organización o una persona, como por ejemplo un empleado que ha sido despedido y con la información conocida hacer grandes daños a la compañía.
- Ataques de emoción: son los ataques lanzados solo por diversión. Son por lo general ataques realizados por personas que descargan aplicaciones para atacar sistemas

vulnerables.

Es importante comprender las diferencias entre las categorías de delitos informáticos para saber cómo proteger un sistema y tomar las acciones correctas cuando ocurre un ataque. El tipo y la cantidad de evidencia que deja un atacante a menudo depende de su experiencia.

La norma ISO/IEC 27001:2013 ayuda a las compañías con el cumplimiento de las obligaciones legales a los reglamentos contractuales de seguridad tanto el diseño, desarrollo, y gestión de los Sistemas de Gestión de Seguridad de la Información.

La Ley estatutaria 1266 de 2008 (diciembre 31): 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[22].

---

[22] COLOMBIA. Congreso de la República. LEY ESTATUTARIA 1266 de 2008. [Sitio web], [Consulta: 20 de noviembre 2020] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.

- Ley 1273 de 2009 (enero 05): 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[23].

- Ley 1341 de 2009 (Julio 30): principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro[24].
- Ley estatutaria 1581 de 2012 (octubre 17): se dictan disposiciones generales para la protección de datos personales[25].
- Decreto 1377 de 2013 (junio 27): Protección de Datos, decreto por el cual se reglamenta la Ley 1581 de 2012[26].

---

[23] COLOMBIA. Congreso de la República. LEY 1273 DE 2009. [Sitio web], [Consulta: 20 de noviembre 2020] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

[24] COLOMBIA. Congreso de la República. LEY 1341 de 2009. [Sitio web], [Consulta: 20 de noviembre 2020] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/c-403_2010.html

[25] COLOMBIA. Congreso de la República. LEY ESTATUTARIA 1581 de 2012. [Sitio web], [Consulta: 20 de noviembre 2020] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1918_2018.html

[26] COLOMBIA. Congreso de la República. DECRETO 1377 DE 2013. [Sitio web], [Consulta: 20 de noviembre 2020] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/c-472_2019.html

5 DISEÑO METODOLÓGICO

5.1 DISEÑO METODOLÓGICO.

Tabla 1. Modelo PHVA de un SGSI

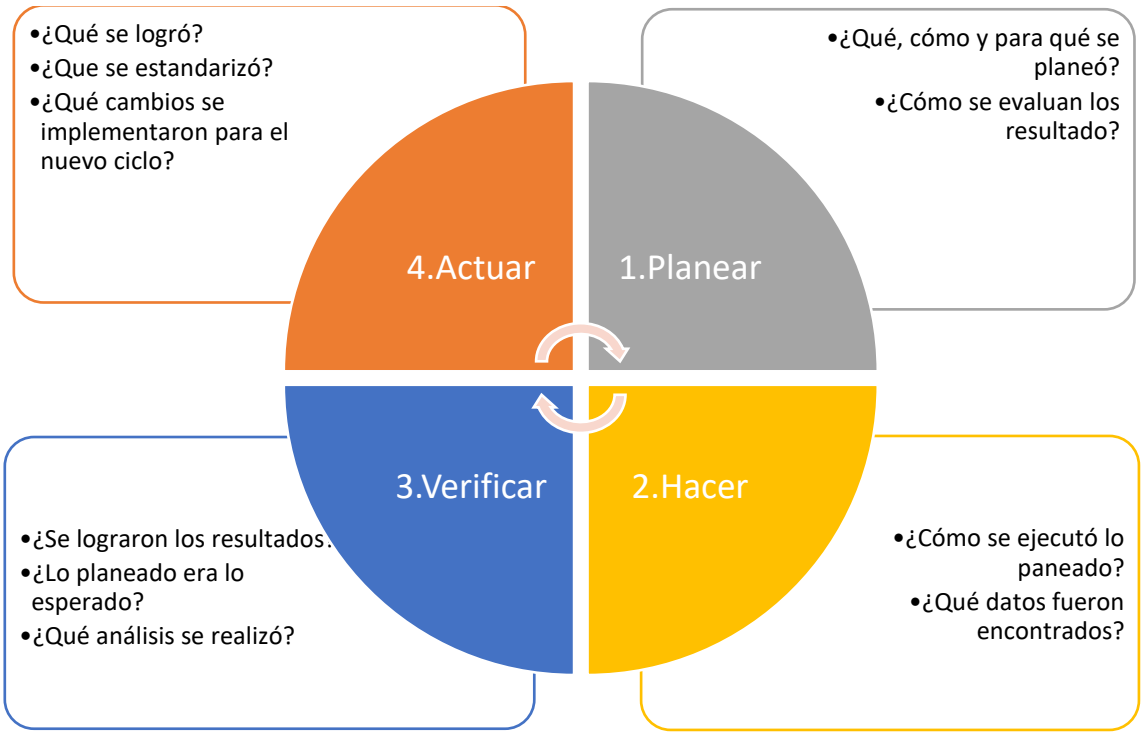
Planificar (Definir el SGSI)	Se inicia en esta etapa estableciendo las políticas, objetivos, y procedimientos para la gestión de los riesgos.
Hacer (implementar el SGSI)	En este nivel se entra a operar la política, procesos y procedimientos del SGSI
Verificar (Realizar seguimiento del SGI)	Se procede a realizar las respectivas evaluaciones de desempeño de la política y los objetivos, se genera un reporte de resultados para la dirección.
Actuar (Mantener el SGI)	Continuar con el uso de acciones correctivas y preventivas obtenidos de las auditorias para la mejora del SGSI.

Fuente: El autor.

La norma ISO9001 especifica que puede aplicarse a todos los procesos la metodología conocida como PHVA (Planificar, Hacer, Verificar, Actuar), como consecuencia de lo anterior se establece una metodología global para implementar los procesos de la norma

ISO27001:2013 para la compañía ESSENSALE SAS, se acoge como metodología el ciclo PHVA (Planificar, Hacer, Verificar, Actuar).

Figura 4. Ciclo PHVA y Desarrollo.



Fuente. El autor

El diseño metodológico adoptado para el diseño del SGSI en ESSENSALE S.A.S está basado en el ciclo PHVA de la Norma ISO27001:2013 en la cual se contextualiza cada uno de sus ciclos y como se desarrollan.

Antes de iniciar las descripciones del ciclo, es necesario que en la compañía identifique el punto donde se va a tomar la decisión de implementar un sistema de gestión por fases, no obstante, esta fase se inicia como una estrategia de la organización donde la dirección halla los beneficios de la implementación de este sistema de gestión donde puede asignar varios responsables como también soluciones a largo plazo.

5.2 MUESTRA POBLACIONAL

Se tomó como grupo experimental 4 áreas de la organización que corresponden a Recursos humanos, Tecnología, Financiero y Mercadeo, siendo áreas de alto riesgo para la compañía ESSENASLE S.A.S, se realizó una encuesta para determinar posibles problemas tomando una muestra aleatoria.

El margen de error que se desea obtener en la encuesta es de 5%, con un nivel de confianza de 80%

Fórmula Muestra población

$$n = \frac{z^2 * p * q * N}{e^2 * (N-1) + z^2 * p * q}$$

Fuente: Normas APA (http://www.normaspa.net)[27]

z: nivel de confianza que se asigne, este indica la probabilidad de que los resultados sean verdaderos o falsos.
n: Tamaño de muestra, cantidad representativa de población.
e: diferencia que puede obtenerse entre los resultados obtenidos con la muestra.
p: Probabilidad a favor.
q: Es la probabilidad en contra, en estos casos se coloca 0,5 para ambos.
N: Población o universo.

[27] NORMAS APA. Fórmula para calcular la muestra de una población. [Sitio web],[Consultado el 20 Noviembre 2020] Disponible en: http://normasapa.net/formula-muestra-poblacion/

Tabla 2. Los valores z más utilizados y sus niveles de confianza

Z	97,5%	85%	80%	75%
Nivel de confianza	2,24	1,44	1,28	1,15

Fuente: Normasapa.net

Calculando Muestra poblacional

$$n = \frac{1.15^2 * 0.05 * 0.95 * 4}{0.05^2 * (4-1) + 1.15^2 * 0.05 * 0.95} = \frac{0.251275}{0.07031} = 3.5733$$

Fuente: El autor

La muestra poblacional da como resultado 4 individuos que están refiriéndose a los coordinadores o jefes de las áreas seleccionadas como críticas en la compañía.

Al presente ESSENSALE.S.A.S cuenta con 60 empleados y se encuentra dividida en 7 áreas de trabajo, de las cuales se seleccionaron como muestra poblacional las 4 áreas con mayor movimiento y complejidad en sus procesos de acuerdo al número de casos generados en su plataforma de servicio al cliente y actividades económicas.

5.3. INSTRUMENTOS.

Se elaboró una encuesta escrita para recolección de información la cual se aplicó a una muestra poblacional de 4 colaboradores jefes de área de la compañía ESSENSALE S.A.S donde se ha detectado mayor complejidad en los procesos.

Tabla 3. Muestra poblacional

Área	Solicitudes
Tecnología	20
Contabilidad	12
Financiero	10
Recursos humanos	10

Mercadeo	20
Control de calidad	30
Operaciones/Despacho	25

Fuente. Archivo SGD de Essensale S.A.S.

5.3.1. APLICACIÓN DEL INSTRUMENTO.

Las encuestas se aplicaron del 10 de febrero al 10 de julio de 2018, se realizó a los jefes de las 4 áreas de mayor actividad en la organización, se tomó un libre de forma virtual, enviada como enlace. para la aplicación del instrumento.

5.4 ÁREA DE INVESTIGACIÓN.

El desarrollo del proyecto se llevará a cabo en las bodegas de la compañía Essensale S.A.S ubicada en la Calle 41 # 6-16, Bodega 8 Parque Industrial La Esmeralda Barrio Las Delicias, Cali, Valle del Cauca.

5.5 ALCANCE DEL PROYECTO

El estudio estará enfocado en las instalaciones de ESSENSALE S.A.S, Bodega 8 Parque Industrial La Esmeralda.

Siendo retroalimentado con entrevistas, encuestas, y pruebas en ambientes controlados con el propósito de determinar riesgos y amenazas.

Las aplicaciones de políticas, controles y procedimientos para los procesos establecidos en el Diseño del Sistema de Gestión de Seguridad de la Información para ESSENSALE.S.A.S. contribuyen a contrarrestar los riesgos y amenazas que afecten los activos de la compañía.

Se formula para la compañía ESSENSALE S.A.S el DOCUMENTO POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN el cual se encuentra basado en la Norma ISO/IEC 27001:2013 y presenta las siguientes políticas:

- Gestión por los activos.
- Seguridad del talento humano.
- Gestión de las comunicaciones y operaciones.
- Control de acceso.
- Mantenimiento del sistema de información.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad del negocio.
- Cumplimiento.

5.6 TIPO DE INVESTIGACIÓN

Para el desarrollo del proyecto la investigación que se planea llevar a cabo corresponde a una investigación de tipo aplicada, se realizará un análisis inicial de la situación actual de la seguridad de los activos informáticos de la compañía ESSENSALE S.A.S. a partir de procesos controlados para lograr los objetivos propuestos y generar la documentación referente, es necesario realizar las actividades presentadas en el estándar ISO/IEC 27001:2013 asociadas a la fase de diseño del Sistema de Gestión de Seguridad de la Información.

5.7 METODOLOGÍA DE DESARROLLO

5.7.1 METODOLOGÍA PARA EL ANÁLISIS DE RIESGOS.

La metodología MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, fue desarrollada por el Consejo superior de Administración Electrónica de España, enfocada a las administraciones públicas, para minimizar los riesgos al implementar nuevas tecnologías de información, actualmente se encuentra en la versión 3 que cuenta con diferentes técnicas y ejemplos de cómo realizar el análisis de riesgos.

5.7.2 METODOLOGÍA PARA EL DESARROLLO DEL DISEÑO DEL SGSI.

Desde el departamento de sistemas se iniciará una visita a cada área con el fin de realizar una evaluación de la seguridad de la información en ESSENSALE S.A.S.

El departamento de desarrollo se encarga de validar la información y es el representante del presente proyecto que posee la libertad para realizar las actividades.

- Definir el alcance del SGSI.
- Definir las políticas de seguridad.
- Definir la metodología para el análisis y la gestión de riesgos.
- Identificar los riesgos y las amenazas.
- Redactar la Declaración de Aplicabilidad de controles.
- Desarrollar el Plan de Tratamiento de Riesgos.

- Controlar y depurar las incidencias.
- Documentar la información.

5.7.3 RESULTADOS ESPERADOS.

La propuesta de implementación del SGSI (Sistema de Gestión de Seguridad de la Información) para la compañía ESSENSALE S.A.S, contendrá los siguientes aspectos:

- Análisis y estado actual de la seguridad de la Información de ESSENSALE S.A.S.
- Desarrollo de la fase de planeación del ciclo PHVA para la formalización del sistema de gestión de seguridad.
- Política general de la seguridad de la información para la compañía ESSENSALE S.A.S.
- Actas de compromiso firmado por parte de los directivos de la empresa ESSENSALE S.A.S donde exprese el apoyo a la implementación del Sistema de gestión de seguridad e la información.

5.7.4 CRONOGRAMA DE ACTIVIDADES.

Tomando el resultado del análisis de los objetivos específicos definidos para el proyecto aplicado a la compañía ESSENSALE S.A.S., se establecieron una serie de actividades que corresponden a tareas prioritarias que ejercerán para el logro los objetivos.

Tabla 4. Cronograma De Actividades

CRONOGRAMA DE ACTIVIDADES
NOMBRE DEL PROYECTO: DISEÑO DE UN SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001:2013 PARA LA COMPAÑÍA ESSENSALE S.A.S.

INTEGRANTES: Cesar Daniel Rincón Brito	**LOCALIDAD**: Essensale S.A.S Cali Colombia

SEMANA / ACTIVIDAD	Mes 1 / 2018				Mes 2 /2018				Mes 3 / 2018				Mes 4 /2018			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Recolectar información	x	x	x													
Generar documentos requeridos			x													
Identificar y valorar los activos				x												
Identificar riesgos y amenazas					x	x										
Definir documento Soa						x	x									
Definir políticas de seguridad							x	x								
Elaborar controles									x	x						
Desarrollar gestion riesgos											x	x				
Realizar pruebas en ambientes controlados													x	x		
Elaborar plan de acción														x	x	
Definir plan de continuidad															x	x

Fuente: El autor.

5.8 RECURSOS DISPONIBLES

5.8.1 RECURSOS MATERIALES.

Los materiales utilizados durante el avance del proyecto fueron:

- Papelería.
- Lapiceros.
- Llamadas telefónicas.
- Carpetas.
- Transporte.
- Revistas.
- Fotografías.

5.8.2 RECURSOS INSTITUCIONALES

Universidad Nacional Abierta y a Distancia. Universidad pública. Su sede principal se encuentra la ciudad de Bogotá D.C. y su sede referente a este proyecto la UDR CALI ubicada en la Av. Roosvelt # 36 – 60 Cali, Valle del cauca.

5.8.3 RECURSOS HUMANOS.

EMPLEADOS. Para el levantamiento de información se utilizaron las experiencias de los colaboradores de la compañía, para conocer el estado de la seguridad de la información en la sede principal.

Las áreas que participaron en el proyecto fueron

- RECURSOS HUMANOS.
- CONTABILIDAD
- MERCADEO
- TECNOLOGIA Y SOPORTE

ASESORES DEL PROYECTO.

las cada una de las fases del proyecto, la UNAD Universidad Nacional Abierta a Distancia, situó a docentes como asesores metodológicos, que dieron las pautas necesarias en cada curso para la consolidación de este.

Docente del curso Proyecto de Seguridad I: Fernando Zambrano Hernández. Ingeniero de Sistemas. Especialista en Magister en Seguridad Informática.

Docente del curso Proyecto de Seguridad II: Juan José Cruz. Ingeniero de Sistemas de la Universidad Cooperativa de Colombia. Especialista en Seguridad Informática de la Universidad Piloto de Colombia.

Director de Proyecto de grado: J Eduard C Salamanca. Ingeniero de sistemas de la Universidad INCCA de Colombia, Especialista en redes de alta velocidad y distribuida de la misma universidad, Magister en seguridad informática de la Universidad Internacional de la Rioja, y auditor interno ISO 27001:2013.

5.8.4 RECURSOS TECNOLÓGICOS.

- Portátil
- Acceso a internet
- Software Microsoft Office 2016
- Sistemas Operativos Windows 7/10
- Sistema Operativo Linux Debian
- Adaptadores de Red Alfa Network
- Dispositivos USB
- Hardware Arduino
- Dispositivo móvil Samsung S7 modelo Exynos
- Routers Lynksys 2.2
- Software Threat Analysis and Modeling Tool 2016

5.8.5 RECURSOS FINANCIEROS.

Tabla 5. Recursos financieros

RECURSO	DESCRIPCIÓN	PRESUPUESTO

Hardware	Portátiles, Dispositivos USB, hardware Arduino, adaptadores red, routers, dispositivos móviles	$ 5’000.000
Licencias de Software	Office, Windows, Threat Analysis and Modeling Toool	$ 300000
Viajes y salidas de campo	Desplazamientos	$100.000
Capacitaciones	Cursos ISO 27001, Administración de servidores Linux, Metodología OWASP	$ 500.000
Proveedores	Servicios de internet, telefonía.	$ 200.000
Ingeniero de proyecto	Desarrollador de proyecto	$3.000.000
Gasto General	Otros Gastos	$1.000.000
Total		$ 10.600.000

Fuente: El autor.

6. DESARROLLO DEL PROYECTO

6.1 CONTROLES DE SEGURIDAD.

Los controles son importantes para anticipar fallos, corregir errores o cualquier tipo de inconveniente que puedan afectar la operación. Con la aplicabilidad del estándar ISO 27001:2013, para llevarlo a cabo se utilizó el ciclo PHVA, enfocado a la ejecución de procesos y mejoras en el Sistema de Gestión de Seguridad de la Información donde se busca cumplir con los pilares fundamentales de la seguridad de la información (integridad, confidencialidad y disponibilidad) en la compañía ESSENSALE S.A.S.

Para lograr el desarrollo y cumplimiento de cada una de las reglas establecidas, se definieron mecanismos de control para contrarrestar el impacto de las amenazas y vulnerabilidades que causaran grandes pérdidas o problemas en la operación a la compañía ESSENSALE S.A.S, para ello se definieron los siguientes dominios de la norma ISO 27001:2013 [28]

- A.5 Políticas de seguridad.
- A.6 Organización de la seguridad de la información.
- A.7 Seguridad en los RRHH (Recursos Humanos)
- A.8 Gestión de Activos.

---

[28] ISO/IEC portal de ISO 27001:2013 en español. [Sitio web], [consulta: el 17 de junio 2020]. Disponible en: https://www.iso27000.es/iso27002.html

- A.9 Control de acceso.
- A.10 Criptografía.
- A.11 Seguridad física y ambiental.
- A.12 Operaciones de seguridad.
- A.13 Seguridad de las comunicaciones.
- A.14 Sistemas de adquisición, desarrollo y mantenimiento.
- A.15 Relaciones con los proveedores.

- A.16 Gestión de incidentes.
- A.17 Continuidad de negocio.
- A.18 Cumplimiento.

Con la declaración de aplicabilidad se procede a verificar si los objetivos de control y los controles se encuentran implementados y en operación, controles que sean obsoletos, como también justificar por qué algunas configuraciones han sido eliminadas y se define como se va a implementar cada uno de los sistemas de seguridad de la información donde relaciona la calificación el plan de tratamiento de riesgos.

Se han tenido en cuenta los 114 controles del Anexo A de la norma ISO 27001:2013, las políticas y procedimientos de la seguridad de la información, la evaluación de los riesgos, tratamiento y sus respectivos informes, no obstante, después de identificados los riesgos la declaración de aplicabilidad esta permite identificar el mínimo de controles para validar si cada control es aplicable.

6.2 DECLARACION DE APLICABILIDAD - SOA

En la compañía ESSENSALE S.A.S., es necesario que se desarrolle la declaración de aplicabilidad SOA definiendo los controles de seguridad que sirvan como una mejora para la protección de la información y los activos. La declaración de aplicabilidad SOA establece una serie de controles de seguridad en el estándar ISO/IEC 27001:2013 del Anexo A, la cual cuenta con un total de 114 controles de los cuales 14 son de dominio y 35 objetivos de control.

6.2 MODELO - SOA

El modelo de Declaración de Aplicabilidad (SOA) estableces los controles seleccionados, las amenazas y vulnerabilidades del Anexo A de la Norma ISO 27001:2013 para el diseño del SGSI (Sistema de Gestión de Seguridad de la Información) en ESSENSALE S.A.S, presentan las siguientes relaciones presentadas en la TABLA 6:

Tabla 6. Selección de controles

L	Requerimiento Obligatorio	De carácter obligatorio para la compañía, de no cumplir con las normas incurrirá en sanciones.
O	Obligación contractual	Contratos que la compañía debe cumplir con los colaboradores o entidades.
N	Requerimiento de negocio	Requerimientos que dependiendo de las actividades deben realizarse.
R	resultado de la evaluación de riesgos	Vulnerabilidades o amenazas encontradas en el análisis de riesgos.

Fuente: El autor

Las 4 estrategias definidas para abarcar los riesgos y las amenazas se definen a continuación en la siguiente Tabla:

Tabla 7. Estrategias de riesgos y amenazas

EXCLUIR/ELIMINAR	El control no tiene aplicabilidad y se descarta
TRANSFERIR/COMPARTIR	Se busca y asigna la responsabilidad a un tercero para dar solución.
ASUMIR/ACEPTAR	La dirección verifica el riesgo y ejecuta las decisiones.
MITIGAR/MEJORAR	Se gestionan y documentan salvaguardas para contrarrestar los riesgos y amenazas.

Fuente: El autor

.

Se desarrolló la matriz de declaración de aplicabilidad establecidos en el estándar ISO/IEC 27001 versión 2013 del Anexo M donde se busca extraer los controles y los objetivos que se consideren necesarios de implementar para contrarrestar las amenazas y vulnerabilidades identificadas con el fin de garantizar la seguridad de la información de la compañía ESSENSALE S.A.S.

La declaración de aplicabilidad SOA basada en los riesgos cuenta con la siguiente información:

- Dominio: Hace referencia al control de acuerdo al anexo A de la Norma ISO/IEC 27001:2013.
- Controles ISO/IEC 27001:2013: Identificación del nombre del control
- Aplicabilidad: Se valida si es aplicable o no a la compañía Essensale.
- Justificación: Razón por la cuál es control debe ser aplicado o no.
- Objetivo del Control: Finalidad para verificar la seguridad de la información.
- Estado del control: Si el control es aplicado y cuenta con la suficiente información y actividad para llegar a su objetivo.

7. DIAGNÓSTICO DEL ESTADO ACTUAL

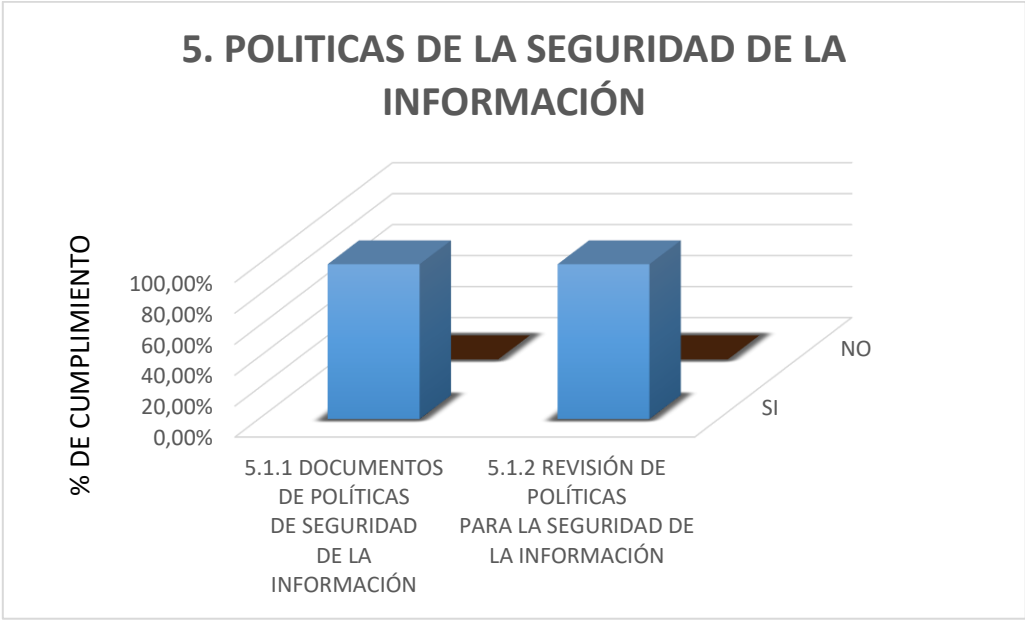
Para conocer la situación actual en materia de seguridad de la información en la empresa ESSENSALE.S.A.S y realizar las mejoras adecuadas se realizaron visitas a las áreas, entrevistas con el personal encargado y encuestas, con el objetivo encontrar todos los elementos necesarios para el desarrollo de la investigación se realizó una lista de chequeo para verificar el cumplimiento de cada uno de los controles establecidos en la norma ISO 27002:2013.

7.1 RESULTADOS DE LA LISTA DE CHEQUEO POR DOMINIO.

Conforme a la lista de chequeo del Anexo G, aplicada a ESSENSALE S.A.S. donde se evaluaron los 114 controles comprendidos dentro de la norma ISO 27002:2013, se ejecutará un estudio del nivel de cumplimiento de cada control y su respectivo dominio.

7.1.1 A.5 DOMINIO: POLÍTICAS DE SEGURIDAD.

Figura 5. Políticas de la seguridad de la información.



Fuente: El autor

De acuerdo al análisis de la lista de chequeo, se pudo evidenciar que la compañía cuenta con un nivel moderado en temas de seguridad de la información, se detectaron algunas falencias en la definición de políticas de seguridad y manejo de activos.

7.1.2 A.6 DOMINIO: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Figura 6. Organización de la seguridad de la información.

Fuente: El autor

El dominio 6 hace referencia a la organización de la Seguridad de la Información, basado en la información recogida de las encuestas y las lista de chequeo para el desempeño de los controles de la ISO 27002:2013, se puede afirmar que, en ESSENSALE S.A.S las responsabilidades de seguridad de la información están asignadas en gran parte al coordinador de sistemas, no obstante el coordinador de desarrollo cuenta con responsabilidades para la seguridad de la información en las aplicaciones de escritorio y aplicaciones web que se utilizan en la compañía. Por lo tanto, el riesgo prevalece en que la forma de organizar esta información sea de conocimiento individual tanto para la administración de los activos como los desarrollos.

Los colaboradores en algunas ocasiones realizan trabajo remoto y no se cuenta con políticas de uso para las redes privadas o el transporte de los activos.

7.1.3 A.7 DOMINIO: SEGURIDAD EN LOS RRHH (RECURSOS HUMANOS).

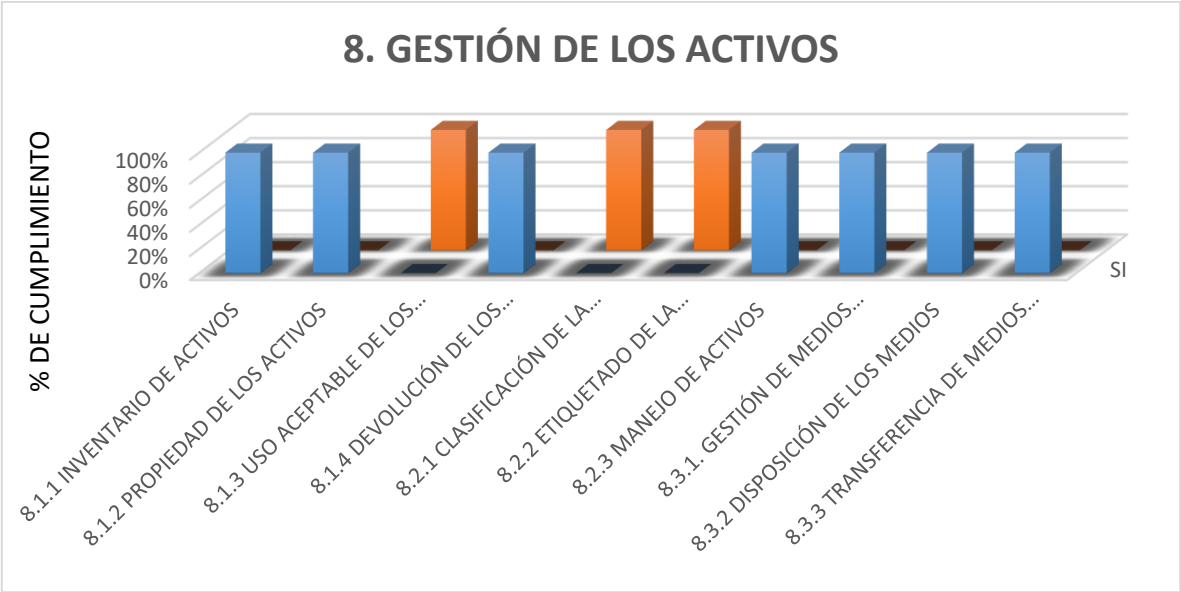
Figura 7. Seguridad de los RRHH.

Fuente: El autor

Con base al análisis de la lista de chequeo relacionado al dominio 7, Seguridad de los recursos humanos, demuestra que existe un buen manejo para la contratación de personal contando con herramientas para la búsqueda de historiales públicos y en algunos casos terceros para contratar, todo esto demostrando que el personal contratado no presenta problemas de tipo judicial o pendientes con el estado u otras entidades.

7.1.4 A.8 DOMINIO: GESTIÓN DE ACTIVOS

Figura 8. Gestión de los activos.



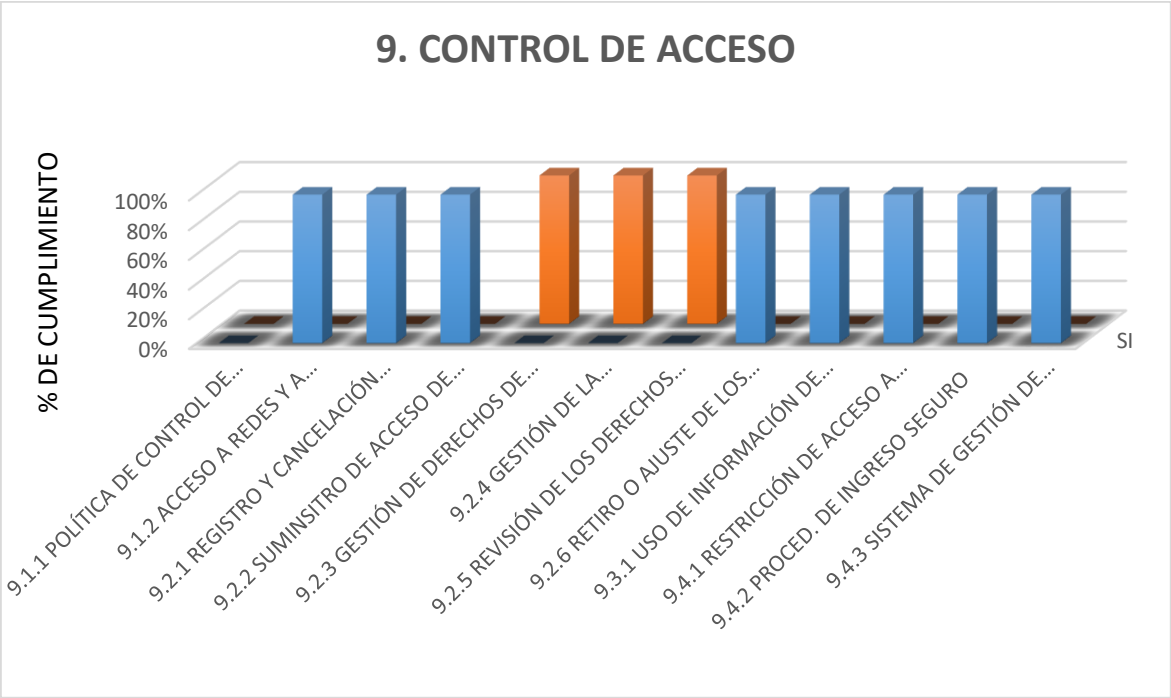
Fuente: Autor.

La gestión de los activos en el dominio 8 la compañía ESSENSALE S.A.S cuenta con formatos diseñados para el registro de movimientos de activos, estos formatos cuentan con información de diferentes tipos, para activos a dar de baja, activos a ser trasladados y la asignación para el colaborador, donde este recibe el acta verificada por el coordinador del área de sistemas, haciendo entrega de cada elemento y sus respectivas instalaciones.

No existe una política para el manejo de dispositivos externos a la compañía, esto puede ocasionar la instalación de programas con objetivos mal intencionados o extracción de información.

7.1.5 A.9 DOMINIO: CONTROL DE ACCESO.

Figura 9. Control de acceso.



Fuente: Autor.

La compañía ESSENSALE S.A.S debido al cambio en el manejo de la información y la adaptación de un sistema ERP implementó un directorio activo donde se definieron usuarios, grupos y políticas de seguridad para la información, se definieron políticas de contraseñas para las redes wifi, pero es muy visible para muchos usuarios ya que existe solo una red, para solucionar este riesgo, una solución es crear varias redes con diferente privilegio para asesores, visitantes, y colaboradores de cada área que necesiten acceder a cierta información.

Algunos usuarios utilizan contraseñas estándar generando un patrón conocido por todos y se han presentado casos donde registros han sido modificados por usuarios que no tiene conocimiento de ciertos módulos.

7.1.6 A.10 DOMINIO: CRIPTOGRAFÍA.

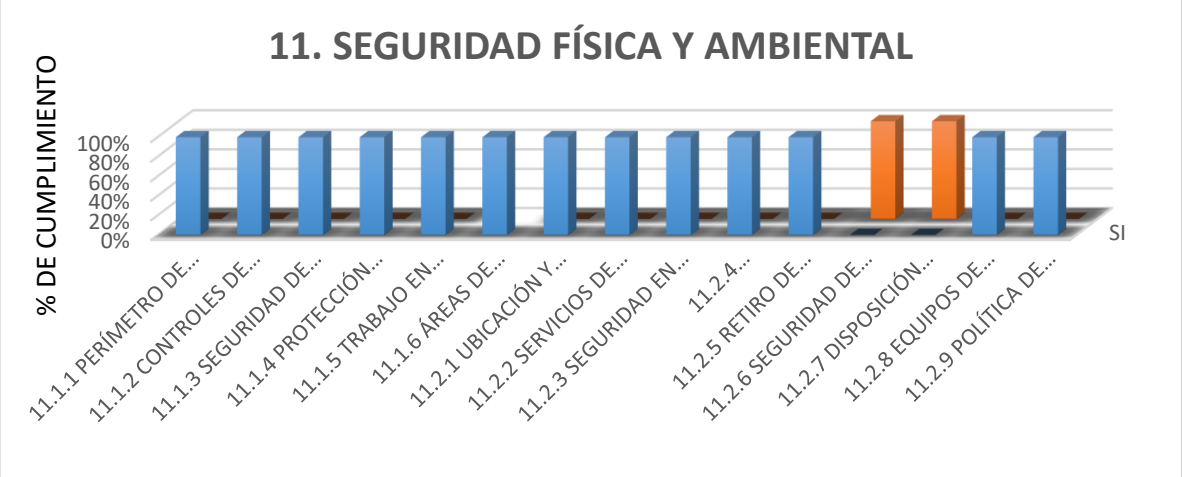
Figura 10. Criptografía

Fuente: Autor.

En este domino en la compañía no se defina una política general y se evidencia que algunas aplicaciones no cuentan con cifrados y se envía información de forma plana, pudiendo ser interceptada y visible por otros usuarios de la red, algunos servidores FTP no poseen estos cifrados, la intranet y el acceso vía internet al sitio web para la realización de pedidos cuenta con encriptación SSL, pero algunos de sus desarrollos poseen vulnerabilidades.

7.1.7 A.11 DOMINIO: SEGURIDAD FÍSICA Y AMBIENTAL.

Figura 11. Seguridad Física y Ambiental



Fuente: El Autor.

Verificando el dominio 11 sobre la seguridad física y ambiental, se evidencia que existe un buen manejo de los activos y el personal, posee las condiciones ambientales adecuadas para su buen funcionamiento, se está en constante seguimiento el control a materiales que puedan ocasionar mal funcionamiento como polvo o temperaturas altas, la infraestructura física es adecuada, solo en algunos casos se pudo observar daños en las instalaciones eléctricas o eran muy visibles para el personal, algunas entradas a las áreas no cuentan con sistemas de verificación como dispositivos biométricos o vigilancia en los sectores.

7.1.8 A.12 DOMINIO: OPERACIONES DE SEGURIDAD.

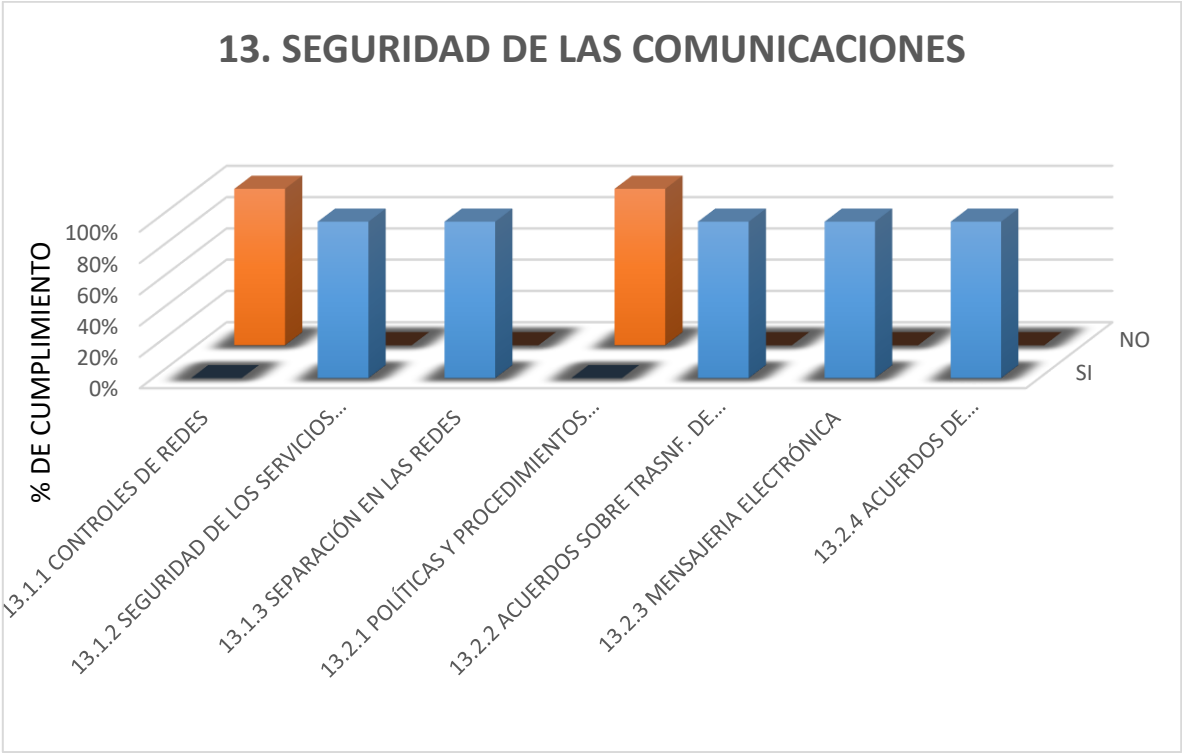
Figura 12. Operaciones de seguridad.

Fuente: Autor.

El equipo de desarrollo durante las actualizaciones o nuevos requerimientos por parte de los colaboradores de otras áreas no se tiene procedimientos para informar a los usuarios sobre cambios implementados, no cuenta con un medio de desarrollo y un medio de producción, pudiendo causar problemas en la operatividad debido a que los cambios se realizan directamente sobre esta.

7.1.9 A.13 DOMINIO: SEGURIDAD DE LAS COMUNICACIONES.

Figura 13. Seguridad de las comunicaciones.

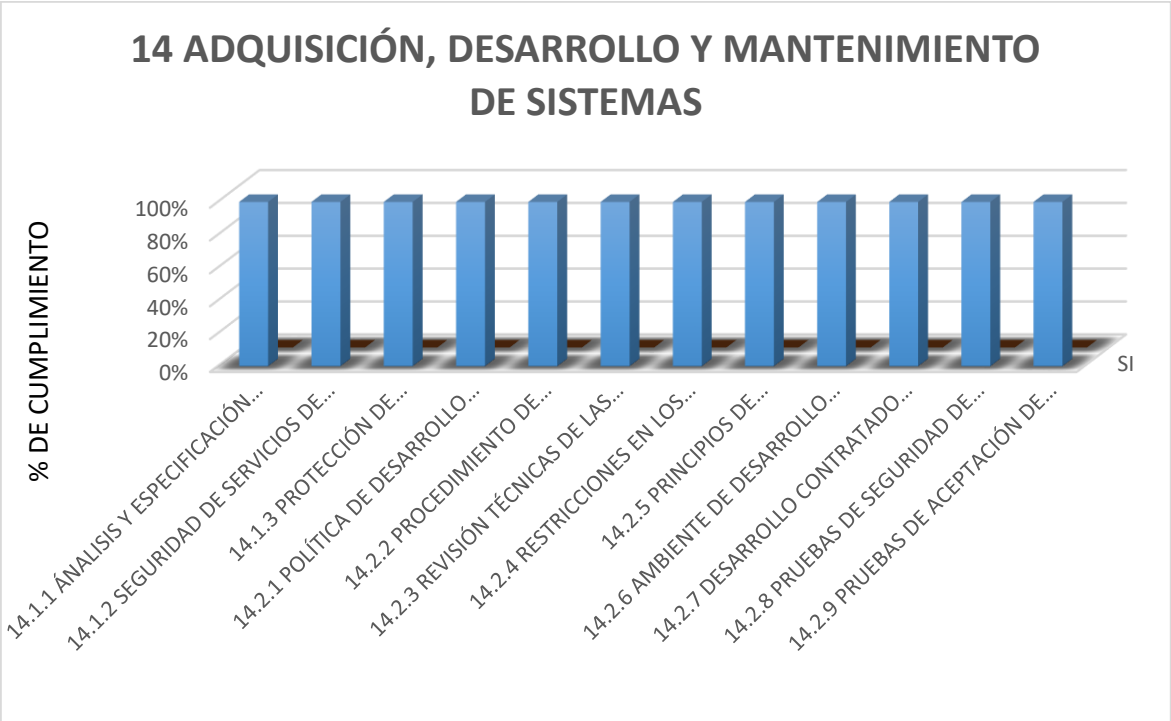


Fuente: El Autor.

Gracias al control que se realiza desde el directorio activo desde que se realizó la implementación del sistema ERP se puede monitorear los usuarios, las bases de datos SQL Server son controladas por nombre de máquina que son asignadas a cada colaborador para verificar la ejecución de consultas que pueden afectar el sistema o detener el negocio, se realizan inventarios de software capturados desde un servidor que monitorea los cambios de aplicaciones o instalaciones nuevas.

7.1.10 A.14 DOMINIO: SISTEMAS DE ADQUISICIÓN, DESARROLLO Y MANT.

Figura 14. Adquisición, Desarrollo y mantenimiento de sistemas.



Fuente: El Autor.

Realizando el análisis para el dominio 14, se pudo observar que la compañía ESSENSALE.S.A.S cuenta con desarrollos propios que utilizan la información del ERP y bases de datos de nuevas aplicaciones que ayudan al negocio.

EL sistema ERP cuenta con seguridades y licencias para ser accedido por los usuarios, las bases de datos pueden ser accedidas y modificadas por el equipo de desarrollo, creando procesos críticos que pueden afectar la producción.

7.1.11 A.15 DOMINIO: RELACIONES CON LOS PROVEEDORES.

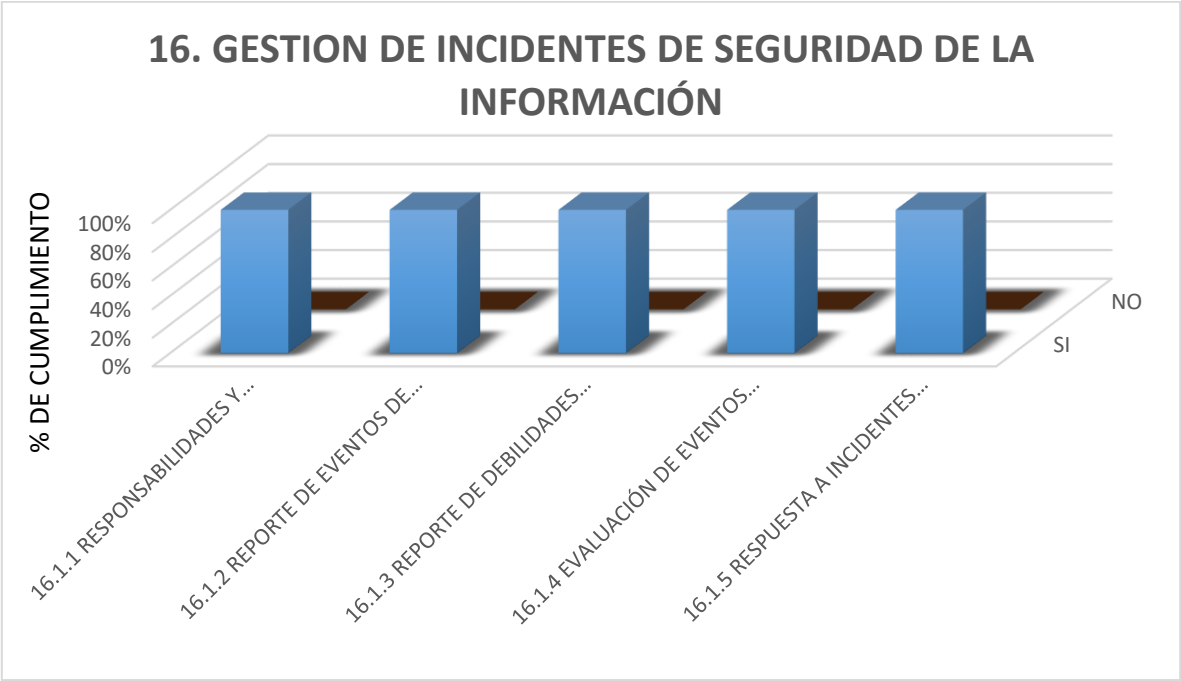
Figura 15. Relaciones con los proveedores.

Fuente: Autor.

Se pudo comprobar que se monitorean los servicios con proveedores, pero puede haber fallas al no existir una política para la realización o ejecución de los servicios o la existencia de listas de chequeo para verificar los puntos requeridos en el servicio, no obstante, se cuenta con un sistema en la intranet para las mejoras en cuanto a niveles de cumplimiento, no se establecen documentos o políticas para la protección del a información con proveedores.

7.1.12 A.16 DOMINIO: GESTIÓN DE INCIDENTES.

Figura 16. Gestión de incidentes de seguridad de la información.

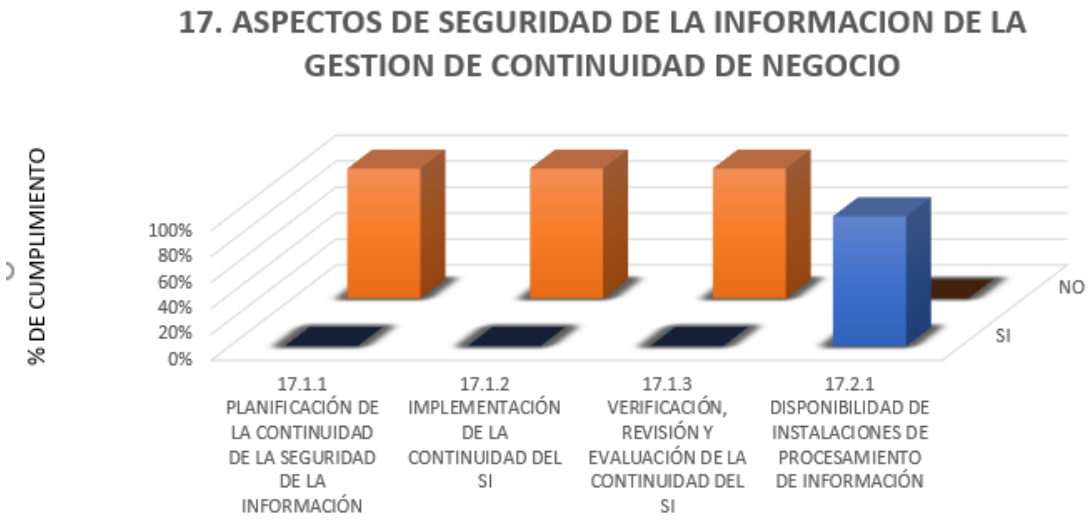


Fuente: Autor.

la política de seguridad de la información la compañía ESSENSALE S.A.S debe establecer responsabilidades para su cumplimiento asegurando que la información se encuentre protegida, Se pudo observar roles en los activos para obtener registros de eventos y controlar la ejecución de todo tipo de procesos en el negocio, se clasifican los activos que son objeto de posibles incidentes y vulnerabilidades los cuales son comunicados y supervisados.

7.1.13 A.17 DOMINIO: CONTINUIDAD DE NEGOCIO.

Figura 17. Aspectos de seguridad de la información de la gestión de continuidad de negocio.



Fuente: Autor.

La compañía ante los franquiciados y clientes garantiza el cumplimiento de contratos, por lo tanto, ante cualquier falla en las actividades del negocio la compañía debe tener una gestión de continuidad del negocio que permita contrarrestar el impacto generado por la dificultad, no obstante, se es necesario establecer controles para asegurar la continuidad del negocio, cuenta con dispositivos para prestar los servicios ofrecidos en la red que permiten garantizar la disponibilidad de las instalaciones y el procesamiento de la información.

7.1.14 A.18 DOMINIO: CUMPLIMIENTO

Figura 18. Cumplimiento.

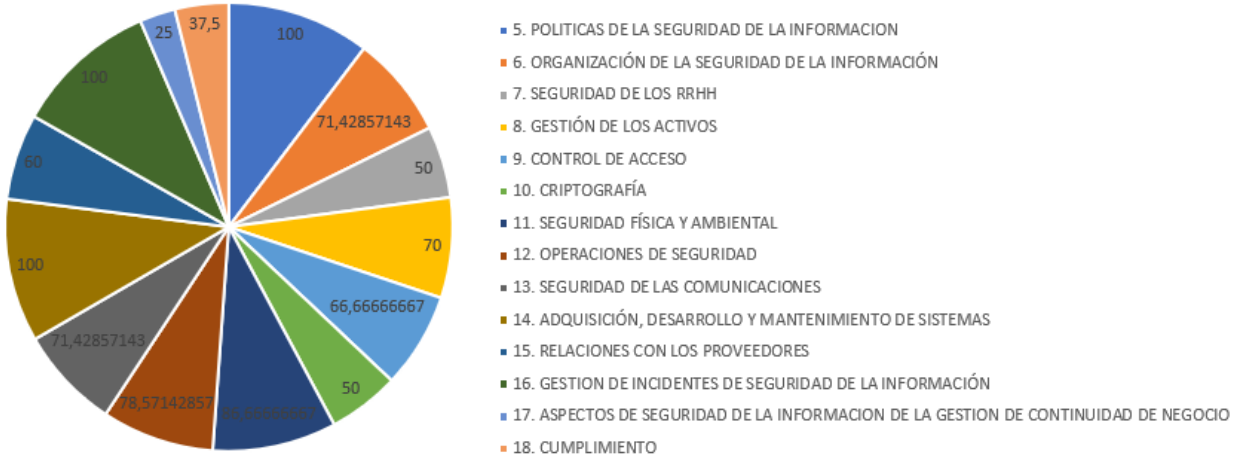
Fuente: Autor.

La compañía realiza sus procesos en el marco del cumplimiento de la ley colombiana, es importante establecer controles de seguridad que garanticen el cumplimiento de todas las obligaciones legales, se somete a la ley de habeas data cumpliendo con los requisitos para el manejo de las bases de datos.

ESSENSALE. S.A.S desarrolla diferentes módulos y accesos a la información generada por la ERP, debe establecer controles criptográficos que garanticen el acceso a los servidores y a la información enviada y obtenida, Se mantiene una constante observación con las entidades especiales, para realizar la revisión independiente de la SI.

7.1.15 GRÁFICO GRADO DE CUMPLIMIENTO

Figura 19. Resultado Diagnóstico de controles.



Fuente: El autor

La figura muestra los resultados del diagnóstico para los dominios de la norma ISO/IEC 27001:2013 evaluados en porcentaje (%) de cumplimiento al aplicar la lista de chequeo para verificación de existencia.

Los porcentajes en cada uno de los dominios son asociados al nivel de grado de cumplimiento los cuales son interpretados a razón del porcentaje de cumplimiento. Para los resultados totales, se determinaron por el promedio de los valores para lograr y verificar el nivel de madurez en cada dominio.

Se pudo comprobar que el resultado basado en la norma ISO/IEC 27001:2013 e ISO/IEC 27002:2013 demuestra que se encuentra en un nivel de madurez, donde se han estudiado actividades para la implementación de controles, compromiso y buenas prácticas.

Se debe realizar las constantes auditorias para definir los procesos que aún son necesarios, implementar otros sistemas de seguridad para lograr el control en indicadores para la toma de decisiones y el mejoramiento de la seguridad de la información.

8. ANÁLISIS DE RIESGOS MAGERIT

Desarrollando la metodología MAGERIT, se procedió a identificar de forma más detalla la información sobre los activos disponibles de la compañía ESSENSALE.S.A.S., contemplando su grado de valor y tratando las amenazas más conocidas y que ocurren con frecuencia que puedan afectar los diferentes activos y establecer su nivel de impacto. El presente análisis de riesgos permite a la compañía ESSENSALE S.A.S. determinar de qué forma, que tanto valor tiene y que tan protegido se encuentra el sistema de información. Esta implantación de medidas de seguridad verificó cada área informando al personal que interactúa con el sistema Identificando las amenazas potenciales y salvaguardas con base en la metodología MAGERIT VERSIÓN 3.

8.1 IDENTIFICACION Y VALORACION DE ACTIVOS.

Para el desarrollo de esta fase se consideraron una serie de activos de la empresa ESSENSALE S.A.S, los cuales se agruparon según el tipo de activo. Mediante la realización de entrevistas a encargados de área como también las visitas, se logró recolectar información suficiente para la creación del inventario de activos y corroborar la información con el almacenado en la compañía.

A continuación, se categorizan los componentes encontrados para cada tipo de activo

Tabla 8. Activos de la empresa Essensale S.A.S. y sus componentes

TIPO	COMPONENTES
Hardware	• SERVIDORES • EQUIPOS DE ESCRITORIO • EQUIPOS
Software	• ERP SIESA ENTERPRISE • NÓMINA CGUNO • ANTIVIRUS SYMANTEC

	• MICROSOFT OFFICE 2016 • SQL SERVER MANAGER • VMWARE • OCS • MYSQL MANAGER • SPARK • TEAM VIEWER
Datos e Información	• BASES DE DATOS SQL SERVER • BASES DE DATOS MYSQL • INFORMACION DE VENTAS • INFORMACIÓN DE PERSONAL
Redes y Comunicaciones	• CABLEADO FIBRA ÓPTICA • REDES WIFI • VOZ IP, SOFTPHONE • INTERNET • CÁMARAS IP
Personal	• INGENIERO DE SOPORTE • INGENIERO DE DESARROLLO • AUXILIARES DE SISTEMA • GERENTE
Localidad	• INFRAESTRUCTURA FÍSICA • BODEGA 8

Fuente: El Autor.

DEPARTAMENTO DE SISTEMAS

Cuenta con seis personas, dos de ellas se encargan de dar soporte, control de redes y control de hardware, dos encargados de los desarrollos, uno se encarga del diseño y el gerente del departamento.

PERSONAL.

1. INGENIERO DE DESARROLLO

   OBJETIVO DEL CARGO.

   Administrar, supervisar y asegurar el uso adecuado de las diferentes bases de datos SQL SERVER, MY SQL que conforman el sistema de información de la compañía, integrando también el desarrollo Python, Php de aplicaciones que permiten al usuario interactuar con estas.

   FUNCIONES

   - Planear actividades o acciones necesarias a desarrollar en las diferentes aplicaciones y/o sistemas de información que responden a requerimiento o nuevas necesidades de la compañía cuando sea necesario.
   - Determinar mensualmente las políticas de acceso a la base de datos y seguridad a nivel de datos y usuarios.
   - Dar soporte y gestionar las diferentes bases de datos, incluyendo las del ERP Siesa Enterprise y las de los desarrollos internos.
   - Garantizar la integridad de la información y la disponibilidad de las bases de datos.
   - Preparar informes mensuales de seguimiento del desempeño de las bases de datos, midiendo indicadores como tiempos de respuesta, accesos fallidos, tamaño en disco, bloqueo de cuentas, etc.

- Crear y configurar nuevas bases de datos relacionales que se requieran en el desarrollo de nuevas herramientas.
- Preparar consultas y reportes de minería de datos que ayuden a otras áreas en la toma de decisiones en la inteligencia de negocios de la compañía.
- Desarrollar herramientas de tecnología de información que permitan a usuarios internos o franquiciados consultar la información siguiendo las necesidades y lineamentos de las áreas que generan los requerimientos de desarrollo.
- Documentar funcionalmente los procesos que se realizan en las aplicaciones desarrolladas, detallar la estructura de información usada realizando diagramas de entidades relacionales y diagramas de flujos de datos, normalización esquemática, localización lógica y física de bases de datos y parámetros de tablas.
- Realizar el levantamiento de requerimientos que sean solicitados por parte de los usuarios finales para realizar modificaciones y/o mejoras a las aplicaciones existentes.
- Administrar los perfiles de usuarios en las diferentes aplicaciones desarrolladas según requerimiento del jefe inmediato de cada persona.
- Administrar los perfiles de usuarios en las diferentes aplicaciones desarrolladas según requerimiento del jefe inmediato de cada persona.
- Validar con el respectivo proveedor de cada una de las aplicaciones o sistemas de información de la compañía la viabilidad y/o factibilidad de implementación de las modificaciones y/o requerimientos de los usuarios.
- Validar la ejecución de las copias de seguridad de las aplicaciones existentes en la compañía día a día.
- Valida que los usuarios de la compañía tengan los permisos correspondientes para la ejecución de las actividades desarrolladas según su cargo.
- Aplicar y promover metodologías actualizadas que conduzcan a la práctica de una cultura de Seguridad Informática.
- Diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos de tal forma que se convierta en un valor agregado en los procesos de negocio entre cliente y empresa, basado en estándares nacionales e

internacionales y en los aspectos éticos y legales que rigen la Seguridad Informática.

- Planear, dirigir y conducir la evaluación de la ley de protección de datos personales.

2. INGENIERO DE SOPORTE

FUNCIONES.

- Desarrollar herramientas de tecnología de información que permitan a usuarios internos o franquiciados consultar la información siguiendo las necesidades y lineamentos de las áreas que generan los requerimientos de desarrollo.
- Documentar funcionalmente los procesos que se realizan en las aplicaciones desarrolladas, detallar la estructura de información usada realizando diagramas de entidades relacionales y diagramas de flujos de datos, normalización esquemática, localización lógica y física de bases de datos y parámetros de tablas.

3. AUXILIAR DE DESARROLLO

FUNCIONES

- Desarrollar herramientas de tecnología de información que permitan a usuarios internos o franquiciados consultar la información siguiendo las necesidades y lineamentos de las áreas que generan los requerimientos de desarrollo.
- Valida que los usuarios de la compañía tengan los permisos correspondientes para la ejecución de las actividades desarrolladas según su cargo.
- Documentar funcionalmente los procesos que se realizan en las aplicaciones desarrolladas, detallar la estructura de información usada realizando diagramas de

entidades relacionales y diagramas de flujos de datos, normalización esquemática, localización lógica y física de bases de datos y parámetros de tablas.

4. AUXILIAR DE SOPORTE
   FUNCIONES

   - Realizar instalaciones y proporcionar capacitación de nuestros productos en los sitios de los clientes o internamente.
   - Proporcionar reparación y mantenimiento preventivo, así como el servicio analítico según sea necesario internamente o en los sitios del cliente
   - Informar y registrar los problemas de los clientes e implementar soluciones.
   - Proporcionar consultas técnicas y soporte al cliente por escritorio remoto, teléfono, correo electrónico, visita si requiere.
   - Apoyar en el campo y en la empresa, como exposiciones de colaboradores, conferencias, informes, etc.

5. GERENTE DE SISTEMAS
   FUNCIONES

   - Proporcione servicios analíticos y soporte de ventas de productos opcionales en casa o en los sitios de los clientes.
   - Generar datos de muestra y escribir informes gerenciales de TI.
   - Ayudar con la compilación de estimaciones y presupuestos para medidas correctivas.
   - Proporcionar asistencia y tutoría a técnicos de campo, personal de ingeniería y personal de oficina.

El departamento de sistemas se encarga de proveer a los demás departamentos todo lo relacionado con el hardware, software y comunicaciones de la compañía.

En ella se encuentran tareas de reportes, procesamiento de datos, consultas, comunicaciones, impresiones, conectividad, almacenamiento, etc.

8.2 DESCRIPCIÓN DE TIPOS DE ACTIVO.

Para el desarrollo de este proceso se consideraron una serie de activos de la empresa ESSENSALE S.A.S, los cuales se agruparon según el tipo de activo.

Tabla 9. Descripción de Activos

TIPO DE ACTIVO	NOMBRE	DESCRIPCIÓN
INFORMACIÓN	Información Física	Es la información contenida en hojas, formatos, copias, impresiones, hojas de vida, procesos, políticas, organigramas, datos de acceso, cargos.
	Información Digital	Es el almacenado de información en dispositivos digitales como USB, discos duros, cd, u otro medio electrónico.
	Base de Datos	Contiene toda la información acerca de compras, ventas y todas las actividades financieras o contables de la compañía.
LOCALIDAD	Infraestructura Física	La compañía ESSENSALE S.A.S. cuenta una bodega principal ubicada en la ciudad de Cali y diferentes tiendas a nivel nacional
	Zona de Accesos Seguridad, Oficina, Equipos	Las zonas de acceso cuentan con personal que controla el manejo de los equipos.

	Aire acondicionado	Cuenta con proveedores para el suministro y mantenimiento del aire acondicionado.
ORGANIZACION	Proveedores de Mantenimiento de Equipo	En la sede principal el equipo de soporte se encarga del mantenimiento de los equipos.
	Proveedores de Software	Es cliente de los servicios de Microsoft, Virtualización VMware, Siesa y otras compañías desarrolladoras de software como ET marcas.
	Proveedores de servicio de Vigilancia, Alarma y Cámaras de seguridad.	La bodega cuenta con vigilancia privada controlando el acceso solo al personal de la compañía, y en su interior están ubicadas cámaras en todas sus áreas.
PERSONAL	Administrador del Sistema	Los sistemas son manejados principalmente por un ingeniero de soporte que se encarga de las configuraciones y un ingeniero de desarrollo en el manejo de las bases de datos y desarrollos a implementar
	Gerente	Es el encargado de los nuevos procesos y las nuevas herramientas para el mejor funcionamiento de la compañía.
	Usuarios	Todos los empleados que accedes a los servicios y recursos de los sistemas.
SOFTWARE	Sistemas Operativos	Cuenta con diferentes sistemas operativos, un servidor Windows, con IIS

	6 , un servidor Windows de bases de datos y un servidor de aplicaciones, también cuenta con un servidor Linux CentOS para algunos procesos
SQL Server 2014	Base de datos utilizada para el ERP SIESA ENTRERPRISE
MYSQL	Base de datos para el uso de intranet y otros datos
CGUNO	Control de Nómina
SIESA ENTERPRISE	Software contable utilizado por ESSENSALE S.A.S. Comprende módulos de: Ventas, Compras, Inventarios, Producción, Planeación, Financiero, Sistema POS.
Antivirus	Antivirus McAfee Total Protection.
Ofimática	Herramientas para el manejo de información utilizando Excel Avanzando, Documentos Word, Presentaciones PowerPoint y envió de correo Outlook y 365.
Skype Spark	Comunicación en línea con los usuarios, videoconferencia y comunicación interna con spark
Navegadores Web	Los más utilizado en la compañía son el Firefox y Chrome.

HARWARE	Servidores	Los servidores se encuentran en la sede principal. Actualmente se cuenta con 1 servidores físico y 7 virtuales: servidor de base de datos Servidor de aplicaciones Servidor IIS Controlador de dominio DNS
	PC	Sede Cali Bodega 8: Contabilidad: 14 equipos Mercadeo: 10 equipos laboratorio: 4 equipos. Despacho: 4 equipos Compras: 3 equipos Sistemas: 6 equipos. Recursos Humanos: 6 equipos
	Cableado	Cableado fibra y UTP utilizado en la compañía
	Router	dispositivo enrutador que proporciona conectividad a nivel de red y controlando la asignación de las IP
	Switch	Interconexión de múltiples equipos y apilamiento de redes.
	Punto de acceso	Proporciona conexión de dispositivos móviles.

8.3 INVENTARIO DE ACTIVOS DE ESSENSALE.S.A.S.

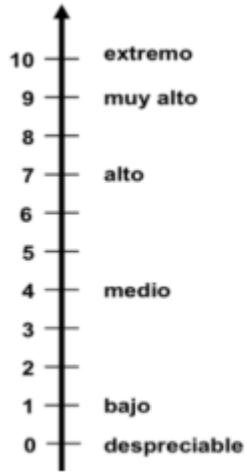
En el ANEXO I se presenta la lista de activos de la compañía ESSENSALE S.A.S

8.4 DIMENSIONES DE VALORACIÓN DE ACTIVOS.

Para evaluar cada uno de los activos informáticos, se establecieron dimensiones de valoración, el respectivo criterio, ubicación y descripción recolectadas en las visitas y entrevistas al área de tecnología y soporte.

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

Tabla 10. Valoración de amenazas



valor		*criterio*
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6-8	alto	daño grave
3-5	medio	daño importante
1-2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Fuente: El autor.

Dimensiones de valoración. A continuación, se observa las diferentes dimensiones de un activo.

[D] disponibilidad. ¿Qué daño se causaría si no estuviera disponible o los clientes no lo pudieran utilizar? Esta valoración es común en los servicios.

[I] integridad de los datos. ¿Qué daño se causaría si fuera destruido o estuviera corrupto? Esta evaluación es común en el acceso a la información.

[C] confidencialidad de los datos. ¿Qué daño causaría el acceso no autorizado? Esta valoración es común en el acceso a la información.

[A] autenticidad de los usuarios y de la información. ¿En qué medida es dañina la falta de conocimiento sobre quién ha hecho una acción? Esta valoración es común en los servicios como la autenticidad del usuario y de los datos relacionado a la autenticidad de las personas que acceden a los datos para ingresar nuevos registros, actualizarlos o solo consultarlos.

[T] trazabilidad del servicio y de los datos. ¿qué daño se causaría al no saber a quién se presta el servicio? Se debe establecer, quien realiza una acción y cuando, como también el acceso a datos.

B8: Bodega 8
B1: Bodega 1
B*: Todas las Bodegas

Tabla 11. Valoración de activo, descripción y ubicación

ACTIVOS	UBICACIÓN	CÓDIGO	[D]	[I]	[C]	[A]	[T]
ACCESS POINT	B 8	[COM]	10	10	10	10	10
AIRE ACONDICIONADO	B*	[AUX]	5	5	5	5	5
ALARMA	B 8	[AUX]	5	5	5	5	5
BÁSCULA	B8, CO	[HW]	5	5	5	5	5
BIABLE	B8	[SW]	6	6	6	6	6
BLUETOOTH	B8	[HW]	6	6	6	6	6

CAMARA *	B8, B1	[HW]	6	6	6	6	6
CELULAR	B*	[HW]	8	8	8	8	8
CISCO	B8	[HW]	8	10	8	10	10
COMPUTADOR/CPU	B*, C0	[HW]	8	10	8	10	8
DISCO DURO *	B8	[HW]	8	10	8	8	8
DOMINIO	*	[SW]	8	10	8	8	8
DVR	B8	[HW]	5	5	5	5	5
ESCANER	B*	[HW]	5	5	5	5	5
FOTOCOPIADORA	B*	[HW]	5	5	5	5	5
IMPRESORA	B*, CO	[HW]	6	8	6	8	6
IPAD MERCADEO	B4	[HW]	8	10	8	8	8
MODEM	B8	[HW]	8	10	8	8	8
MODULO SOFTWARE	B*	[SW]	6	6	6	6	6
PORTATIL	B*	[HW]	5	5	5	5	8
REGULADOR DE ENERGIA	B*	[HW]	8	10	8	10	8
ROUTER	B8	[HW]	10	10	10	10	10
SERVIDOR	B8	[HW]	10	10	10	10	10
SOTFWARE EXTRANET	B8	[SW]	10	10	10	10	10
SOTFWARE INTRANET	B*	[SW]	10	10	10	10	10
TELEFONO ALAMBRICO	B*	[HW]	5	5	5	6	5
TELEFONO INALAMBRICO	B*	[HW]	5	5	5	6	5
CLAVE CRIPTORÁFICA VPN	B*	[K]	10	10	10	10	10
CLAVE CRIPTORÁFICA WEB	B*	[K]	10	10	10	10	10
SERVICIO FTP	B8	[S]	8	9	8	8	8
SERVICIO SSH	B8	[S]	8	9	10	10	8
FIREWALL	B8	[HW]	10	9	9	9	9
PERSONAL*		[P]	8	8	9	10	9
UPS	B*	[HW]	5	5	5	5	5

Fuente: El Autor

8.5 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Las amenazas son eventos que podrían sucederle a los activos y afectar su valor. Una amenaza puede causar un incidente en la organización, generando daños a la propiedad o pérdidas intangibles en sus activos.

Las amenazas se clasifican según el Catálogo de elementos de MAGERIT versión 3 [1] en:

De origen natural. El sistema de información es una víctima pasiva de los desastres naturales (terremotos, fuego, inundaciones, pandemias ...); se procede a evaluar cuáles son las consecuencias.

De origen ambiental. El sistema de información es una víctima pasiva de algunos desastres industriales (contaminación, fallas eléctricas, derrame de producto químico ...); se procede a evaluar cuáles son las consecuencias.

Amenazas accidentales causadas por personas. Los colaboradores u otro tipo de personas con acceso al sistema de información pueden causar problemas involuntarios, especialmente debido a un error o incumplimiento de políticas.

Ataques causados por personas de forma deliberada. Los colaboradores u otro tipo de personas con acceso al sistema de información pueden causar problemas intencionados como ataques deliberados para obtener una ventaja de forma ilegitima o con la intención de causar daños.

A continuación, se relacionan las amenazas que pueden afectar los diferentes tipos de activos de la compañía.

Tabla 12. Análisis de riesgos con base en la metodología MAGERIT

ACTIVOS	CÓDIGO	AMENAZAS

ACCESS POINT INT	[COM]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.5] Avería de origen físico o lógico [A.4] Manipulación de la configuración [A.10] Alteración de secuencia [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.24] Denegación de servicio [A.30] Ingeniería social [A.15] Modificación deliberada de la información
AIRE ACONDICIONADO	[AUX]	[N.1] Fuego [N.*] Desastres naturales [I.5] Avería de origen físico o lógico
ALARMA	[AUX]	[N.1] Fuego [N.*] Desastres naturales [I.5] Avería de origen físico o lógico
BACKUP	[HW]	[N.1] Fuego [N.*] Desastres naturales [I.5] Avería de origen físico o lógico
BIABLE	[SW]	[E.2] Errores del administrador [E.4] Errores de configuración [E.14] Escapes de información [E.19] Fugas de información [E.21] Errores de mantenimiento [E.24] Caída del sistema por agotamiento de

		recursos [A.5] Suplantación de la identidad del usuario [A.7] Uso no previsto
BLUETOOTH	[HW]	[E.19] Fugas de información
CAMARA *	[HW]	[A.4] Manipulación de la configuración [A.14] Interceptación de información (escucha)
CELULAR	[HW]	[E.19] Fugas de información [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información (escucha)
CISCO	[COM]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.5] Avería de origen físico o lógico [A.4] Manipulación de la configuración [A.10] Alteración de secuencia [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.15] Modificación deliberada de la información [A.24] Denegación de servicio
COMPUTADOR/CPU	[HW]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales

DISCO DURO *	[MEDIA]	[I.1] Fuego [I.5] Avería de origen físico o lógico [A.4] Manipulación de la configuración [A.10] Alteración de secuencia [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [A.7] Uso no previsto [A.11] Acceso no autorizado
DOMINIO 1 ANO	[SW]	[A.4] Manipulación de la configuración
DVR	[MEDIA]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [A.14] Interceptación de información (escucha)
ESCANER	[HW]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [A.7] Uso no previsto
FOTOCOPIADORA	[HW]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [A.7] Uso no previsto
IMPRESORA	[HW]	[N.1] Fuego [N.2] Daños por agua

		[N.*] Desastres naturales [A.7] Uso no previsto
IPAD MERCADEO	[HW]	[A.7] Uso no previsto [A.14] Interceptación de información (escucha)
MODEM	[COM]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.5] Avería de origen físico o lógico [A.4] Manipulación de la configuración [A.10] Alteración de secuencia
MODULO NOMINA	[SW]	[E.1] Errores de los usuarios [E.14] Escapes de información
PORTATIL	[HW]	[N.1] Fuego [E.14] Escapes de información [A.7] Uso no previsto [A.14] Interceptación de información (escucha)
PORTATIL MAC	[HW]	[E.14] Escapes de información [A.7] Uso no previsto [A.14] Interceptación de información (escucha) [N.1] Fuego
REGULADOR DE ENERGIA	[HW]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales

ROUTER	[HW]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.5] Avería de origen físico o lógico [A.4] Manipulación de la configuración [A.10] Alteración de secuencia [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.24] Denegación de servicio [A.30] Ingeniería social
SERVIDOR	[HW]	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [I.1] Fuego [I.5] Avería de origen físico o lógico [A.4] Manipulación de la configuración [A.10] Alteración de secuencia [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.24] Denegación de servicio

SOTFWARE EXTRANET	[SW]	[A.10] Alteración de secuencia [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.14] Escapes de información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento [A.3] Manipulación de los registros de actividad (log) [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.14] Interceptación de información (escucha) [A.19] Divulgación de información [A.30] Ingeniería social

SOTFWARE INTRANET	[SW]	[A.10] Alteración de secuencia [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.14] Escapes de información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento [A.3] Manipulación de los registros de actividad (log) [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.14] Interceptación de información (escucha) [A.19] Divulgación de información [A.30] Ingeniería social
TELEFONO ALAMBRICO	COM	[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales [A.7] Uso no previsto [A.14] Interceptación de información (escucha)
TELEFONO INALAMBRICO	COM	[N.1] Fuego [N.2] Daños por agua

		[N.*] Desastres naturales [A.7] Uso no previsto [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información (escucha)
CLAVE CRIPTORÁFICA VPN	[K]	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.4] Errores de configuración [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Escapes de información [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.21] Errores de mantenimiento [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso
SERVICIO FTP	[S]	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.4] Errores de configuración [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Escapes de información [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.21] Errores de mantenimiento [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso

SERVICIO SSH	[S]	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.4] Errores de configuración [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Escapes de información [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.21] Errores de mantenimiento [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso
FIREWALL	[HW]	[E.2] Errores del administrador [E.4] Errores de configuración [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [A.5] Suplantación de la identidad del usuario [E.21] Errores de mantenimiento
CLAVE CRIPTORÁFICA WEB	[K]	[E.1] Errores de los usuarios [E.2] Errores del administrador [E.4] Errores de configuración [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Escapes de información [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.21] Errores de mantenimiento

		[A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso
PERSONAL	[P]	[A] Ataques intencionados [A.3] Manipulación de los registros de actividad (log) [A.4] Manipulación de la configuración
UPS		[N.1] Fuego [N.2] Daños por agua [N.*] Desastres naturales

8.6 CUADRO DE ESTIMACIÓN DE IMPACTO Y PROBABILIDAD UTILIZANDO LA METODOLOGÍA MAGERIT.

Identificadas las amenazas y que pueden afectar a los activos de la compañía ESSENSALE S.A.S se procede a valorar la degradación con respecto a la probabilidad de ocurrencia tomando como referencia la metodología MAGERIT versión 3 [29].

DEGRADACIÓN: qué tan afectado podría salir el activo en cuanto a su valor si llegara a ocurrir un incidente.

Tabla 13. Criterios de valoración

DEGRADACIÓN

ESCALA	VALOR	FRECUENCIA	LAPSO
MA (MUY ALTO)	5	Muy frecuente	Diario
A (ALTO)	4	Frecuente	Mensual
M (MEDIO)	3	Normal	Anual
B (BAJO)	2	Poco frecuente	Décadas
MB (MUY BAJO)	1	Frecuencia casi nula	Siglos

Fuente: El autor.

PROBABILIDAD DE OCURRENCIA: Qué probabilidad hay de que una amenaza sea realidad

Tabla 14. Criterios de valoración (probabilidad)

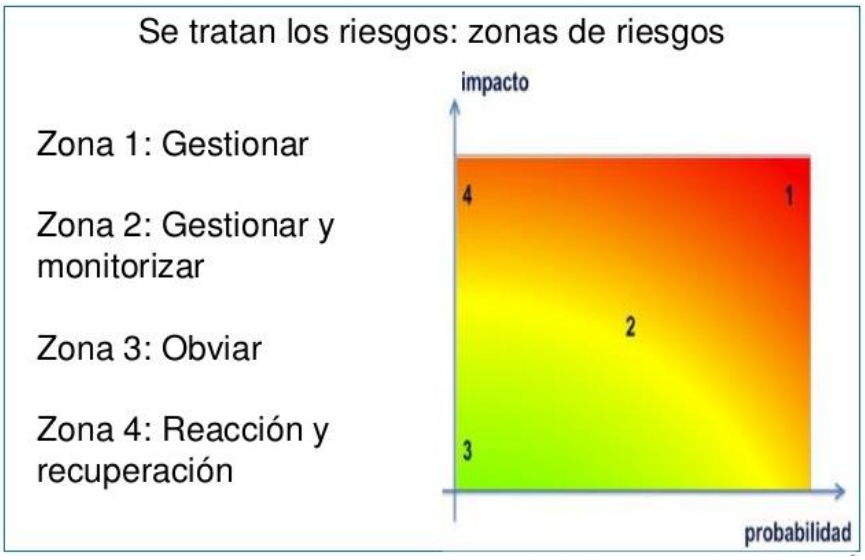
PROBABILIDAD DE OCURRENCIA			
ESCALA	**VALOR**	**PROBABILIDAD**	**LAPSO**
MA (MUY ALTO)	5	100	Diario
A (ALTO)	4	10	Mensual
M (MEDIO)	3	1	Anual
B (BAJO)	2	1/10	Décadas
MB (MUY BAJO)	1	1/100	Siglos

Fuente: El autor.

[29] MAGERIT – version 3.0 Methodology for Information Systems Risk Analysis and Management

De acuerdo a la metodología MAGERIT, se definen las zonas para determinar el tratamiento de los riesgos.

Figura 20. Función Impacto Vs Probabilidad.



Fuente: Ministerio de hacienda España [En línea] Magerit 3.0 (Recuperado 19 noviembre 2020). Disponible en https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Utilizando la información anterior se procede a evaluar los activos identificando la valoración en el siguiente cuadro:

[D]: Degradación
[P]: Probabilidad
[R]: Riesgo Zona

Z1: Zona 1
Z2: Zona 2
Z3: Zona 3
Z4: Zona 4

Tabla 15. Matriz de valoración de riesgos

ACTIVO	AMENAZAS	[D]	[P]	[R]
HARDWARE	fallo en los dispositivos	M	M	Z2
	Deterioro físico	M	M	Z2
	Pérdida de equipo	B	B	Z3
SOFTWARE	Aplicaciones maliciosas tipo troyanos, gusano, keyloggers.	A	A	Z1
	Mal funcionamiento de aplicaciones	M	M	Z2
	Errores de almacenamiento	A	B	Z4
	Robo de equipos o información	B	B	Z3
	Accidente por agua, incendio, químicos	A	A	Z1
	Uso no autorizado de equipos	M	M	Z2
	Accesos no autorizados	M	M	Z2
	Incumplimiento de políticas existentes	B	B	Z3
REDES	Mal funcionamiento	A	A	Z1
	Daño físico	M	M	Z2
	Pérdida de equipo	B	B	Z3
PERSONAL	Empleados internos	B	B	Z3
	Asesoras tiendas	B	B	Z3
	Ingeniería social	B	B	Z3
	Abuso de privilegios	M	M	Z2
	Accesos no autorizados	M	M	Z2
	Uso no autorizado de equipos	M	M	Z2

Fuente: El autor.

8.7 ANÁLISIS DE RESULTADOS DE LA MATRIZ DE RIESGOS.

La empresa ESSENSALE S.A.S. se pudo apreciar que es objeto de diversa amenazas y vulnerabilidades que pueden poner en riesgo los activos de la compañía. Conforme a

la matriz de riesgos realizada, se considera la valoración del nivel de riesgo clasificado en crítico, alto y medio, se puede observar lo siguiente:

Zona 1 Gestionar. Nivel Crítico.

Se identificaron sobrecargas eléctricas, presentes en la entrada principal, con falta de protección generando daños por medio ambiente y peligros a los colaboradores.

Todos estos inconvenientes afectan en primera instancia a los servidores alojados en el área de tecnología que soportan el sistema ERP y otras aplicaciones para ESSENSALE.S.A.S., se puede presentar errores de red como las asignaciones de direcciones IP, el inicio del cortafuegos, y el proxy para el control de descargas y navegación. Por otro lado, los colaboradores de la compañía pueden verse afectados ya que se generan descargas que atentan contra la salud o vida donde se presenta el fallo.

Esta zona cuenta con un almacenamiento de líquidos inflamables como alcohol, pudiendo ocasionar daños por fuego.

Zona 2 Gestionar y monitorizar. Nivel Medio.

La compañía ESSENSALE S.A.S. no cuenta con un control seguro de entrada y salida de equipos, el personal tiene libre uso de los activos, pudiendo llevar estos al exterior, ocasionando pérdidas o robo.

Zona 3 Obviar. Nivel Medio.

La compañía ESSENSALE S.A.S. cuenta con un directorio activo y una administración de roles para los usuarios de intranet como también para la extranet, no obstante, el control de contraseñas no presenta una política estricta donde cada usuario sea responsable de el buen manejo de la misma, se ha presentado accesos a intranet, o sistema ERP desde usuarios que no permanecen en la compañía o no estaban presentes a la hora de generado el evento.

Zona 4 Reacción y recuperación. Nivel Medio.

Debido a que La compañía ESSENSALE S.A.S. posee en sus instalaciones los servidores de bases de datos y no ha optado por manejar la infraestructura de “cloud”,

debe generar backups constantes en cada uno de sus procesos con su respectiva base de datos, se ha presentado pérdida de información en servicios que han dejado de usarse y al no ser custodiados han sido suprimidos.
a continuación, se presenta el tratamiento de riesgos del área de tecnología para contrarrestarlos estableciendo los controles necesarios.

PROCESO SOFTWARE	**FECHA DE ELABORACIÓN**	15/03/2018	**VERSION** 1.x
Realizar e importar los pedidos vía intranet.	**Elaborado por:** Daniel Rincón Brito		**Aprobado por:** Alex Escobar
Responsable: Esteban Viáfara	**Revisado por:** Daniel Rincón		Código 001

OBJETIVO GENERAL.

1) Controlar y minimizar los riesgos asociados al envió y la importación de archivos planos al sistema ERP.

OBJETIVOS ESPECÍFICOS.

1) controlar duplicados de información.
2) Controlar usuarios de sistema.
3) Controlar usuarios y contraseñas de archivos planos
4) Verificar funciones de los nuevos desarrollos.

RECURSOS.

Humano: Asesoras de ventas, auxiliar de operaciones, auxiliar de sistemas, auxiliares contables.

Físico: Equipos de escritorio, redes, servidores.

RESPONSABLES.

Gerente de operaciones

Auxiliar de sistemas

Ingeniero de desarrollo.

PROCESO HARDWARE	**FECHA DE ELABORACIÓN**	15/03/2018	**VERSION** 1.x
Instalación, configuración de software, hardware y redes de la compañía.	**Elaborado por:** Daniel Rincón Brito		**Aprobado por:** Alex Escobar
Responsable: Joaquín Vargas Frank Ortiz	**Revisado por:** Daniel Rincón		Código 002

OBJETIVO GENERAL.

1) Controlar y minimizar los riesgos asociados a la instalación y configuración de equipos en la compañía.

OBJETIVOS ESPECÍFICOS.

1) Controlar el acceso, roles y privilegios.
2) Configurar la protección mínima de los equipos.
3) Validar el dominio del sistema
4) Controlar la red local y las conexiones externas.

RECURSOS.

Humano: Asesoras de ventas, auxiliar de operaciones, auxiliar de sistemas, auxiliares contables.

Físico: Equipos de escritorio, redes, servidores.

RESPONSABLES.

Gerente de operaciones

Auxiliar de soporte

Ingeniero de soporte

Administrador de redes

PROCESO DISEÑO Y DESARROLLO	**FECHA DE ELABORACIÓN**	15/03/2018	**VERSION** 1.x
Realizar y mantener las aplicaciones de la compañía.	**Elaborado por:** Daniel Rincón Brito		**Aprobado por:** Alex Escobar
Responsable: Daniel Rincón Esteban Viáfara	**Revisado por:** Daniel Rincón		Código 002

OBJETIVO GENERAL.

1) Controlar y minimizar los riesgos asociados al diseño y desarrollo de las aplicaciones en la compañía.

OBJETIVOS ESPECÍFICOS.

1) Controlar el acceso, roles y privilegios.
2) Verificar las funciones de las aplicaciones.
3) Resolver errores de aplicaciones

RECURSOS.

Humano: Asesoras de ventas, auxiliar de operaciones, auxiliar de sistemas, auxiliares contables.

Físico: Equipos de escritorio, redes, servidores.

RESPONSABLES.

Gerente de tecnología

Ingeniero de desarrollo

Auxiliar de desarrollo

9. INFORME DE AUDITORIA

A continuación, se presenta un resumen de los hallazgos identificados durante el desarrollo del Sistema de Gestión de Seguridad de la Información para la compañía ESSENSALE S.A.S. y las respectivas sugerencias para el gerente de tecnología.

9.1 HALLAZGOS DE AUDITORIA.

Hallazgo 1

No existe una política de seguridad para el ingreso de personal a la compañía ESSENSALE S.A.S. el ingreso al área de tecnología y servidores es de fácil acceso y no es custodiado o restringido por algún tipo de seguridad.

Recomendaciones.

- Establecer una política de seguridad para el ingreso de personal a la compañía y el acceso a equipos que son importantes para la operación.
- Implementar controles de acceso a los servidores de la compañía y una política para manipulación de activos por medio de terceros.

Hallazgo 2

En los procesos de selección de personal no se evidenció una política de confidencialidad de la compañía ni existe un manual o capacitación en seguridad de la información.

Recomendaciones

- Es importante que en el proceso de selección y contratación se defina la capacitación del colaborador acerca de la importancia de la seguridad de la información en las diferentes áreas de la compañía ESSENSALE S.A.S
- Es necesario definir una política de seguridad en el área de recursos humanos para establecer las cláusulas de contratación, en especial el manejo de la información y la confidencialidad de esta especificando las consecuencias que lleva el no cumplirlas.

Hallazgo 3

Se encontró acceso a servidores FTP sin seguridad de cifrado para la autenticación.
Recomendaciones

- Se debe generar un método de cifrado para la autenticación FTP, el no cifrado puede llevar al robo de contraseñas por otro usuario de la red de la compañía ESSENALE S.A.S.
- Generar y monitorear el log del servicio FTP presentando un informe de los usuario y archivos gestionados.

Hallazgo 4

Se detectó en la compañía ESSENSALE S.A.S que la contraseña de red Wi-Fi es una para todas las áreas incluyendo usuarios fuera de la compañía, el acceso a la red vía Wi-Fi es posible escanear servidores de bases de datos y todos los demás equipos de los colaboradores.

Recomendaciones

- Se debe establecer roles para el acceso a la red local vía Wi-Fi, definir grupos con acceso a información especial y los recursos necesarios.

Hallazgo 5

Se detectaron vulnerabilidades en algunos de los activos de los colaboradores del a compañía ESSENSALE S.A.S permitiendo el acceso a la máquina pudiendo extraer todo tipo de información.
Recomendaciones

- Verificar los puertos y servicios vulnerables que pueden ser aprovechados por un usuario con mayor privilegio en la compañía.

Hallazgo 6
En el desarrollo de las aplicaciones de la compañía ESSENSALE S.A.S no se encontró el proceso de desarrollo, pruebas y producción para el lanzamiento de nuevas

aplicaciones o nuevos requerimientos haciendo que se realicen copias de las bases de datos en diferentes equipos de los desarrolladores, como también parches realizados a aplicaciones ya en producción.

Recomendaciones.

- Definir un versiona miento para controlar el desarrollo de las aplicaciones y evitar el uso indebido de bases de datos o parches en producción sin las pruebas necesarias que pueden llegar a comprometer el sistema.
- Definir una política de seguridad para el manejo de las bases de datos del sistema Enterprise y la intranet.

Hallazgo 7

Se evidenció en la compañía ESSENSALE S.A.S el uso de contraseñas de forma general, utilizando la mayoría de los colaboradores un mismo patrón haciendo que cualquier colaborador pueda utilizar un usuario y realizar acciones en el sistema para su beneficio.

Recomendaciones.

- Establecer una política de seguridad para el manejo de contraseñas como el cambio periódico, longitud, y caracteres especiales.
- Capacitar a los colaboradores acerca del uso adecuado de contraseñas.

Hallazgo 8

Se encontraron vulnerabilidades de inyección SQL en las aplicaciones de la intranet para el control de entrada y salida de las asesoras de ventas.

Recomendaciones

- Se debe establecer un framework actualizado para mejorar la seguridad de las aplicaciones web, o crear métodos para codificar la información recibida por el servidor.

Hallazgo 9

Se pudo encontrar en la compañía ESSENSALE S.A.S sitios con cableado eléctrico defectuoso que puede alterar el funcionamiento de los activos.

Recomendaciones

- Definir una política de control y monitoreo para el cableado eléctrico, definiendo visitas constantes del proveedor encargado.
- Informar al proveedor de cambios o anomalías en el funcionamiento de los activos y de la UPS.

Hallazgo 10

Se evidenció en la compañía ESSENSALE S.A.S el uso de dispositivos externos como USB que pueden ser utilizados para el robo de información o datos de los activos como contraseñas de red utilizando métodos de “Rubber Ducky” o instalación de software malicioso[30].

Recomendaciones.

- Establecer una política de seguridad que restrinja el uso de dispositivos externos en los activos y el bloqueo de ejecución de aplicaciones desconocidas para ESSENSALE S.A.S.

[30] HACK5. USB Rubber Ducky. Disponible en internet< http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/>

10. ALTERNATIVAS DE SOLUCIÓN A HALLAZGOS

A continuación, se especifican las políticas basadas en los hallazgos de auditoria encontrados en las áreas de la compañía ESSENSALE S.A.S detallados en el informe de auditoría, las cuales servirán como esquema general para la implementación el Sistema de Gestión de Seguridad de la información.

10.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE ESSENSALE S.A.S

Preservar la Confidencialidad, Integridad, y Disponibilidad de la información concerniente a las partes interesadas en los servicios de ESSENSALE S.A.S con una implementación adecuada del Sistema de Gestión de Seguridad de la Información se compromete a contrarrestar una gran cantidad de problemas de acceso, administración y responsabilidades. Esta política es de cumplimiento obligatorio por parte de todo el personal interno, externo y proveedores de la organización

10.1.1 OBJETIVO

- Establecer políticas de seguridad para el desarrollo del Sistema de Gestión de Seguridad de la Información de la compañía ESSENSALE S.A.S la cual tiene como prioridad garantizar la disponibilidad, integridad y confidencialidad de la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, o acceso no autorizado que garanticen el adecuado cumplimiento de la ley.
- Los colaboradores de la compañía estarán en capacidad de conocer y aplicar estas políticas con el fin de preservar los activos y la confidencialidad e la información.
- Propiciar la cultura de seguridad de la información a través de la toma de conciencia.
- Gestionar los riesgos de seguridad de la información que concierne a ESSENSALE S.A.S.
- Gestionar los incidentes que afecten los pilares fundamentales de la seguridad de la información realizando análisis y recolección de evidencias tomando las acciones necesarias para la mejora y continuidad del sistema de información.

10.1.2 ALCANCE

Las Políticas de Seguridad de la Información definidas se implementan en instalaciones de ESSENSALE S.A.S, Bodega 8 Parque Industrial La Esmeralda.

10.2 POLITICA GENERAL

- ESSENSALE S.A.S tiene como prioridad conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, o acceso no autorizado que garanticen el adecuado cumplimiento de la ley.
- ESSENSALE S.A.S se compromete a adoptar una guía interna de políticas y procedimientos para garantizar el apropiado cumplimiento de la ley para la atención de consultas y reclamos por parte de los titulares, garantizando, en todo momento, el pleno y efectivo ejercicio del derecho de hábeas data.
- ESSENSALE S.A.S se compromete cumplir las instrucciones y requerimientos que solicite la Superintendencia de Industria y Comercio, realizar a tiempo la actualización, rectificación o eliminación de los datos en los términos de la ley y abstenerse de publicar o comprometer información de los titulares.

10.2.1 POLITICA DE GESTION DE ACTIVOS

- El coordinador de TI será el encargado de llevar un historial de equipos de cómputo con su respectivo colaborador asignado.
- El coordinador de TI será el encargado de controlar el software instalado en cada activo, permitiendo o denegando nuevas aplicaciones requeridas por los colaboradores de la compañía.
- Los colaboradores estarán obligados a realizar la entrega de los activos al terminar su contrato verificando y registrando el estado de cada uno.
- Lo colaboradores serán responsables por el buen uso y estado de los activos entregados por la compañía.
- Los colaboradores deberán comunicar a su jefe directo cuando se presenten accesos no autorizados a su sistema y existan riesgos con los datos personales de los titulares o la operación.

10.2.2 POLÍTICA DE CONTRASEÑAS

- Los colaboradores de ESSENSALE S.A.S tienen el deber de cambiar sus contraseñas en ciertos periodos de tiempo, siendo notificados por el sistema o forzados para que realicen con más frecuencia el cambio de contraseña, deben contener como mínimo un número y una letra en mayúscula, debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se otorga o se niega el acceso a la información dependiendo del nivel de sensibilidad de los datos.

10.2.3 POLÍTICA DE ACCESO FÍSICO

- Se prohíbe el ingreso de personal externo como Vendedores PAP, Domiciliarios, visitas familiares a cualquier área de la compañía ESSENSALE S.A.S, todos los colaboradores son responsables de la atención de los mismos y la recepción gestionar el ingreso.
- Permitir el acceso a la información de los servidores de aplicaciones únicamente a las personas que pueden tener acceso a ella gestionando diferentes tipos de usuarios con sus respectivos privilegios para acceder a los datos sin comprometer el sistema.
- En caso de observar alguna anomalía como el intento de ingreso a la una de las instalaciones se deberá reportar inmediatamente a recepción o jefe inmediato.

10.2.4 POLÍTICA DE ACCESO FÍSICO

- Deben estar de acuerdo los directivos participantes en el área que requiere el nuevo personal y realizar el proceso de requisición de personal con el fin de poder iniciar el proceso de evaluación psicológico.
- Los nuevos colaboradores deben estar en capacidad de conocer, aplicar las políticas establecidas y firmar el acuerdo de confidencialidad con el fin de preservar los activos y la confidencialidad e la información.

10.2.5 POLÍTICA DE COPIAS DE SEGURIDAD

- Prevenir la pérdida de datos en caso de complicaciones realizando copias diarias de seguridad y disponer de un medio para recuperarlos en caso de una catástrofe

informática, accidente de sustancias peligrosas, eventos naturales o ataque; restaurar archivos que puedan haberse eliminado fortuitamente, corrompido, infectado por un virus informático u otros orígenes.

- Permitir el traslado de información a ubicaciones distintas realizando copias idénticas que no afecten el funcionamiento del sistema ni la fuga de datos personales.

10.2.6 POLÍTICA DE USO DE SOFTWARE Y PROTECCION

- El coordinador estará encargado de verificar el inventario de software instalado en los activos, realizando monitoreo de actualizaciones y nuevas aplicaciones que sea autorizadas y rechazar las innecesarias para las funciones del colaborador.
- El coordinador de TI deberá controlar el manejo de las peticiones, para aceptarlas o rechazarlas, los datos o variables recibidas se comprueban para que cumplan con las características esperadas o predefinidas. Todas las entradas del sistema deben pasar por el filtrado de los datos contenidos para corroborar su usabilidad.

10.2.7 POLÍTICA DE USO DE INTERNET

- El coordinador de soporte deberá implementar herramientas tecnológicas necesarias en sus sitios web tales como certificados digitales SSL para la transmisión segura de la información a través de internet, asegurando que terceros no puedan obtener o leer su contenido.
- El coordinador de desarrollo deberá verificar la fuente de las aplicaciones con los métodos de escáner de vulnerabilidades y pruebas de penetración para contrarrestar accesos no permitidos que aprovechen vulnerabilidades SQL (Inyección SQL), peticiones HTTP falsas (*Cross-site request forgery)*, código HTML y de scripts ejecutados en el cliente (Cross-Site Scripting XSS) y los intentos de acceso utilizando múltiples palabras (*ataque de diccionario)*.
- Los colaboradores no están autorizados a ingresar sitios web que no sean esenciales para el desarrollo de sus funciones
- Los colaboradores no podrán descargar ni instalar software sin licencia.

10.2.8 POLÍTICA DE ACCESO REMOTO

- Los colaboradores tendrán la responsabilidad de dar cumplimiento a sus funciones y compromisos ya establecidos.
- Los colaboradores accederán a la red local de la compañía mediante canales seguros VPNs.
- El coordinador de TI deberá monitorear todos los equipos conectados a la compañía, reconocer cada uno y verificar las peticiones realizadas.

10.3 PROCEDIMIENTOS

Con el propósito de dar solución a los hallazgos encontrados se presentan los procedimientos que pueden aplicarse a ESSENSALE S.A.S., para establecer controles a los procesos que requieran de la protección de los activos, la información y el mejoramiento continuo.

10.3.1 PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES (CLÁUSULA A.16.1.5)

En este procedimiento se busca resolver o contrarrestar los incidentes que pueden ocurrir en la compañía utilizando los mecanismos adecuados que permitan estar preparados si se da dicho incidente, y tener la capacidad de revelar cualquier debilidad en el sistema de gestión de seguridad, la confidencialidad, la integridad y disponibilidad.

Objetivos.

- Gestionar los incidentes de seguridad que se presenten en los activos de información de la compañía ESSENSALE S.A.S., que afecten la confidencialidad, integridad y disponibilidad de los servicios.
- Definir los responsables para llevar los procedimientos y custodiar el funcionamiento de la operación de la compañía.
- Implementar las salvaguardas necesarias a los incidentes que se presenten, contrarrestando el impacto generado.
- Definir y clasificar los incidentes presentados registrándolos en bitácoras para el análisis y toma de decisiones.

Alcance. El procedimiento comienza con la creación del personal encargado de dar soluciones o respuestas ante incidentes de seguridad de la información, realizando la detección, reporte, seguimiento, documentación y cierre del incidente.

Responsabilidades.

Coordinador de sistemas

- Resolver los incidentes y requerir apoyo a proveedores cuando sea necesario.
- Documentar los incidentes para la toma de decisiones que eviten una nueva ocurrencia del incidente.
- Velar por el cumplimiento del proceso.
- Custodiar maquinas afectadas para evitar la réplica del incidente.
- Clasificar los incidentes

Auxiliar de soporte técnico

- Evaluar si los eventos reportados son verdaderos y puedan causar daños a los activos.
- Identificar las causas del incidente, la referencia del fallo técnico de los activos afectados y las plataformas que han presentado alteraciones o caídas de servicios.

Colaboradores

- Reportar los incidentes presentados al coordinador de TI
- Describir el proceso que genera la falla en el activo.

Descripción.

El colaborador tiene el deber de notificar al coordinador de TI eventos anormales a los procesos realizados a diarios y que estos lleven también a fallas para los activos en el desarrollo de las funciones.

A continuación, se detallará la forma de proceder del coordinador de sistemas ante un incidente:

- Aislar la máquina de la red de la compañía desconectándolo de todos los medios configurados.

- Establecer una comunicación con el colaborador para realizar una retroalimentación del incidente ocurrido.
- El coordinador establece la causa del incidente con la información recolectada.
- El coordinador valida el impacto generado por el incidente y los sistemas que pudieron ser afectados en su entorno.
- El coordinador registra la evidencia para ejecutar las medidas necesarias y tratar el incidente.
- Documentar el incidente

10.3.2 PROCEDIMIENTOS DE OPERACIÓN PARA GESTIÓN DE TI (CLÁUSULA A.12.1.1)

El área de TI de la compañía ESSENSALE S.A.S contiene la infraestructura para el desarrollo de la operación, todo su sistema ERP y aplicaciones a la medida se encuentran alojadas en este lugar, implementando sus propios servidores, lo cual es necesario disponer de un sitio seguro que salvaguarde el sistema de información y las comunicaciones.

Objetivo. Definir las normas que contengan las condiciones ideales para mantener el sistema de información seguro de la compañía ESSENSALE S.A.S.

Alcance. El procedimiento se enfoca en las acciones que se deben implementar para el óptimo desarrollo de la central de información ubicado en el área de TI en la bodega 8 de ESSENSALE S.A.S en la ciudad de Santiago de Cali.

Responsabilidades.

Coordinador de sistemas.

- Realizar las adecuadas instalaciones y actualizaciones de componentes a cada uno los activos.
- Mantener el inventario de activos actualizado.
- Definir un plan constante de mantenimiento preventivo para los activos que influyen en la operación.

- Supervisar el control del mantenimiento preventivo prestado por terceros tanto al software como el hardware.
- Monitorear el acceso de visitantes a la bodega principal y el acceso al área de TI.

Gerente de tecnología.

- Definir las visitas periódicas con el proveedor tecnológico del sistema ERP
- Definir el plan presupuestal para el mantenimiento de los activos.

Descripción. El procedimiento establece las medidas que deben ser implementadas para el mantenimiento y óptimo funcionamiento de la operación en la central de información del a compañía ESSENSALE S.A.S.

- Sistema de alimentación ininterrumpida.

  Realizar un monitoreo a la UPS previniendo tiempos de inactividad y pérdida de información en el desarrollo de las operaciones.

  Se debe verificar el estado de las baterías, cargadores inversores e interruptores para garantizar la transferencia automática de corriente a los equipos ya que se ha comprobado que existe en la zona un alto porcentaje de cortes de fluido eléctrico en épocas lluviosas.

  Realizar una mejoría al tamaño de la UPS para permitir el suficiente tiempo y capacidad para el 100% de los equipos de la compañía logrando la salvaguarda de información.
- Servicio de canal de internet y seguridad de la red.

  Implementar un sistema de seguridad y monitorear el cortafuegos para el control de acceso en las instalaciones de ESSENSALE S.A.S verificando que se utilicen los recursos con la debida autorización, garantizando que los colaboradores sean los autorizados.

  Supervisar el acceso a terceros para el desarrollo de los servicios ofrecidos por los proveedores como actualizaciones o mejoramiento de infraestructura.

  Monitorear el directorio activo implementando un sistema de autenticación para contraseñas seguras y cantidad de accesos.

Monitorear el cifrado de información de los certificados instalados para su sistema ERP, intranet y extranet.

Asegurar la integridad de los datos orientado a la conexión TCP IP, contando con un canal alterno para evitar interrupciones en las funciones de los colaboradores, y la operación.

11. CONCLUSIONES

Se pudo apreciar que con la metodología de análisis y gestión de riesgos MAGERIT la compañía ESSENSALE S.A.S logre un mayor control en el uso de sus activos en cuanto a los posibles riesgos que pueda verse afectada, se realizó la identificación de activos, pensando también en los posibles nuevos activos debido a su gran crecimiento. Se detectaron los casos específicos los cuales se les asignó una dimensión de valoración realizando respectivamente un criterio de estimación para obtener una relación con dicha dimensión, en cuanto a las amenazas encontradas se registraron algunas de carácter importante que son significativas para la empresa.

Se implementó el anexo A de la norma NTC: ISO/IEC 27001 la cual trata de los objetivos de control donde se determinó que controles debían ser implementados para ayudar a la empresa tener un claro control de inventario con su referente documentación.

Finalmente, la implementación del SGSI para Essensale S.A.S ofrecerá mayor protección a los activos de la compañía, mejora la continuidad de la operación, contrarrestando todo tipo de amenaza generando confianza a nuevos clientes en el uso de los productos ofrecidos por los diferentes medios tecnológicos.

12. RECOMENDACIONES

- La gerencia de la compañía Essensale S.A.S tiene el deber de dar a conocer y mejorar los nuevos elementos que se presenten en el proyecto, capacitando a todo el personal de lo que es y puede lograr el SGSI para la continuidad del negocio y las operaciones.

- Continuar supervisando los activos de la compañía identificando de manera correcta como se ha realizado en el proyecto para contrarrestar las amenazas que se presenten en la compañía.

- Custodiar el cumplimiento de las políticas para el personal y nuevo personal que sea parte de la compañía y los procesos que afecten el sistema de información, monitorizando que el SGSI no pierda su integridad.

- Contar con personal capacitado en seguridad de la información para corregir de manera eficiente cualquier incidente o cambio en el SGSI.

BIBLIOGRAFIA

James Kurose y Keith Ross, Computer Networking: A Top-Down Approach, Séptima edición, Pearson, 2016, ISBN: 978-0133594140.

Santiago Medina Serrano, Windows Server 2016 NETWORKING VPN & DIRECTACCESS, Edición en español, publicado independientemente, 2017, ISBN: 520220677.

Antonio Luís Cardador Cabello, Implantación de aplicaciones web en entornos internet, intranet y extranet, Edición en español, IC EDITORIAL, 2015, ISBN:9788416433094

Eric Chou, Mastering Python Networking, Primera Edición, Packt Publishing, 2017, ISBN: 1784397008.

Matt Walker, CEH Certified Ethical Hacker Bundle, Tercera edición, McGraw-Hill Education, 2017, ISBN: 125983753X

Implementing the ISO / IEC 27001 ISMS Standard 2nd Edition Feb 1, 2016 de Edward Humphreys.

Beata Akselsen, Intrusion Detection Systems, Scitus Academics Llc, 2016, ISBN: 978-1681172668.

Kali Linux, The Kali Linux penetration testing platform, [Sitio web] [Consultado: 15 Febrero 2018] Disponible en: https://tools.kali.org/.

Todd Lammle, SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System, Primera Edición, Sybex, 2015, ISBN: 978-1119155034.

Peter Kim, The Hacker Playbook 2: Practical Guide To Penetration Testing Paperback, CreateSpace Independent Publishing Platform, 2015, ISBN: 978-1512214567.

Omar Santos, Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security (Networking Technology), Primera Edición, Cisco,2015, ISBN: 978-1587144387.

Yang-Im Lee (Autor), Cyber Security Management: A Governance, Risk and Compliance Framework, Primera Edición, Routledge, 2014, ISBN: 978-1472432094.

Enterprise Security Risk Management: Concepts and Applications - 29 Nov 2017, de Brian J Allen (Author), Rachelle Loyear (Author), Kristen Noakes-Fry (Editor).

PETERSON, Richard. Linux Manual de referencia, Segunda Edición, Osborne McGraw-Hill, Aravaca Madrid, 2000, ISBN: 0-07-212940-9.

Brian J Allen, Rachelle Loyear, Kristen Noakes-Fry, Enterprise Security Risk Management: Concepts and Applications, Rothstein Associates, 2017, ISBN: 978-1944480448M.