DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TI DE LA ORGANIZACIÓN LA ESPERANZA S.A FUNDAMENTADO EN LA NORMA ISO27001:2013

ARMANDO JOSÉ QUINTERO MIRANDA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA, NORTE DE SANTANDER
2016

DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TI DE LA ORGANIZACIÓN LA ESPERANZA S.A FUNDAMENTADO EN LA NORMA ISO27001:2013

ARMANDO JOSÉ QUINTERO MIRANDA

Tesis de grado para optar por el título:

Especialista En Seguridad Informática

Director de Proyecto:

Msc. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CÚCUTA, NORTE DE SANTANDER
2016

CONTENIDO

Pág.

.

LISTA DE FIGURAS

Pág.

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

RESUMEN

Cuando se habla de seguridad de la información, se piensa en medidas que permitan proteger la información en las empresas, manteniendo la disponibilidad, confidencialidad y la integridad de la información. La Seguridad de la información no debe ser comparada con seguridad informática esto a razón que la seguridad informática vela por la seguridad sobre los medios tecnológicos. En cambio, la seguridad de la información hace referencia a aquella información que tiene un valor relevante y especial que se debe proteger.

El aumento de incidentes de seguridad al interior de las empresas, hace necesario implementar políticas basadas en estándares de seguridad, que permiten guiar y gestionar los riesgos que se presentan en el desarrollo del negocio.

Palabras Clave: INFORMACIÓN, RIESGOS, SEGURIDAD, TECNOLÓGICO, POLÍTICAS.

DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TI DE LA ORGANIZACIÓN LA ESPERANZA S.A FUNDAMENTADO EN LA NORMA ISO27001:2013

Los sistemas de información cumplen un rol importante dentro de las organizaciones, por tanto, es significativo garantizar que la información y los datos generados sean seguros, confiables y oportunos. Es por esto que se hace necesario contar con mecanismos de seguridad de la información a fin de protegerla de cualquier evento inesperado u amenaza, que coloque en riesgo los datos de la organización.

Diseñar políticas, Objetivos, procesos y procedimientos permitirá determinar y establecer los controles de seguridad que apoyen a la gestión de los riesgos de seguridad de la información preservando la integridad, disponibilidad y confidencialidad de la información para la Organización La Esperanza S.A.

Con base a lo anteriormente expuesto, el objetivo principal de la investigación propuesta es diseñar un sistema de gestión de seguridad de la información para la empresa Organización la Esperanza S.A fundamentado en la norma ISO 27001:2013.

1. DISEÑAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TI DE LA ORGANIZACIÓN LA ESPERANZA S.A FUNDAMENTADO EN LA NORMA ISO27001:2013

La seguridad informática ha tenido un gran auge, en base a las cambiantes condiciones y nuevas plataformas tecnológicas que existen en el mercado actual. El lograr interconectarse por medio de redes ha traído de la mano el mejoramiento de la productividad dentro de las organizaciones, de igual forma aparecen nuevas amenazas que colocan en riesgo los sistemas de información, lo cual puede afectar la estabilidad y rendimiento de la organización. Siendo la información uno de los activos importantes dentro de la organización este requiere ser protegido de forma adecuada frente a amenazas que puedan presentarse y colocar en riesgo la continuidad del negocio.

Todas las organizaciones ya sean de gobierno o privadas, afrontan riesgos que conllevan al desarrollo de lineamientos que orientan sobre el uso adecuado de la tecnología, de esta forma sacar el máximo provecho y evitar la mala utilización e indebido de las mismas, lo cual puede generar problemas a las operaciones de la organización.

La disponibilidad, integridad y confidencialidad de la información se convierte en uno de los aspectos importantes para que el responsable o coordinador del área implemente los mecanismos necesarios partiendo de la norma ISO/IEC 27001 para garantizar el desarrollo de las actividades en un orden lógico para lo cual se utiliza el modelo (PHVA) planear, Hacer, verificar, Actuar.

La empresa Organización La Esperanza S.A en una entidad del sector privado, que tiene como objeto primordial de sus actividades promover planes y servicios en provisionalidad para sus clientes con altos estándares de calidad, teniendo siempre presente los valores del respeto y calidad humana de sus clientes. Esto ha generado un crecimiento a través de los años, llevando consigo a ampliar su

plataforma tecnológica, hardware, software, equipos de red, comunicaciones y recurso humano entre otros.

En entrevista formal con la Ingeniera Rosa Marina Castellanos, se logró verificar que existen diversas deficiencias en algunos de los servicios que en una forma u otra inciden en la seguridad de la Organización la Esperanza. Entre las deficiencias que se puntualizan se encuentran:

(a) Carencia de control de acceso al centro de computo
(b) Accesos a la base de datos por parte de los usuarios del área
(c) Carencia de un control continuo de la administración del sistema de Antivirus
(d) Las funciones de desarrollo y mantenimiento de políticas y estándares de seguridad no están definidas dentro de los roles de la empresa.

Este tipo de falencias genera problemas como: acceso de personas no autorizadas, falta de continuidad en los procesos administrativos, presencia de virus en los equipos de cómputo, perdida de información importante para la continuidad de procesos administrativos, manipulación de información por parte de usuario no autorizados entre otros. Este tipo de situaciones pueden ser gestionadas de forma adecuada contando con un plan de seguridad, que apoye a realizar la clasificación de las acciones a tomar para minimizar los incidentes de seguridad que se presenten.

2. FORMULACIÓN DEL PROBLEMA

La ISO 27001, expresa que un sistema de Gestión de la Seguridad de la Información, es un sistema que comprende la política, estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Se debe determinar con cuales herramientas dispone la alta dirección de la empresa Jardines de Esperanza S.A para llevar a cabo las políticas y objetivos de seguridad (integridad, confidencialidad y disponibilidad). Para proponer políticas de seguridad que proporcionen mecanismos cuya finalidad sea resguardar los activos de información y los sistemas que la procesan.

¿Cómo se puede mejorar la seguridad de la información para el área de TI de la organización La Esperanza?

3. OBJETIVOS DEL PROYECTO

3.1 GENERAL

Diseñar un sistema de gestión de seguridad de la información para el área de TI de la organización la esperanza s.a fundamentado en la norma ISO 27001:2013

a. ESPECÍFICOS

- Identificar los activos de información con los cuales cuenta la Organización la Esperanza S.A.

- Realizar un análisis del estado actual de la seguridad de la información del área de tecnologías de la información, acuerdo al anexo A de la norma ISO 27001:2013.

- Realizar un análisis de riesgos al área de Tecnología de la información de la Organización la Esperanza.

- Diseñar las políticas de seguridad de la información aplicables para el área de TI de organización enmarcadas en la norma ISO 27001:2013.

4. JUSTIFICACIÓN DEL PROYECTO

En la actualidad la seguridad informática está vinculada en muchas de las actividades que se realizan dentro de las organizaciones. El desarrollo de sus actividades cotidianas requiere de un adecuado funcionamiento dentro de sus sistemas de información y en especial de su seguridad. A pesar de las grandes inversiones que se realizan en dispositivos como: firewalls, sistemas antivirus, y demás dispositivos, no son suficientes para decir que un sistema de seguridad es seguro en relación a los principios de confidencialidad, disponibilidad e integridad de la información, de ahí que surge la necesidad de incorporar in Plan de Seguridad de la Información.

Los planes de Seguridad de la información le permiten a las empresas u organizaciones ya sean de carácter privado o público escalar en mayor forma todos los esfuerzos realizados para asegurar la información. Apoyando dentro de un marco legal y una metodología para analizar y gestionar los riesgos, asegurando la correcta implantación de medidas que garanticen el valor de la información de la empresa.

Teniendo en cuenta que los datos que se gestionan, procesan y almacenan en la oficina de TI de la empresa Jardines de Esperanza S.A, son de gran apoyo ya que brinda a los directivos de la empresa las herramientas administrativas necesarias para tomar decisiones que trascienden en las proyecciones comerciales de la empresa.

El desarrollo de este proyecto pretende, además, proponer los controles que pueden ser aplicados para garantizar la confidencialidad, integridad y disponibilidad de la información, establecer políticas, y objetivos claros que apoyen a mejorar los niveles de seguridad de la información de Organización la Esperanza S.A.

Entre las actividades propias a desarrollar al abordar la implantación de la norma ISO 27001 se encuentran:

- Definición de Políticas de Seguridad
- Identificación de riesgos
- Desarrollo de un plan de tratamiento de riesgos
- Desarrollo de programas de formación y concientización en seguridad de la información
- Elaboración de procedimientos y documentación asociada.

5. DELIMITACIÓN

El desarrollo del presente proyecto propone para el área de tecnologías de la información de la empresa Organización la esperanza el diseño de un plan de Seguridad de la Información. Basado en la norma ISO 27001:2013, identificando los activos, con los cuales cuenta la organización. Realizando un análisis de las amenazas y riesgos teniendo en cuenta la situación actual del área de tecnologías de la información de la empresa, todos estos componentes permitirán realizar un análisis y determinar las políticas de seguridad a ser diseñadas dentro de la Organización.

6. MARCO REFERENCIAL

6.1 MARCO TEÓRICO

SGSI "El Sistema de Gestión de Seguridad de la Información - SGSI, es un conjunto de políticas de administración de la información el cual consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización*."*.[1]

La información en unión con los procesos que forman parte del conjunto de políticas del SGSI se convierten en un activo de carácter importante para la empresa, estas llegan a ser esenciales para mantener un nivel de competitividad de cara a el logro de los objetivos de la organización.

Dentro del marco de la norma ISO27001 se establecen unos requisitos que permiten instaurar, establecer, salvaguardar y dar una mejora continua al sistema de Seguridad de la información según se conoce el "Ciclo de Deming ":[2] Planear, Hacer, verificar, Actuar. Estos requisitos son un punto clave que permite gestionar de manera eficiente el acceso a la información, buscando asegurar la integridad, disponibilidad e integridad de los activos de la empresa reduciendo los riesgos de información que se puedan presentar.

PLAN DE SEGURIDAD INFORMÁTICA (PSI) Un plan de seguridad informática reúne todos los procesos y servicios que se involucran en la seguridad de la información. Un PSI tiene en cuenta todos los aspectos de seguridad de la

---

[1] http://www.qbe.com.co/index.php/sistemas-de-riesgo-y-gestion/sgsi-sistema-de-gestion-de-la-seguridad-de-la-informacion

[2] http://www.pdcahome.com/5202/ciclo-pdca/

información para determinar los alcances de los procesos involucrados en la administración de las vulnerabilidades. Para que las políticas de seguridad sean aceptadas dentro de la empresa, estas deben integrarse a las estrategias del negocio a su misión y visión con el propósito que los altos directivos quienes son los que toman decisiones validen la importancia de las mismas y las incidencias en las proyecciones y utilidades de la empresa.

La definición y desarrollo de un plan de seguridad informática les permite a las empresas implantar cultura acerca de seguridad de información, adicionalmente definir alternativas de respaldo, políticas a seguir en momentos de crisis y los tiempos en los cuales está prevista la recuperación de la misma.

A pesar de no existir un documento con contenido específico acerca de los planes informáticos el mismo debe ser elaborado de manera tal que considere los intereses de los usuarios, teniendo en cuenta las razones por las cuales se establecen las políticas para los mismos.

ISO 27002 Recopilación de buenas prácticas para un SGSI en la compañía la cual contiene recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una compañía y describe los aspectos a analizar para garantizar la seguridad de la información y especifica los controles y medidas recomendables a implementar.

Si no se toman las medidas de seguridad necesarias, para asegurar los sistemas podría detonar amenazas y causar riesgos en los activos de información, lo que podría generar pérdidas económicas para las empresas. Una de las formas para mitigar los riesgos que pueden afectar los activos es la elaboración de normas, políticas y concientizar a los usuarios sobre la aplicación e implementación de buenas prácticas para reducir la probabilidad de un impacto a los cuales pueden estar expuestos los activos.

La norma ISO 27002 es una herramienta que permite establecer políticas con el objetivo de reducir los riesgos que presentan los activos de la empresa, de tal forma que al momento de generarse una incidencia estos se minimizan y se asegura la continuidad del negocio, posteriormente se genera un ahorro en costos derivados de la eliminación de sobrecostos e inversiones innecesarias, de igual forma no puede faltar la certificación por parte del sistema de gestión de seguridad de la información, de esta forma se contribuye a mejorar el nivel competitivo de la empresa en el mercado.

ISO 27005-2008 Establece las directrices para la gestión del riesgo en la seguridad de la información. Para lo cual previamente se debe tener conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002, que es aplicable a todo tipo de organizaciones que tienen la intención de gestionar los riesgos que puedan comprometer la seguridad de la información. La norma ISO 27005 fue diseñada por el comité técnico conjunto ISO/ IEC JTC, esta norma provee directrices en materia de gestión del riesgo en la seguridad de la información, brindando un soporte a los requisitos del sistema de gestión de seguridad de la información(SGSI), sin embargo, la norma no define ninguna metodología de forma específica para la gestión del riesgo.

Para comprender la norma es necesario tener los conocimientos de procesos y términos descritos en la norma ISO 27001.

GESTIÓN DEL RIESGO Las empresas administran la información conexa a sus procesos ya sea de forma física o digital sin tener en cuenta el medio de almacenamiento o transmisión, estos recursos son importantes para mantener la continuidad del negocio.

No todos los sistemas de información están ligados a un sistema informático, los sistemas se pueden representar como personas, objetivos, etc. Es por ello que la gestión de riesgo permite establecer, examinar, evaluar y clasificar el riesgo, para identificar e implementar de manera oportuna herramientas que permitan controlarlo.

Incorporar la gestión del riesgo y la seguridad de la información genera costos económicos, costos en relación al tiempo y el consumo de otro tipo de recursos, que en muchas ocasiones las pequeñas empresas no cuentan con ellos; razón por la cual estas empresas no establecen la gestión del riesgo como una de sus prioridades.

La gestión del riesgo en su forma habitual comprende cuatro fases:

Análisis: Se establecen los elementos del sistema que requiere protección, sus vulnerabilidades, y las amenazas que ponen en riesgo una vez calculado el grado del riesgo.

Clasificación: Establece si los riesgos que se encuentran y los que restan son aceptables.

Reducción: Especifica las medidas de protección. Adicionalmente sensibiliza a los usuarios conforme a las medidas que se deben tomar.

Control: Se analiza el funcionamiento, certeza y medidas para determinar los ajustes y medidas deficientes.

Figura 1. Gestión Del Riesgo

Fuente https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/

Todos los procesos se fundamentan sobre políticas de seguridad, reglas y directrices que hacen parte del marco operante del proceso con la finalidad de potenciar las capacidades y reduciendo vulnerabilidades reduciendo de esta forma los riesgos. Orientar un funcionamiento operativo, que garantice la aplicación y corrección de buenas prácticas.

Análisis del Riesgo El análisis de riesgos permite realizar una evaluación e individualización de los activos, inicialmente se debe realizar la identificación de los activos que serán protegidos, esta identificación comprende realizar una comparación del riesgo de forma detallada teniendo en cuenta criterios definidos anteriormente.

La comparación de los riesgos permite lograr un nivel razonable de consenso de cara a los objetivos que están planteados y hacen parte del horizonte de la empresa. De esta forma se aseguran niveles mínimos que permiten generar indicadores estratégicos que permiten medir y realizar la evaluación del riesgo.

Al interior del análisis del riesgo surgen elementos que forman parte del concepto de análisis del riesgo.

PROBABILIDAD Se puede realizar la definición de la probabilidad como la cantidad de veces que puede que ocurra un evento, teniendo como objeto de referencia la ocurrencia de acciones que permiten establecer una medida. Existen diferentes probabilidades tales como incendios (información estadística de empresas aseguradoras), estos datos permiten que se establezca de forma objetiva la probabilidad de ocurrencia de un hecho. Por ejemplo, cuando se irrumpe de manera no autorizada a un centro de datos.

AMENAZAS la definición de amenaza hace referencia a toda aquella operación que trate de infringir en contra de la seguridad de la información de una organización. Las amenazas surgen a raíz de la materialización de vulnerabilidades las cuales son tomadas por atacantes y sacar el máximo provecho comprometiendo la seguridad, integridad y confidencialidad de la información. Muchas de las amenazas surgen de la carencia de capacitación por parte de usuarios acerca de temas en seguridad de la información y cuál es la importancia de aplicar reglas y mecanismos a fin de disminuir los ataques que podrían materializarse en amenazas

VULNERABILIDAD La palabra vulnerabilidad refiere a una falencia del sistema que le permite a un atacante trasgredir la confidencialidad, integridad, disponibilidad del sistema, datos y aplicaciones. Las vulnerabilidades hacen referencia a diversos fallos por no implementar mecanismos tecnológicos para salvaguardar la información. Un ejemplo claro de vulnerabilidad es la tenencia de un software antivirus y este no estuviese actualizado de forma correcta y oportuna, lo cual podría generar posibles ataques y ocasionar daños de índole mayor.

ACTIVOS Se puede identificar un activo como a todos los elementos que poseen un valor para la organización y que deben protegerse, tales como aplicaciones software, equipos de tecnología, equipos de comunicación. Todas las empresas deben tener identificados los activos de tal forma de tener planes de contingencia ante desastres que se puedan presentar, los activos deber ser documentados y clasificados con el fin de incrementar el valor interno y poder determinar el impacto y los niveles de riesgo respectivos.

IMPACTO Son el resultado de ocurrencia de las amenazas que por lo regular son negativas, financieras, estructurales, o de largo plazo. Por eso siempre será oportuno preguntarnos ¿Que tan malo podría llegar a ser si ocurre? Siempre se debe tener presente que al momento de realizar el análisis de riesgos los administradores de TI deben proyectar a futuro cual sería el impacto que estas posibles vulnerabilidades u amenazas pueden generar al interior de la organización.

INFORMACIÓN El termino información refiere a un conjunto de datos ya sean numéricos, gráficos, almacenados en cualquier medio, la información permite a usuarios tomar decisiones y aporta a su conocimiento.

TECNOLOGÍA DE LA INFORMACIÓN Tecnología de la información es el compendio de herramientas tecnológicas y de comunicación que tienen la finalidad de mejorar los procesos de comunicación entre los usuarios y los diversos mecanismos tecnológicos con el objetivo de mejorar los ambientes sobre los cuales se realiza la aplicación del conjunto de herramientas de TI. En la actualidad las tecnologías de la información al igual que las comunicaciones se encuentran ligados de tal forma que cambian y facilitan la vida diaria de las personas, acortando distancias y facilitando el acceso a este tipo de recursos.

6.2 MARCO LEGAL

El alto y creciente auge de las tecnologías de la información al interior de las organizaciones y más aún en la vida diaria ha generado un alto impacto que genera un marco normativo que permita salvaguardar y garantizar la libre implementación de este tipo de servicios tecnológicos.

La Ley 1273 de 2009 diseño nuevos y diversos tipos penales que se relacionan con delitos informáticos y la protección de los datos con penalidades que van de 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. [2]

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

- Artículo 269A: Acceso abusivo a un sistema informático.
-Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Artículo 269C: Interceptación de datos informáticos.
-Artículo 269D: Daño informático.
-Artículo 269E: Uso de software malicioso.
-Artículo 269F: Violación de datos personales.
-Artículo 269G: Suplantación de sitios web para capturar datos personales. [3]

[2] Ley 1273 http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
[3] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

Todo en la vida cotidiana de los seres humanos cambia de manera sustancial, hoy por hoy las personas pueden realizar pagos y diversos trámites desde la comodidad de sus hogares u oficina en una computadora. Es por ello que las leyes juegan un papel importante en la implementación de mecanismos que controlen y protejan todos los datos que circulan por la red o que almacenan y procesan información, ya que estas tienen como finalidad el salvaguardar los derechos fundamentales, así como los mecanismos para su protección.

6.3. MARCO CONTEXTUAL

HISTORIA ORGANIZACIÓN LA ESPERANZA S.A. En el año de 1978 dos empresarios de la región Norte Santandereana, El Dr. Enrique Cuadros y el Dr. Álvaro Riscos inician el proyecto de un parque cementerio para la ciudad de Cúcuta y el área metropolitana. Y es así que el 5 de diciembre de 1982 se da apertura al parque cementerio en la ciudad de Cúcuta denominado “Parque cementerio Jardines de Esperanza”.

Con la apertura y gran acogimiento del parque cementerio en la ciudad este grupo de empresarios emprenden una nueva tarea de planear la construcción de un parque cementerio en la ciudad de Ocaña en norte de Santander, de igual forma en 1985 se da inauguración al parque cementerio en la ciudad de Ocaña. No obstante, surge la necesidad de brindar servicios complementarios a estos parques cementerios lo que conlleva el 23 de junio de 1988 a abrir en la ciudad de Cúcuta Casa de Funerales La Esperanza. De la misma forma y en el año de 1993 se dio apertura a la casa de funerales en la ciudad de Ocaña.

Con el crecimiento administrativo surge la necesidad de crear instalaciones que brinden el apoyo correspondiente a este tipo de actividades administrativas, en el año de 1996 se da apertura a la sede administrativa al igual que a la nueva casa de Funerales La Esperanza, Ubicados en la ciudad de Cúcuta en la Diagonal Santander # 8 – 93.

El crecimiento comercial de la entidad y la necesidad de expansión y cobertura de otro tipo de regiones conlleva a realizar estudios en la región Santandereana donde años más tarde se da la inauguración del primer Mausoleo en altura en el área metropolitana de la ciudad de Bucaramanga. Destacándola como una de las empresas con una alta cobertura en el campo de prestación de servicios exequias en la región.

Los altos niveles de calidad empleados al interior de la organización impulsan a la empresa en un amplio crecimiento tanto en infraestructura, tecnología, comercio y de calidad lo que lleva a la empresa a certificar la calidad de prestación de sus servicios en el año 2008 obteniendo la certificación ISO 9001 versión 2008 en gestión comercial y servicios exequiales. Hoy en día Organización La Esperanza cuenta con más de 32 años de experiencia que los han convertido en una de las empresas líder en la prestación de servicios exequiales.

La empresa cuenta con el respaldo de los grupos de la Red Exequial y el grupo Prever del sector funerario lo que le brinda una presencia y cubrimiento de servicios en 87 municipios de Colombia.

La empresa Organización La Esperanza S.A en una entidad del sector privado, que tiene como objeto primordial de sus actividades promover planes y servicios en provisionalidad para sus clientes con altos estándares de calidad, teniendo siempre presente los valores del respeto y calidad humana de sus clientes. Esto ha generado un crecimiento a través de los años, llevando consigo a ampliar su plataforma tecnológica, hardware, software, equipos de red, comunicaciones y recurso humano entre otros.

MISIÓN Servir, aportando beneficios en vida a nuestros clientes, comercializando y prestando servicios exequiales, apoyándolos con sensibilidad, experiencia y la fuerza de nuestras manos, construyendo relaciones que trasciendan a través del respeto, incorporando procesos de innovación en nuestros productos y servicios.[4]

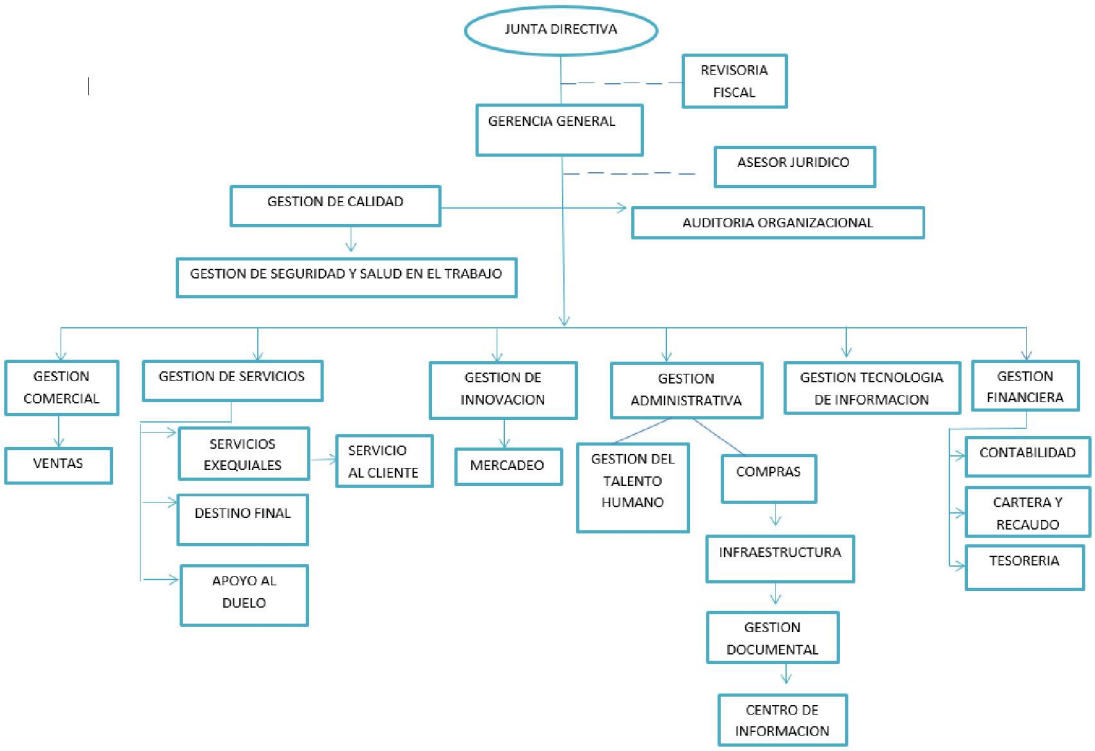
VISIÓN Organización La Esperanza, será en el 2017, el líder en el oriente colombiano en la prestación de servicios exequiales, comercialización de productos en previsión y memorialización de los fallecidos, con reconocimiento y proyección nacional.[5]

[4] Organización la esperanza S.A.
[5] Organización la esperanza S.A

7. ESTRUCTURA ORGANIZACIONAL

Organización la Esperanza está conformada según la estructura organizacional que se muestra a continuación:

Figura 2. Diagrama Organizacional Organización la Esperanza S.A



Fuente: Organización La Esperanza S.A.

8. METODOLOGÍA

El desarrollo del presente proyecto se realiza en diferentes fases las cuales se describen a continuación:

Fase 1 identificación de los activos dentro de la organización en materia de seguridad de la información.

Actividades:

- Encuestar a personal de diferentes áreas a fin de identificar el estado actual de seguridad de información de la empresa.

Fase 2 En segunda instancia realizar el análisis del estado actual teniendo en cuenta el anexo A de la norma ISO 27001:2013 los cuales se agrupan en 14 dominios y 113 controles.

Actividades:

- Realizar el análisis del Anexo A de la norma ISO 27001:2013

Fase 3 Realizar El análisis de Riesgos que vincula los activos utilizados en el área de Tecnologías de la información.

Actividades:

- Realizar la identificación de las amenazas en conjunto del área de TI de organización la esperanza s.a

- Realizar la identificación de Vulnerabilidades que pueden tener mayor afectación en la oficina de TI de organización la esperanza s.a.
- Realizar la identificación de Salvaguardas ya sean físicos o lógicos que permitan reducir los riesgos que se puedan presentar.

- Realizar la evaluación del Riesgo en el cual el área de TI priorice los de problemas potenciales en los cuales puede incurrir.

- Realizar el tratamiento del riesgo por parte del área de TI de organización la esperanza s.a.

Fase 4 Diseñar las políticas de seguridad que serán aplicadas al área de tecnologías de la información de Organización la Esperanza S.A.

9. DESARROLLO DEL PROYECTO

En relación a los objetivos que se persiguen en el desarrollo del presente proyecto, fue diseñado un cuestionario con el cual se podrá comprobar que existen problemas de seguridad de información y la posibilidad de aceptación del diseño de un plan de seguridad de la información.

De igual forma se realizó la entrevista entre el Líder del Área de tecnología y el ("encuestador") donde se obtuvo información acerca de problemas específicos que se están presentando dentro del área de tecnología de la Organización La Esperanza S.A. Con la utilización de esta técnica "Entrevistas" se analizaron cuáles son los causales de los problemas que se presentan, siendo los siguientes:

- El área de TI no cuenta con un plan de seguridad de información.

- La aplicación de medidas de seguridad que garanticen que la información que viaja por la red está protegida es poco convencional, se limitan al nivel de seguridad que brinda el proveedor del servicio de comunicaciones.

- No cuentan con mecanismos software para reporte de incidencias que se presentan al interior de la organización en materia de TI, por lo general cuando se detectan errores en las aplicaciones se reportan vía e-mail al equipo de soporte quien brinda la atención primaria a este tipo de situaciones.

- Los empleados de las diferentes áreas de la empresa tienen poco conocimiento en materia de seguridad de información.

- La aplicación de configuraciones que se consideran estándar implican que personal externo a la organización utilice mecanismos para escanear la red y acceder a información de la empresa.

- No se realiza una evaluación de riesgos que permita detectar cuales son las posibles vulnerabilidades o amenazas que pueden afectar la operación normal del área de TI de la organización.

9.1 ANÁLISIS DE RESPUESTAS

En materia de seguridad de la información diseñar un plan de seguridad informática le permite al equipo de TI conocer la importancia, el valor y el nivel de impacto frente a las vulnerabilidades que se presentan al interior de la empresa. Luego de aplicar la encuesta (Anexo1), se logra obtener los resultados reflejados en la tabla 2.

Analizando dichos resultados se puede reflejar que con respecto a la pregunta 1 que obtuvo un 30% de respuesta por el SI, se puede concluir que son pocos los usuarios del área de TI que tienen conocimiento de los estándares en seguridad de la información al interior de la empresa.

Al realizar la pregunta 2, cuando se obtuvo respuesta negativa a la respuesta 1, se expuso una idea general acerca de planes de seguridad de la información, obteniendo como resultado que las personas a quienes se les aplico el cuestionario respondieran al si en un 100%.

Tabla 2. Tabulación respuesta encuesta

	Respuesta	
Preguntas	Si	NO
Pregunta 1	30%	70%
Pregunta 2	100%	0%
Pregunta 3	100%	0%
Pregunta 4	100%	0%
Pregunta 5	100%	0%
Pregunta 6	80%	20%
Pregunta 7	20%	80%
Pregunta 8	40%	60%
Pregunta 9	0%	100%
Pregunta 10	100%	0%

Fuente: Autor

La respuesta obtenida acerca de la pregunta 3 y 4 de un 100% para el SI, refleja la aceptación por parte del equipo de TI y demás usuarios a quienes se les aplico la encuesta, relacionado que a estos usuarios se les ha expuesto que es un plan de seguridad de información y cuáles son los aspectos positivos de aplicarlos en la empresa.

La capacitación y orientación a los usuarios acerca de temas como la seguridad de la información es importante ya que permite que los usuarios identifiquen posibles vulnerabilidades que se puedan presentar en la empresa. Es por ello que se percibe un SI del 100% en la pregunta número 5.

La aplicación de planes de seguridad al interior de las organizaciones trae consigo cambios que de alguna manera u otra afectan la operación diaria, ya que trae consigo restricciones que algunos usuarios no aceptan en primera instancia, sin embargo muchos apoyan y ven con buenos ojos que implementar este tipo de planes de seguridad beneficiaran y apoyaran el crecimiento en calidad de información y seguridad de la misma, lo cual se refleja en la respuesta de la pregunta 6 en la cual se nota un SI del 80% y un NO del 20%.

Al interior de la organización existen planes de contingencia, pero no cubren la recuperación ante un desastre naturas, según el análisis realizado por parte del encuestador según lo expuesto por el líder de TI de la empresa la información que se tiene almacenada en las instalaciones no cuenta con medios de protección.

La información tampoco se almacena en medios diferentes a DVD o servidores ubicados físicamente fuera de las instalaciones, lo cual recuperarse de una catástrofe natural seria de alto costo para la empresa ya que toda la información esta almacenada en un espacio físico sin condiciones adecuadas ante este tipo de situaciones es por ello que la respuesta de la pregunta 7 tiene como resultado un Si del 20% que son personas que tienen algún conocimiento del que se debe hacer en estas situaciones y un NO del 80%.

Algunos de los usuarios a los cuales se les aplico la encuesta no tenían claro el concepto de evaluación de riesgos por eso el resultado del 60% en un NO, la detección de los riesgos permiten analizar y evaluar de forma permanente la magnitud de los daños que podrán causar, de esta forma diseñar estrategias que permitan minimizar el impacto de los riesgos presentados, los usuarios que contestaron SI con un 40%, conocen de alguna manera que el realizar una evaluación de riesgos constituye para el área de TI una herramienta para planificar soluciones ante los incidentes que se presenten de forma objetiva y a la medida de la organización.

El área de TI no ha realizado una evaluación de vulnerabilidades de la red, según lo informan los integrantes del área es por eso que se registra un porcentaje del 100% del NO en la pregunta 9, más aun cuando en la actualidad existen diversos proyectos que permiten en múltiples plataformas realizar escaneos de puertos, análisis de tráfico, detectar vulnerabilidades en sitios web, u aplicaciones que se ejecuten en servidores web y otros más que se puedan ejecutar sobre la red de datos de la empresa.

La empresa cuenta con software antivirus actualizado reflejado en un 100% por el SI de la pregunta 10, el software que utiliza actualmente la empresa cuenta con software antivirus con los componentes de detección de malware, antivirus de archivos, protección en navegación web y servicio de antivirus para servidores.

9.2 IDENTIFICACIÓN DE ACTIVOS

En esta fase se realiza un informe de los resultados que se obtuvieron durante el levantamiento de información de los activos de Organización La Esperanza S.A. el objetivo primordial es realizar la caracterización de los elementos por tipo de activo.

Se denomina activo a todo aquel recurso del sistema de información que se encuentra relacionado y que cumple con los objetivos establecidos por la alta dirección. Uno de los activos que se considera esencial es la Información ya que alrededor de estos datos o información se pueden identificar cuáles son los activos que más repercuten dentro de la Organización.

A continuación, se presenta la clasificación de activos realizada para Organización la Esperanza S.A donde se detallan activos como Hardware, Software, Comunicaciones, Equipamiento Auxiliar.

9.2.1 Disponibilidad

Para realizar la valoración del criterio de disponibilidad debemos responder a la pregunta de cuál sería la importancia que tendría el activo si no estuviese disponible.

Tabla valoración de disponibilidad

CRITERIO DE EVALUACIÓN		
DISPONIBILIDAD	VALOR	DESCRIPCIÓN
BAJO	1	Se debe disponer de la información al menos un 15% del tiempo
MEDIO	2	Se debe disponer de la información al menos un 50% del tiempo
ALTO	3	Se debe disponer de la información al menos un 95% del tiempo

Fuente: Autor

11.2.2 Integridad

Para este criterio se debe responder sobre la importancia del activo si fuese alterado sin autorización alguna ni control

Tabla valoración de integridad

CRITERIO DE EVALUACIÓN		
INTEGRIDAD	VALOR	DESCRIPCIÓN
BAJO	1	No relevante, no genera alto impacto si hay carencias de información
MEDIO	2	la información debe estar de forma correcta y completa en al menos un 50%
ALTO	3	La información debe estar de forma correcta y completa en al menos un 98%

Fuente: Autor

11.2.3 Confidencialidad

Este Criterio se define en base a la importancia que tendría el activo si se accediera de manera no autorizada.

Tabla valoración de Confidencialidad

CRITERIO DE EVALUACIÓN		
CONFIDENCIALIDAD	VALOR	DESCRIPCIÓN
BAJO	1	Daño Bajo, el incidente no trascenderá del área de afectación
MEDIO	2	Daño relevante, los incidentes generados afectan a otras áreas
ALTO	3	Daño de forma catastrófica, se compromete la imagen y reputación de la empresa

Fuente: Autor

9.3 CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Tabla 3 Equipamiento Auxiliar

Tipo de Activo	Código / Nombre	Servicios Soportados	Datos e Información Comprendida	Áreas Asociadas	Grado de Criticidad		
					Confidencialidad	Integridad	Disponibilidad
[AUX] Equipamiento Auxiliar	UPS	Sistemas de alimentación ininterrumpida	Soporta los Equipos del centro de Datos	Oficina de TI	Bajo	Bajo	Bajo
	Aire Acondicionado	Equipos de Climatización	Mantiene temperatura en centro de computo	Todas las áreas	Medio	Medio	Medio
	Armario Rack	Mobiliario: armarios, etc.	Gabinete para equipos Rack, protección de personal no autorizado	Oficina de TI	Bajo	Bajo	Bajo
	Discos para Copias de Seguridad	Almacenamiento de información, DVD	DVD para almacenamiento de información, copias de respaldo	Oficina de TI	Medio	Alto	Medio
	Puestos de trabajo	Mobiliario para estaciones de trabajo, mesas, sillas, etc.	Mobiliario	Todas las áreas	Bajo	Bajo	Bajo

Fuente: Autor

Tabla 4 Redes de Comunicación

Tipo de Activo	Código / Nombre	Servicios Soportados	Datos e Información Comprendida	Áreas Asociadas	Grado de Criticidad		
					Confidencialidad	Integridad	Disponibilidad
[COM] Redes de Comunicación	Radio Enlace Principal–Cúcuta	Transmisión de datos	Datos, Internet	Todas las áreas	Alto	Alto	Alto
	Radio Enlace Parque cementerio Tienda Store Huellas	Transmisión de datos	Datos	Todas las áreas	Alto	Alto	Alto
	Conexión Datos Cúcuta - Ocaña	Transmisión de datos	Datos, Internet	Todas las áreas	Alto	Alto	Alto
	Conexión Datos Cúcuta - Bucaramanga	Transmisión de datos	Datos, Internet	Todas las áreas	Alto	Alto	Alto
	Canal de Comunicación Mega-Wireless	Transmisión de datos	Datos, Internet (Canal Secundario)	Todas las áreas	Alto	Alto	Alto

Fuente: Autor

Tabla 5 Software

Tipo de Activo	Código / Nombre	Servicios Soportados	Datos e Información Comprendida	Áreas Asociadas	Grado de Criticidad		
					Confidencialidad	Integridad	Disponibilidad
[SW] Aplicaciones Software [os] Sistema Operativo	Base de Datos DB2	Administración de base de datos Operaciones administrativas	Datos Personales de Clientes, Proveedores y personal de la empresa	Oficina de TI	Bajo	Bajo	Bajo
	Base de Datos Progress	Administración de base de datos Operaciones Contables	Administración de base de datos Operaciones Contables	Contabilidad, Oficina OTI	Bajo	Bajo	Bajo
	Sistema Datajardes	Operación Administrativa y Comercial	Operación Administrativa y Comercial	Todas las áreas	Medio	Bajo	Medio
	Kaspersky Internet Security	Antivirus estaciones de trabajo, servidores, protección software mal intencionado, spam, malware	Antivirus estaciones de trabajo, servidores, protección software mal intencionado, spam, malware		Bajo	Bajo	Bajo
	Aplicación Integrity	Datos, informes gerenciales	Información contable, cuentas, pagos a terceros, información financiera	Contabilidad	Medio	Bajo	Bajo
	Clientes de correo Electrónico	Clientes de correo Electrónico	Información relacionada con cuantas de correo	Todas las áreas	Medio	Medio	Bajo
	Sistema Operativo Windows 2008 server	Bases de Datos, Fuentes de aplicaciones propias	Bases de Datos, Fuentes de aplicaciones propias	Oficina de TI	Bajo	Bajo	Bajo
	Sistema Operativo Windows 2012 server	Gestión de identidades de usuarios	Información relacionada con sesiones de usuarios, control de acceso remoto a estaciones de trabajo	Oficina de TI	Bajo	Bajo	Software
	Sistema Operativo Windows 2003 server	Servidor de archivos	Documentos, imágenes , videos, etc.	Todas las áreas	Bajo	Bajo	Medio
	Sistema Operativo Suse 10 Server	Servidor de archivos, almacenamiento de ejecutables para operación	Documentos, imágenes , videos, fuentes de aplicaciones	Todas las áreas	Bajo	Bajo	Bajo

		administrativa					
	Sistema Operativo Red Hat Linux	Servidor de archivos	Documentos, imágenes , videos, fuentes de aplicaciones	Todas las áreas	Bajo	Bajo	Bajo
	Sistema Operativo Windows 7 Profesional	Configuración de sistema en estaciones de trabajo	Ejecución de Aplicaciones desarrolladas por la empresa, configuraciones de estaciones de trabajo, credenciales de usuarios	Todas las áreas	Medio	Medio	Medio
	Office 2010 Home and Bussines	Aplicaciones Ofimáticas	Aplicaciones Ofimáticas Word, Excel, Power Point, etc.	Todas las áreas	Bajo	Medio	Bajo

Fuente: Autor

Tabla 6 Hardware

Tipo de Activo	Código / Nombre	Servicios Soportados	Datos e Información Comprendida	Áreas Asociadas	Grado de Criticidad		
					Confidencialidad	Integridad	Disponibilidad
[HW] Equipos Informáticos (Hardware)	Servidor de Recaudo	Bases de datos	Información relacionada con recaudos de clientes de forma electrónica	Todas las áreas	Alto	Alto	Alto
	Servidor DHCP	Servicios DHCP, Firewall	Información relacionada con direccionamiento ip	Todas las áreas	Medio	Alto	Alto
	Servidor DB2	Bases de datos Operaciones Administrativas	Información relacionada con las ventas, Recursos Humano, Clientes, labores Administrativas	Todas las áreas	Alto	Alto	Alto
	Servidor de Datos Progress	Bases de datos, operaciones comerciales	Información Contable, Cuentas, Pagos	Contabilidad, cartera	Alto	Alto	Alto
	Servidor Web	Aplicaciones Web, Portal Institucional	Cuantas de correo, portal web empresarial, aplicaciones móviles(Recaudo)	Todas las áreas	Medio	Medio	Alto
	Servidor Directorio Activo	Gestión de identidades	Gestión de identidades, Manejo de credenciales de Usuarios	Oficina de TI	Alto	Alto	Alto
	Servidor De Documentos	Manejo de documentos, servicios de directorios	Todo tipo de documentos, imágenes videos, fuentes de desarrollos propios de la empresa	Todas las áreas	Medio	Alto	Alto

	Servidor De Antivirus	Manejo de virus informáticos	Almacenamiento de firmas de virus	Oficina de TI	Medio	Bajo	Medio
	Computadores de Escritorio	Operación Administrativa, ejecución de aplicaciones propias del negocio	Aplicaciones, documentos, imágenes	Todas las áreas	Bajo	Medio	Alto
	Computadores Portátiles	Operación Administrativa, Alta gerencia	Aplicaciones gerenciales, documentos, informes Estadísticos	Gerencia Administrativa, Comercial y Financiera	Medio	Bajo	Medio
	Switch Datos HP	Transferencia de Datos	Datos información dependencias	Oficina de TI			
	Switch Datos Cisco	Transferencia de Datos, Servidores	Datos, información entre servidores servicios de comunicación	Oficina de TI	Alto	Alto	Alto

Fuente: Autor

10. ANÁLISIS ACTUAL DE SEGURIDAD DE LA INFORMACIÓN DEL ÁREA DE TECNOLOGÍAS DE LA INFORMACIÓN DE ACUERDO AL ANEXO A DE LA NORMA ISO 27001:2013

<table>
<tr><td>A.5</td><td colspan="4">POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.5.1</td><td colspan="4">Orientación de la dirección para la gestión de la seguridad de la información</td></tr>
<tr><td colspan="5">Objetivo: Brindar la orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td rowspan="5">A.5.1.1</td><td rowspan="5">Políticas para la seguridad de la información</td><td rowspan="5">Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Las políticas de la seguridad de la información proveen un direccionamiento estratégico acorde a los requerimientos de la organización, cumpliendo con leyes y regulaciones. Este documento es de carácter obligatorio en la norma ISO 27001:20123,</td></tr>
<tr><td colspan="2">IMPLEMENTADO</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">No se tiene implementado un SGSI, no existen documentos que contemple las políticas de la seguridad de la información</td></tr>
</table>

Observación: No se ha realizado el diseño de un SGSI, pero si es aplicable al área de TI en razón de proteger información que es de vital importancia para la empresa.

<table>
<tr><td rowspan="5">A.5.1.2</td><td rowspan="5">Revisión de las políticas para la seguridad de la información</td><td rowspan="5">Control: las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su convivencia, adecuación y eficacia continúas.</td><td colspan="2">APLICA</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">La validación de las políticas de manera periódica ayudan a validar si las políticas establecidas están acordes a los objetivos del negocio</td></tr>
<tr><td colspan="2">IMPLEMENTADO</td></tr>
<tr><td>SI</td><td>NO</td></tr>
<tr><td colspan="2">Se deben establecer políticas de seguridad de la información y ser validadas de forma periódica.</td></tr>
</table>

Observación: Con la aplicación de políticas de seguridad se minimizan los daños y amenazas y se acrecientan las oportunidades y de esta forma asegurar la continuidad del negocio.

A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.6.1	**Organización Interna**		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización			
A.6.1.1	roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información	**APLICA** **SI** / **NO** La asignación de roles, especifica cada una de las funciones que debe desempeñar cada miembro del área de tecnología de la información. **IMPLEMENTADO** **SI** / **NO** Se deben definir los roles y asignar las responsabilidades para cada miembro del área de tecnología.

Observación: La aplicación e implementación de roles en el área de TI permite llevar un control de las actividades que realizan los integrantes del área de TI.

A.6.1.2	Separación de Deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	**APLICA** **SI** / **NO** La definición de las áreas y sus actividades correspondientes apoyan la gestión general de la organización. **IMPLEMENTADO** **SI** / **NO** Se definen las áreas de trabajo dependiendo de las afinidades de cada una de las mismas, apoyando las actividades entra las mismas buscando el logro de los objetivos trazados al interior de la organización.

Observación: La definición de las áreas de trabajo establece métricas de desarrollo y seguridad al ser definidos los espacios en los cuales los integrantes del área ejecutan sus actividades.

A.6.1.3	Contacto con las Autoridades	Control: Se deben mantener contactos apropiados con las autoridades pertinentes	**APLICA** **SI** / **NO** Mantener una comunicación con las autoridades pertinentes garantiza que al momento de ocurrencia de algún incidente se puede dar aviso a las autoridades y aplicar las medias de ley correspondientes **IMPLEMENTADO** **SI** / **NO** Se debe mantener contacto con las autoridades a fin de que se presenten incidentes y sea aplicada la ley correspondiente.

Observación: No se implementa este control a razón que no están definidas políticas que permitan dar aviso a las autoridades pertinentes.

A.6.1.4	Contacto con grupos de Interés especial	Control: Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	**APLICA** **SI** / **NO** El contacto con grupos y foros en matrería de seguridad informática permite debatir acerca de nuevas prácticas que se puedan implementar dentro de la organización **IMPLEMENTADO** **SI** / **NO** se comparte información que puede ser de utilidad, se verifica la posibilidad de implementar conocimiento adquirido de otras fuentes

Observación: La adopción de nuevas prácticas en materia tecnológica y poder debatir cómo se pueden incorporar a los procesos que existen actualmente es una fortaleza para el líder de equipo ya que refleja que cuenta con un equipo que está a la vanguardia de nuevas tecnologías aplicables.

A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**		
A.6.2	**Dispositivos móviles y teletrabajo**		
Objetivo:	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles		
.6.2.1	Política para Dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	**APLICA** **SI** / **NO** La utilización de teléfonos móviles dentro de la organización genera riesgos de fugas de información ya que se puede extraer información en los dispositivos. **IMPLEMENTADO** **SI** / **NO** Aplicar políticas de uso de dispositivos dentro de la organización, evitar la transferencia de información por medio de móviles y la utilización de los mismos dentro de áreas seguras.

Observación: Se puede realizar la aplicación de políticas de utilización de teléfonos móviles dentro del área de TI, esto garantiza que no se filtre información el momento de tomar decisiones de alto impacto al interior del área.

A.6.2.2	Teletrabajo	Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	**APLICA** **SI** / **NO** La implementación del teletrabajo, apoya a los empleados de la organización que tienen algún tipo de discapacidad o enfermedad que le impida estar de manera presencial en su puesto de trabajo habitual **IMPLEMENTADO** **SI** / **NO** Se deben utilizar mecanismos que aseguren el acceso a información procesada o por procesar cuando se realiza teletrabajo

Observación: La aplicación del teletrabajo no se aplica al interior de la organización se implementan herramientas de acceso remoto solo para temas de soporte a usuarios.

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1	Antes de Asumir el Empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y so idóneos en los roles para los que se consideran.			
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y debe ser proporcionales a los requisitos del negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos	APLICA SI / NO La verificación de los antecedentes es parte primordial de la selección de los empleados ya que con esta se puede evidenciar si la persona es idónea para el puesto que le será asignado. IMPLEMENTADO SI / NO Se realizan las validaciones en los diferentes entes de validación de antecedentes, procuraduría, fiscalía policía etc.

Observación: En conjunto del área de talento humano se realiza la verificación de los aspirantes a vacantes a algún cargo al interior del área de TI, de tal forma que sean personas que cumplan con los requisitos de ley.

A.7.1.2	Términos y condiciones de Empleo	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuento a la seguridad de la información	APLICA SI / NO La definición del objeto contractual tanto a funcionarios como contratistas permite delimitar las funciones que realizara dentro de la organización IMPLEMENTADO SI / NO Se definen las funciones y actividades que debe realizar el empleado al momento de la selección se le debe explicar muy bien cuáles son los alcances de las actividades asignadas

Observación: Se realiza la socialización de las funciones y actividades que realizaran los integrantes del área de TI.

A.7.2	Durante la Ejecución del Empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y so idóneos en los roles para los que se consideran.			
A.7.2.1	Responsabilidades de la Dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	**APLICA** **SI** / **NO** Una vez definidas las responsabilidades y funciones dentro del proceso contractual A.7.1.2 el empleado debe cumplir a cabalidad los lineamientos establecidos dentro de la organización en materia de seguridad de la información. **IMPLEMENTADO** **SI** / **NO** Se deben implementar acuerdos de confidencialidad en los cuales se le indica al empleado cuales son las penas legales por no cumplir las directrices de seguridad de la información establecidas en la empresa.

Observación: Se implementa el acuerdo de confidencialidad con todos y cada uno de los nuevos empleados que ingresan a la organización y al área de TI, se realiza socialización del acuerdo para que el nuevo integrante conozca y entienda el alcance e implicaciones legales que tiene lugar la firma del mismo.

A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización y en donde sea pertinente, los contratistas, deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo	**APLICA** **SI** / **NO** La educación a los empleados sobre políticas y nuevas técnicas de seguridad de la información les permiten mantenerse actualizados, para así aplicar estos conocimientos al interior de la organización **IMPLEMENTADO** **SI** / **NO** Se deben implementar capacitaciones ya sea de forma virtual o Presencial a los empleados del área de tecnología a fin de capacitarse en nuevas técnicas, estándares que pueden aplicarse en seguridad informática

Observación: No se realizan capacitaciones al área de TI en materia de seguridad, se deben programar capacitaciones en las cuales intervenga todo el equipo de TI, y este a su vez pueda realizar difusión de conceptos a los usuarios finales para mayor comprensión acerca de la importancia de implementar seguridad en la organización.

A.7.2.3	Proceso Disciplinario	Control: Se debe contar con un proceso formal, en el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	**APLICA**	
			SI	**NO**
			Al momento de realizar la legalización del contrato ya sea del funcionario o contratista se les explica cuáles son los aspectos legales si llegase a realizar alguna violación las políticas de seguridad establecidas en la organización	
			IMPLEMENTADO	
			SI	**NO**
			Todos los empleados que ingresan a la organización deben firmar el acuerdo de confidencialidad, en el cual se exponen las penalidades interpuestas por violar la seguridad de la información de la organización.	

Observación: Todos los empleados diligencian y firman el acuerdo de confidencialidad el cual es presentado al momento de haber sido seleccionados para un cargo dentro del área de TI, teniendo presentes la penalidad en la que puede incurrir si viola alguna de las clausulas interpuestas en el acuerdo.

A.7.3	**Terminación y cambio de Empleo**			
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.				
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	**APLICA**	
			SI	**NO**
			La aplicación de normativas legales dentro de la organización al momento de incorporar un empleado garantiza que no incurra en faltas que puedan generar falencias o fugas de información al interior de la organización.	
			IMPLEMENTADO	
			SI	**NO**
			Se debe establecer un tiempo de validez de los acuerdos de confidencialidad una vez el funcionario o contratista se ha desvinculado de la organización.	

Observación: La duración de la validez del acuerdo de confidencialidad es en común acuerdo con el jefe de área de talento humano y el líder del área de TI.

A.8	GESTIÓN DE ACTIVOS		
A.8.1	Responsabilidad de los Activos		
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas			
A.8.1.1	Inventario de Activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	**APLICA** **SI** / **NO** La identificación de los activos permite realizar una estimación de los riesgos y amenazas, los cuales pueden afectar el funcionamiento de la organización. **IMPLEMENTADO** **SI** / **NO** Se deben implementar mecanismos que agilicen la identificación de activos e instalaciones de la organización, existen diversos agentes que pueden ser utilizados para realizar esta labor, Aranda GLPI etc.

Observación: La aplicación e implementación de herramientas de software libre o de pago que permitan llevar un control del inventario tecnológico que reside en la organización es una de las tareas del líder del área de TI ya que debe seleccionar en base a su experiencia la mejor opción y designar a un integrante del equipo para que realice de forma correcta el inventario de equipos tecnológicos.

A.8.1.2	Propiedad de los Activos	Control: Los activos mantenidos en el inventario deben tener un propietario	**APLICA** **SI** / **NO** La asignación de los implementos y equipos de trabajo a los empleados es garante a que exista un responsable y si ocurre algún deterioro por mala manipulación este sea el responsable de los mismos. **IMPLEMENTADO** **SI** / **NO** Se realiza la asignación de los activos mediante el acta de entrega de bienes, la cual responsabiliza al empleado a mantener en óptimas condiciones los equipos de trabajo asignados.

Observación: Se deben entregar los equipos para el desarrollo de las labores de los empleados no solo del área sino de toda la organización, por medio de un acta de entrega la cual designa la responsabilidad el buen uso al usuario.

A.8.1.3	Uso Aceptable de los Activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con la información e instalaciones de procesamiento de información.	**APLICA**	
			SI	**NO**
			Los usuarios que tienen acceso a información procesada deben conocer las implicaciones legales a los cuales son acreedores si utilizan la información con fines diferentes a los trazados e asignados dentro de la organización.	
			IMPLEMENTADO	
			SI	**NO**
			Se realiza la debida identificación de los documentos que son utilizados por los empleados (Formatos, Líneas de cartera, etc.) para realizar las actividades para las cuales fueron contratados.	

Observación: Todos los activos entregados son marcados y relacionados con los usuarios a los cuales se les realiza entrega mediante formatos que deben ser diligenciados por el encargado de realizar la entrega de los bienes.

A.8.1.4	Devolución de Activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo	**APLICA**	
			SI	**NO**
			Los empleados realizan la devolución de los bienes asignados tanto físicos como digitales e información, ya sea al inicio de las actividades laborales como en el desarrollo de sus ejercicios como funcionario o contratista, así la empresa realiza cálculos de detrimento de los activos en sus cortes financieros.	
			IMPLEMENTADO	
			SI	**NO**
			Los empleados por medio del acta de entrega de bienes realizan la entrega de los bienes activos entregados, se realiza checklist de la información entregada y se validan que los permisos y credenciales entregados sean desactivados.	

Observación: A todos los empleados se les requiere la devolución de todos los equipos y dispositivos tecnológicos que hubiese recibido para el desarrollo de sus actividades para las cuales fue contratado, se verifica que sus credenciales de acceso al sistema y puntos de lectura biométrica sean dados de baja.

A.8.2	Clasificación de la Información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.			
A.8.2.1	Clasificación de la Información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	**APLICA** **SI** / **NO** El archivo de los documentos debe realizarse teniendo en cuenta la ley general de archivo LEY 594 de 2000, la cual es explicita de los principios generales que rigen la función archivística y la forma en particular como debe ser archivado un documento y los cuidados que se deben tener hacia los mismos. **IMPLEMENTADO** **SI** / **NO** El área de gestión documental realiza el archivo correspondiente y vela por el óptimo cuidado de los documentos que en su área reposan, teniendo en cuenta los lineamientos establecidos para el archivo de los documentos por parte de la alta dirección.

Observación: Todos los documentos generados en el área de TI son remitidos y custodiados por el área de gestión documental.

A.8.2.2	Etiquetado de la Información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	**APLICA** **SI** / **NO** La implementación de las políticas y procedimientos para clasificar la información agiliza los procesos de consulta de documentos físicos que se requieran en cualquier instante de tiempo. **IMPLEMENTADO** **SI** / **NO** La Organización clasifica la información dependiendo del serial del documento y la fecha de generación del documento.

Observación: Todos los documentos que se generan al interior del área de TI y demás son remitidos al área de gestión documental quien clasifica y archiva según la reglamentación de archivo

A.8.2.3	Manejo de Activos	Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	**APLICA** **SI** / **NO** La clasificación de activos según su característica permite definir las áreas responsables de los mismos. **IMPLEMENTADO** **SI** / **NO** Los activos están clasificados según su tipo, tecnológicos, mercadeo, ventas, casa de funerales, estos detallan que tipos de activos opera en las dependencias al interior de la organización.

Observación: El área de gestión documental se encarga de realizar la clasificación de los documentos generados por las áreas.

A.8.3	**Manejo de Medios**		
Objetivo: Evitar la Divulgación, modificación, el retiro o la destrucción no autorizados de Información almacenada en los medios			
A.8.3.1	Gestión de Medios Removibles	Control: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	**APLICA** **SI** / **NO** Los usuarios deben mantener el resguardo del a información que contienen en los medios removibles asignados, de igual forma deben informar cualquier cambio o eliminación de la información. **IMPLEMENTADO** **SI** / **NO** Los medios de almacenamiento asignado a los usuarios ya sean USB, DVD, Discos externos deben ser utilizados únicamente para transporte de la información, todos los dispositivos deben ser escaneados cada vez que se ingresen a una estación de trabajo de la organización. Todos los dispositivos deben someterse a revisión periódica para verificar las políticas establecidas.

Observación: A los usuarios se les informa que no deben utilizar medios de almacenamiento que no estén autorizados o sean asignados por el área de TI, los dispositivos que están asignados a usuarios autorizados son escaneados de forma periódica en busca de infecciones.

A.8.3.2	Disposición de los Medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran utilizando procedimientos formales.	**APLICA** **SI** / **NO** Se realiza la devolución de los medios removibles asignados al área de tecnología a fin de que se genere el reporte respectivo al área de talento humano para que se descargue de los activos que el contratista o funcionario tienen asignado. **IMPLEMENTADO** **SI** / **NO** Todos los medios removibles que no serán utilizados deben borrados siempre y cuando se genere copia de seguridad e la información contenida en la misma, se deben almacenar en lugares seguros, la información que se encuentra en los medios debe estar disponible en la mayor cantidad de tiempo posible.

Observación: Los dispositivos que fueron entregados a los usuarios autorizados deben ser devueltos por los usuarios, a estos dispositivos se les realiza un análisis con herramientas antivirus y es generada una copia de seguridad de la información, y se realiza un borrado del dispositivo de forma controlada por uno de los integrantes del equipo de TI se completa la plantilla de devolución del medio removible y se relaciona la capacidad y estado del mismo.

A.8.3.3	Transferencia de medios Físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	**APLICA** **SI** / **NO** Se deben aplicar políticas de protección de información, la documentación que contienen los medios extraíbles debe ser protegida con mecanismos de seguridad idóneos al caso. **IMPLEMENTADO** **SI** / **NO** Se deben aplicar políticas de protección de información, encriptar el contenido de los mismos, instalar o verificar de forma periódica contra código malicioso o ataques mal intencionado.

Observación: Los dispositivos se encuentran reguardados en el área de almacén, la información que se encuentra en los dispositivos no cuenta con mecanismos de encriptación de datos que permita blindar la información de ataques de terceros o cualquier código malicioso.

A.9	CONTROL DE ACCESO		
A.9.1	Requisitos del Negocio para control de acceso		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información			
A.9.1.1	Política de Control de Acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	APLICA SI / NO Establecer un control de acceso que permita controlar que personal no autorizado no ingrese a las áreas a las cuales se procesa información o a diversas áreas. IMPLEMENTADO SI / NO se tiene definido que todo el personal que trabaja en la organización debe ingresar su huella dactilar en el control biométrico para controlar el acceso a las instalaciones administrativas en las cuales se procesa información, los agentes externos deben registrarse y obtener un pase que les permita el acceso al área correspondiente.

Observación: Todos los integrantes del área de Ti deben estar registrados en el equipo biométrico el cual permite el acceso al área de TI donde se encuentran los equipos de procesamiento de datos.

A.9.1.2	Acceso a Redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	APLICA SI / NO Se definen las categorías del personal contratista o socios de la organización a los cuales se les permite el ingreso a la red, auditando los recursos a los cuales tienen acceso. IMPLEMENTADO SI / NO Se realiza el control de acceso a la red mediante políticas de firewall que permiten el acceso a la red con limitaciones de acceso a recursos tecnológicos de la organización

Observación: Se realiza control de tráfico y acceso a niveles de la red mediante políticas definidas en un servidor firewall, el cual segmente la red, por áreas de trabajo y sucursales, solo los usuarios con el nivel de acceso autorizado pueden ingresar a otro nivel dentro de la red.

A.9.2	Gestión de acceso de Usuarios			
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios				
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso	**APLICA**	
			SI	**NO**
			Los empleados que ingresan a la organización deben tener un usuario y contraseña de los aplicativos sobre el cual desarrollara sus funciones.	
			IMPLEMENTADO	
			SI	**NO**
			Se realiza una asignación de permisos a aplicaciones software las cuales ejecutara durante el desarrollo de las funciones asignadas, el personal de TI recibe una solicitud del área de talento humano para la creación de los permisos correspondientes.	

Observación: Al momento de ser contratado el usuario el grupo de talento humano informa al área de TI cuales son las funciones del nuevo usuario, se diligencia el formato de asignación de credenciales el cual detalla a que aplicaciones podrá tener acceso y el perfil asociado a esa cuenta.

A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios	**APLICA**	
			SI	**NO**
			El área de talento humano informa cuales son las actividades y funciones dentro de la organización de los nuevos empleados de esta forma se establece un lineamiento que permita definir en base a las funciones asignadas definir a que aplicaciones tendrá acceso	
			IMPLEMENTADO	
			SI	**NO**
			Se deben implementar mecanismos que identifiquen de forma clara cuales son los aplicativos a los cuales tendrá acceso el empleado, para lo cual se debe implementar una plantilla de asignación de credenciales a los empleados donde se definen cuáles son los permisos y aplicativos a los cuales tendrá acceso	

Observación: Se realiza el diligenciamiento del formato de asignación de credenciales el cual detalla a que aplicaciones podrá tener acceso y el perfil asociado a esa cuenta, de esta forma se controla al acceso a los usuarios a aplicaciones a las cuales quieran acceder de forma no autorizada.

A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	**APLICA**	
			SI	**NO**
			La asignación de permisos a aplicaciones software debe ser vigilada y auditada por uno de los integrantes del área de TI, esta responsabilidad debe recaer sobre uno de los miembros que tenga el conocimiento de cuáles son las diferencias de roles en las aplicaciones ya sean generadas por los desarrolladores de la organización o las tercer izadas.	
			IMPLEMENTADO	
			SI	**NO**
			Solo uno de los integrantes del área de TI debe tener el control de que permisos son otorgados a los empleados de la organización de esta forma se evita que diferentes integrantes del área ejecuten la aplicación de permisos.	

Observación: Uno de los integrantes del equipo de TI es el responsable del diligenciamiento y asignación de los permisos de acceso a las aplicaciones las cuales hacen parte del ejercicio diario de la organización.

A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	**APLICA**	
			SI	**NO**
			La entrega de credenciales para acceder a información se debe realizar implementando mecanismos que garanticen que otros usuarios no tendrán acceso a esas credenciales asegurando uno de los principios de la seguridad de la información " La Confidencialidad"	
			IMPLEMENTADO	
			SI	**NO**
			La asignación de claves secretas para acceder a información se debe realizar utilizando mecanismos tales como correo electrónico en el cual se detalle cual es el usuario asignado, la contraseña para acceder y la validez de la misma, se le ha de recordar al usuario en que aplicaciones deberá usar este tipo de autenticación	

Observación: La entrega de las credenciales se realiza de forma informal, por consiguiente, no se puede garantizar que el usuario confirme el recibido de las credenciales y logre acceder a las aplicaciones si ningún contratiempo.

A.9.2.5	Revisión de los Derechos de acceso de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	**APLICA**	
			SI	**NO**
			La entrega de información de autenticación se debe constatar que el usuario ha recibido la contraseña emitiendo una alerta al momento de recibir y utilizar la información de acceso suministrada de forma segura	
			IMPLEMENTADO	
			SI	**NO**
			Se implementan alertas que identifiquen el momento en el que el usuario realiza el cambio de contraseña, tales mecanismos deben realizar la validación de las mismas al momento de solicitar la actualización automática de las credenciales de autenticación solicitando el ingreso de la misma para validar la veracidad de la cuenta.	

Observación: El sistema genera una alerta de cambio, mediante la confirmación vía correo electrónico de la acción realizada por el usuario al momento de realizar el cambio de clave de acceso al sistema.

A.9.2.6	Retiro o Ajuste de los derechos de Acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	**APLICA**	
			SI	**NO**
			Una vez se ha completado la labor designada al usuario u empleado se deben retirar las credenciales entregadas a fin de evitar faltas a la seguridad de la información o este decida tomar retaliaciones en contra de la organización, la modificación de permisos debe presentarse por mecanismos de información que notifiquen tales cambios	
			IMPLEMENTADO	
			SI	**NO**
			El área de talento humano debe informar acerca de los cambios o terminaciones de contratos a los que tenga lugar un empleado a fin de realizar los cambios en los perfiles y permisos asignados para con el mismo.	

Observación: Una vez se informa al área de TI sobre la terminación de contrato de algún usuario se debe diligenciar el formato de credenciales indicando la revocatoria de los permisos respectivos.

A.9.3	Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación			
A.9.3.1	Uso de Información de autenticación Secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	**APLICA** **SI** / **NO** El incumplimiento de las políticas establecidas para el uso de credenciales de forma única, genera incidentes de seguridad lo que impacta en que las mismas dejen de ser seguras y facilita que se cometa suplantación de identidad al momento de realizar cualquier transacción al interior de la organización. **IMPLEMENTADO** **SI** / **NO** Se deben realizar capacitaciones acerca de la correcta utilización de las credenciales asignadas, haciéndoles ver cuáles son las sanciones a las cuales se hacen acreedores.

Observación: Se realizan socializaciones acerca de las sanciones y medidas legales que son tomadas ante la generación de un incidente de seguridad por parte de un usuario.

A.9.4	Control de acceso a sistemas y aplicaciones		
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones			
A.9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	**APLICA** **SI** / **NO** Se debe validar que en verdad el usuario que ingresa sea quien dice ser, este tipo de accesos es posterior a la autenticación, se debe velar por que el usuario tenga acceso solo a los recursos que tiene permitidos **IMPLEMENTADO** **SI** / **NO** Los usuarios deben ser conscientes de aplicar buenas prácticas de manejo de los accesos otorgados, que sean dentro de los horarios establecidos para el desarrollo de sus funciones, todos los servicios de la red deben ser susceptibles a controles de acceso

Observación: Se implementan mecanismos que garantizan la valides de autenticación del usuario que ingresa acceder al sistema, como lo son ingresar caracteres Capcha.

A.9.4.2	Procedimiento de Ingreso Seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	**APLICA**	
			SI	**NO**
			Teniendo en cuenta las aplicaciones y servicios a los cuales tiene acceso el usuario, se definen los mecanismos de ingreso a los mismos validando siempre que los ingresos se realizan en entornos de trabajo seguros y realizando la autenticación correspondiente.	
			IMPLEMENTADO	
			SI	**NO**
			Los usuarios utilizan los mecanismos de ingreso a los servicios y aplicaciones asignados teniendo presente las medidas de ingreso establecidas	

Observación: El área de TI de la organización mantiene en las aplicaciones que están instaladas para la ejecución de labores propias de los usuarios controles de acceso que permiten identificar que el usuario que está tratando de acceder al aplicativo es quien dice ser.

A.9.4.3	Sistema de gestión de Contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas	**APLICA**	
			SI	**NO**
			No se realiza generación de contraseñas con mecanismos que aseguren la calidad e integridad de las mismas.	
			IMPLEMENTADO	
			SI	**NO**
			se deben implementar mecanismos de generación de contraseñas que al momento de vencer el plazo máximo de utilización de las mismas este interactúe con el usuario y valide el grado de complejidad teniendo en cuenta los lineamientos y políticas de generación de contraseñas	

Observación: No se tiene implementado un tiempo de expiración de uso de contraseña, este tipo de mecanismos promueve que los usuarios deben realizar cambios de claves así si se trata de acceder o captar la contraseña esta ya no estará en funcionamiento ya que ya fue cambiada.

A.9.4.4	Uso de programas utilitarios Privilegiados	Control: Se deben restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones	**APLICA** **SI** / **NO** Los controles y políticas de instalación de software no autorizado le permiten al departamento de TI el inventario de software a nivel general de la organización. **IMPLEMENTADO** **SI** / **NO** Se debe restringir y controlar la instalación de software no autorizado, diseñando políticas que soliciten credenciales de alto nivel de administración.

Observación: Los usuarios de la organización tienen asignado para el desarrollo de sus tareas un equipo tecnológico (PC, Portátil, ETC.) que utilizan la infraestructura tecnológica de la organización, pero no pueden realizar instalaciones de software a menos que esté autorizado por el jefe del área y explicando el motivo por el cual lo requiere.

A.9.4.5	Control de Acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	**APLICA** **SI** / **NO** Se establece un responsable a fin de mantener la integridad de las aplicaciones software propio de la organización. **IMPLEMENTADO** **SI** / **NO** Se debe establecer un mecanismo formal para realizar cualquier actualización, modificación o restauración sobre el código fuente, a los mismos solo se debe autorizar el acceso al líder de desarrollo quien deberá auditar los procesos realizados en los mismos.

Observación: Los cambios que sean efectuados al código fuente de las aplicaciones debe tener aprobación del comité evaluador, seguido de documento que indica cual es el cambio a realizar específicamente, los cambios que se deben realizar deben ser analizados por el equipo de desarrollo, se deben crear y colocar en producción sobre ambientes de pruebas antes de ser colocados en sistemas que están en marcha.

A.10	CRIPTOGRAFÍA		
A.10.1	Controles Criptográficos		
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.			
A.10.1.1	Política sobre el uso de controles Criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	APLICA SI / NO Cuando se aplican políticas criptográficas se debe tener en cuenta los objetivos del negocio y la información a proteger, considerar las regulaciones y restricciones que se pueden aplicar. IMPLEMENTADO SI / NO Implementar mecanismos de protección criptográficas por medio de software PKI o entes que generen certificados digitales de confianza con altos estándares, utilizar software de encriptación de archivos y/o documentos.

Observación: No se implementan mecanismos criptográficos ya que no se cuenta con los recursos para contratar con un ente generador de certificados digitales.

A.10.1.2	Gestión de Llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	APLICA SI / NO Las llaves criptográficas debe ser generadas por entidades certificadoras a fin de garantizar la validez y confiabilidad de las llaves generadas, adicionalmente las llaves deben tener un factor de tiempo de expiración lo cual asegura que las llaves no se utilizaran de forma indefinida dando lugar a incidentes de seguridad IMPLEMENTADO SI / NO se deben implementar mecanismos de claves publicas ya sean simétricos o asimétricos, que permiten realizar transacciones y envíos de información de forma segura

Observación: Este tipo de técnicas criptográficas solo se implementa a través de mecanismos TOKEN para temas bancarios y no son controlados por el área de TI de la organización.

A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A.11.1	**Áreas Seguras**		
Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.			
A.11.1.1	Perímetro de Seguridad Física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	**APLICA** **SI** / **NO** La organización debe tener un área de atención o medios de control de acceso físico a las áreas o edificios donde funcionen áreas de procesamiento de información o equipos que sean sensibles a daños por terceros. **IMPLEMENTADO** **SI** / **NO** Los perímetros de seguridad al interior de la organización deben estar debidamente definidos, donde existan puertas se deben tener controles de acceso biométrico a los cuales solo el personal autorizado tenga acceso, sistemas de detección de humo e sistemas contra incendios.

Observación: Se tiene implementado mecanismos de control de puerta por medio de control biométrico en el cual solo los usuarios que están autorizados pueden acceder a ese tipo de áreas.

1.2	Controles de Acceso Físicos	Control: Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	**APLICA** **SI** / **NO** Todas las personas externas a la organización deben ser registradas, se debe tener presenta al momento del registro la fecha, hora de ingreso, motivo por el cual ingresa, hora de salida. **IMPLEMENTADO** **SI** / **NO** Las áreas al momento de realizar algún cambio al interior de la organización, deben validar los niveles de permisos y accesos de manera física asignados. Todo visitante que ingrese a las instalaciones debe estar siempre acompañado durante su estadía en la organización.

Observación: Todo visitante que ingresa a la entidad es anunciado, se registra el número de documento y se le entrega un distintivo que lo acredita como visitante y la sección en la cual se encontrara realizando alguna actividad, si es encontrado en otra área diferente a la cual está autorizado a ingresar será retirado y el líder de área deberá responder ante la subdirección por las actuaciones del visitante.

A.11.1.3	Seguridad en oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones	**APLICA**	
			SI	**NO**
			Todos los lugares en los cuales se encuentren equipos de procesamiento de información deben estar protegidos de cualquier tipo de acceso no autorizado, empleando mecanismos de control y autenticación, sistemas de monitoreo como cámaras de seguridad tanto en entradas y salidas.	
			IMPLEMENTADO	
			SI	**NO**
			Se implementan mecanismos de control biométrico para que tanto empleados como agentes externos puedan acceder a zonas administrativas, se debe diligenciar el formato de ingreso para agentes externos y se debe portar la identificación que acredita como visitante a las instalaciones.	

Observación: Se relacionan en el formato de control de visitantes a todos aquellos externos que realizaran actividad alguna al interior de las instalaciones, una vez el personal es autorizado a ingresar este debe portar el distintivo que lo acredita como visitante en la empresa.

A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentales	**APLICA**	
			SI	**NO**
			Se deben tener zonas para el resguardo de los equipos en los cuales se procesa información, estas zonas deben tener todas las medidas de seguridad estándar contra desastres naturales.	
			IMPLEMENTADO	
			SI	**NO**
			Se diseñan y aplican protecciones contra desastres naturales, fuego, inundaciones, terremotos, todos los activos de información deben protegerse para evitar daños que generen altos costos a la organización o sean irreparables.	

Observación: Se tienen diseñados planes de contingencia ante emergencias o desastres naturales, pero ante estas circunstancias los equipos no se encuentran protegidos a fin de evitar daños.

A.11.1.5	Trabajo en Áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	**APLICA** **SI** / **NO** Todos los centros de procesamiento de información deben estar resguardados de cualquier acceso no autorizado A.11.1.3 **IMPLEMENTADO** **SI** / **NO** se deben aplicar mecanismos de protección física, con lineamientos para trabajar en zonas seguras, se deben controlar todos los accesos no autorizados por personas que pertenezcan o no a la organización, evitar el acceso no autorizado de dispositivos móviles Tablet etc.

Observación: No se tienen implementados mecanismos para restringir el uso de dispositivos móviles tales como Smartphone y otros dispositivos de este tipo.

A.11.1.6	Áreas de Despacho y carga	Control: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**APLICA** **SI** / **NO** La entrada y salidas de mercancía deben ser verificadas por la empresa de seguridad de una forma rigurosa con la finalidad que no ingresen materiales de alto riesgo y que se cuente con la autorización respectiva de entrada. **IMPLEMENTADO** **SI** / **NO** Las áreas de recepción de equipos u otros materiales deben estar debidamente identificados, todos los equipos que ingresen o salgan de las instalaciones deben ser registrados y en aquellos casos que se requiera una autorización por parte del coordinador de área.

Observación: El área de almacenaje de equipos y demás implementos se encuentra debidamente identificados, solo la persona encargada a esta área puede acceder.

A.11.2	Equipos		
Objetivo: Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.			
A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	**APLICA** **SI** / **NO** Todos los equipos de cómputo en general deben estar protegidos contra fallas que se puedan presentar en el suministro de energía o amenazas de medio ambiente con mecanismos de soporte alternos. **IMPLEMENTADO** **SI** / **NO** Se debe tener un monitoreo sobre variables tales como fuego, donde deben existir extintores y sistemas de detección de humo, en el caso de Robo todos las personas que ingresan deben portar la identificación que los acredita como visitantes , en el caso de inundaciones los equipos deben estar ubicados a un nivel superior de calle o donde se pueda almacenar agua en altas proporciones

Observación: No se tienen implementados sistemas de detección de humo, sistemas contra incendios u cualquier otro tipo de catástrofe natural o causada por cualquier agente externo, los equipos de procesamiento de datos se encuentran en un lugar al interior de la empresa y al alcance de los integrantes del área de TI.

A.11.2.2	Servicios de Suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro	**APLICA** **SI** / **NO** Se debe contar con los mecanismos de protección esenciales para garantizar la continuidad del negocio A11.2.1 **IMPLEMENTADO** **SI** / **NO** Todos los elementos eléctricos y redes de energía deben estar separados según normas técnicas. Los equipos deber estar protegidos contra fallas eléctricas o sobrecargas de energía, los dispositivos de respaldo de energía deben contar con especificaciones técnicas según la cantidad de equipos a ser soportados.

Observación: Los equipos de transferencia de datos se encuentran protegidos contra fallas eléctricas, los dispositivos se encuentran conectados a un sistema de energía ininterrumpida (UPS), todo el sistema cuenta con mecanismos de puesta a tierra, diseñados bajo especificaciones técnicas que garanticen el respaldo contra descargas eléctricas.

A.11.2.3	Seguridad del Cableado	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se deben proteger contra interceptación, interferencia o daño.	**APLICA**	
			SI	**NO**
			La infraestructura debe estar acondicionada para el transporte del cableado estructurado siguiendo normas técnicas. Se demarcan las zonas por la cuales se transporta el cableado sin generar grandes cambios en la infraestructura.	
			IMPLEMENTADO	
			SI	**NO**
			Todo el cableado de la red debe estar protegido contra interferencias y manipulación de cualquier persona, preferiblemente que no esté a la vista del personal de la empresa.	

Observación: El cableado de datos no se encuentra visible a los usuarios se lleva protegido por ducteria plástica el mantenimiento del cableado es realizado por personal especializado, la ducteria plástica por la cual se lleva el cableado no protege de interferencias que se puedan presentar.

A.11.2.4	Mantenimiento de Equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	**APLICA**	
			SI	**NO**
			Se deben realizar mantenimientos según las recomendaciones del fabricante, los soportes realizados deber ser ejecutados por personal tanto autorizado como calificado para estas tareas, se deben tener presentes las pólizas de garantías y hasta qué punto son responsabilidad los mantenimientos a los equipos.	
			IMPLEMENTADO	
			SI	**NO**
			Tantos dispositivos UPS como generadores de energía deben ser revisados y probados a fin de detectar posibles fallas que puedan afectar la continuidad de la empresa, se debe contar con mecanismos de apagado en casos de emergencias de cualquier índole.	

Observación: Se realizan de forma programada pruebas de carga y autonomía de los sistemas de respaldo de energía (UPS).

A.11.2.5	Retiro de Activos	Control: Los equipos de información o software no se deben retirar de un sitio sin autorización previa.	**APLICA** **SI** / **NO** Los equipos para procesamiento de información u otras actividades inherentes de la empresa deber ser verificados por la seguridad de la empresa constatando la autorización de salida de los mismos. **IMPLEMENTADO** **SI** / **NO** Se debe implementar un mecanismo autorización que lleve la firma del jefe inmediato y el motivo por el cual el equipo será retirado de las instalaciones.

Observación: No se tienen implementados formatos que validen el préstamo de algún equipo tecnológico, en el cual se responsabilice del bien que tiene asignado el usuario.

A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	**APLICA** **SI** / **NO** Todos los activos de la empresa deben contar con pólizas que cubran amenazas como robo, fallas de suministro eléctrico, líquidos. **IMPLEMENTADO** **SI** / **NO** Todos los equipos que deban procesar información deben estar autorizados por el líder o coordinador de área o superior a cargo, se debe tener presente las medidas de precaución al momento de retirar un equipos de las instalaciones.

Observación: Los equipos de procesamiento de información reposan en las instalaciones y al interior del área de TI, los equipos que se requieren para procesamiento de datos fuera de las instalaciones deben ser autorizados por el líder de área de TI.

A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobre escrito en forma segura antes de si disposición o reusó.	**APLICA**	
			SI	**NO**
			Se realiza la verificación de todos los equipos que son entregados por funcionarios o contratistas que se retiran de la organización a fin de soportar y reutilizar los equipos entregados.	
			IMPLEMENTADO	
			SI	**NO**
			Se ejecuta el protocolo de limpieza del equipo entregado, se valida la capacidad del mismo, que no contenga errores de volumen, una vez se ha completado el proceso se procede a restaurar el equipo y se dispone del mismo para su nueva asignación.	

Observación: Se realiza proceso de limpieza de equipo tanto de hardware como de software, en el cual se revisa que el equipo entregado este libre de virus u malware. Se entrega una relación de capacidad de almacenamiento, memoria, pantalla y demás accesorios.

A.11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	**APLICA**	
			SI	**NO**
			Los equipos que no están supervisados de forma continua deben ser protegidos por el ente de seguridad de signado, o en su defecto por mecanismos que vigilen la permanencia del mismo en el lugar asignado.	
			IMPLEMENTADO	
			SI	**NO**
			Los equipos de control de acceso están vigilados por el equipo de seguridad contratada por la organización, adicionalmente se tienen sistemas de vigilancia automáticos.	

Observación: Los equipos de acceso a las instalaciones como Sensor biométrico y cámaras de vigilancia son soportadas por la empresa que presta los servicios de vigilancia dentro del perímetro de la empresa.

A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	**APLICA** **SI** / **NO** Se debe implementar una política de escritorio limpio de cualquier tipo de documento o medios extraíble con información sensible de la organización, todo con el fin de reducir incidentes de seguridad ya sea durante o fuera del horario laboral establecido. **IMPLEMENTADO** **SI** / **NO** Toda la información sensible debe estar almacenada en zonas seguras que garanticen la protección ante cualquier circunstancia que se pueda presentar, fuertes impactos, robo o inundación, todas las zonas de impresión o de envió de fax deben ser protegidos contra accesos no autorizados.

Observación: Toda la información que se genera de procesamiento de datos, copias de seguridad y demás información es almacenada al interior de la oficina de TI, no se cuenta con medios óptimos para mantener durante periodos de tiempo prolongados la información generada.

A.12	**SEGURIDAD EN LAS OPERACIONES**		
A.12.1	**Procedimientos Operacionales y Responsabilidades**		
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información			
A.12.1.1	Procedimientos de Operación Documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan	**APLICA** **SI** / **NO** Los manuales de procedimientos son documentos que describen actividades que se realizan por parte de una o más funciones al interior de la organización. **IMPLEMENTADO** **SI** / **NO** La tarea de preparar manuales de carácter administrativos requieren de precisión ya que estos manuales dan una referencia de como los datos están presentados en el sistema, los manuales deben contener información concreta, clara a fin de quien los consulta no cometa errores.

Observación: Los manuales que se implementan son básicos y orientan al usuario en tareas específicas, que deben realizar en base a las funciones que tiene designadas el usuario, los manuales no brindan una noción acerca de cómo resolver algún tipo de eventualidad que se presente, en base a algún error se acude al área de soporte de TI de la empresa.

A.12.1.2	Gestión de Cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de información que afectan la seguridad de la información.	**APLICA** **SI** / **NO** Todos los cambios que se efectúen tanto a nivel de procesos como de infraestructura deben ser informados a los líderes de procesos de las áreas para evitar incidentes de seguridad por el desconocimiento de los cambios efectuados. **IMPLEMENTADO** **SI** / **NO** Los cambios que se generan al interior de la organización deben ser evaluados por la alta dirección y los líderes de proceso, para implementar mecanismos y evaluar los mismos

Observación: Al realizar justas directivas en las cuales se plantean cambios de alto impacto en procesos que afectan el desarrollo normal de las aplicaciones y sus operaciones no se tienen en cuenta muchos de los factores operacionales con los cuales la empresa trabaja actualmente, lo que genera reproceso, tiempos y costos de implementación más altos de los esperados.

A.12.1.3	Gestión de Capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura para asegurar el desempeño requerido del sistema	**APLICA** **SI** / **NO** La aplicación de seguimiento se establece ya que se pueden presentar peticiones de actualizaciones o mejoras dentro del sistema. **IMPLEMENTADO** **SI** / **NO** Se deben establecer los alcances de los requisitos de actualización o modificaciones ya que estos pueden afectar el correcto funcionamiento del sistema.

Observación: Toda solicitud es analizada por el equipo de desarrollo y el líder del área de TI a fin de determinar cuál es el alcance del requisito solicitado por alguna de las áreas de la empresa.

A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	**APLICA**	
			SI	**NO**
			Los ambientes de desarrollo, pruebas y operación deberán estar en el mejor de los casos separados de forma física, y se definirán mecanismos de transferencia de información debidamente documentados.	
			IMPLEMENTADO	
			SI	**NO**
			Se debe ejecutar el software de ambientes de desarrollo y de operación en diferentes directorios para no ocasionar conflictos, no se debe permitir el uso de compiladores en las áreas de operación a menos que estos estén disponibles y autorizados para su ejecución.	

Observación: Realizar pruebas del software que se implementa debido a cambios solicitados y previamente autorizados se realiza en ambientes de pruebas controlados, se utilizan espejos de información para realizar pruebas de capturas, y procesamiento de datos, el equipo de desarrollo evalúa los resultados de las pruebas realizadas y son puestas en conocimiento del líder del área de TI.

A.12.2	**Protección contra códigos Maliciosos**			
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra código malicioso				
A.12.2.1	Controles contra Códigos Maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	**APLICA**	
			SI	**NO**
			Se debe proteger la integridad del software, se deben tomar las medidas pertinentes contra ataques de virus, bombas lógicas y cualquier otro tipo de virus que pueda afectar la operación del software, los usuarios deben ser conscientes del peligro de ingresar código malicioso por medio de dispositivos que no estén autorizados.	
			IMPLEMENTADO	
			SI	**NO**
			Se deben definir los controles para detección y prevención contra software malicioso. Se debe prohibir la instalación y uso de software no autorizado, se deben tener lineamientos acerca del uso y permisos de puertos de conexión sobre todo tipo de dispositivos.	

Observación: se encuentran establecidos mecanismos de control para virus o cualquier software malicioso, se tienen implementados mecanismos para prevenir instalaciones no autorizadas por parte de los usuarios, cualquier tipo de instalación que desee realizarse solicita usuario y contraseña de administrador, la cual es conocida solo por el equipo de soporte.

A.12.3	Copias de Respaldo		
Objetivo:	Proteger contra la perdida de datos		
A.12.3.1	Respaldo de la Información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	APLICA SI / NO Se deben implementar rutinas para la generación de respaldo de la información y verificar mediante la restauración de los mismos la veracidad de los datos. IMPLEMENTADO SI / NO Se deben definir las rutinas para generar copias de respaldo, se deben generar las copias teniendo en cuenta desde la identificación clara que permita identificar qué tipo de información esta almacenada, el lugar de almacenamiento y de ser necesario el cambio de los medios en los cuales se almacena información

Observación: se tiene implementado un mecanismo software que realiza copia de seguridad de archivos, y bases de datos y son almacenadas en DVD rotulados con la fecha de creación y el tipo de información que contiene, lo que permite una fácil identificación en caso de requerir restaurar algún documento o dato especifico de la base de datos transaccional de la empresa.

A.12.4	Registro y Seguimiento		
Objetivo:	Registrar eventos y generar evidencia		
A.12.4.1	Registro de Eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	APLICA SI / NO Se deben tener registros de auditoria con los cuales se logre registrar las actividades y eventos de seguridad de la información de todos los usuarios, los registros encontrados servirán como evidencia para posibles investigaciones. IMPLEMENTADO SI / NO Se deben tener soportes de los registros de fechas de ingreso al sistema, identidad del equipo, que archivos accede, las veces que el usuario logra acceder o no al sistema.

Observación: Las aplicaciones que se ejecutan diariamente tienen activo registros Log que permiten identificar acceso y mensajes de error ocurridos durante alguna interrupción o mal funcionamiento del software.

A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	**APLICA**	
			SI	**NO**
			Se deben tener controles de protección para los registros de eventos A12.4.1, así como contra cambios no autorizados u otro tipo de operaciones.	
			IMPLEMENTADO	
			SI	**NO**
			Los mecanismos utilizados para salvaguardar los registros se deben revisar y validar que no sufran ningún tipo de alteración u acceso no autorizado	

Observación: Solo el personal autorizado puede ingresar al área donde se resguardan los registros o copias de seguridad generados en la empresa por parte del área de TI.

A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad	**APLICA**	
			SI	**NO**
			Se deben mantener bajo supervisión y revisión las actividades y operaciones que realiza el administrador y los operadores del sistema.	
			IMPLEMENTADO	
			SI	**NO**
			Realizar la revisión de las cuentas de administrador que estén involucradas en la operación del sistema, llevar registro de todas las actividades eventos, manipulación de archivos fallas reportadas en la sesión.	

Observación: Se realiza copia del log de los servidores a fin de tener el registro de todos los cambios realizados por el encargado de los servidores de datos ya sean contables u de operación administrativa.

A.12.4.4	Sincronización de los relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	**APLICA** **SI** / **NO** Se debe mantener una correcta configuración de zonas horarias, la configuración horaria debe ser suministrada por políticas. **IMPLEMENTADO** **SI** / **NO** Se debe tener un procedimiento de ajuste de tiempo, se debe validar contra una fuente externa, debe verificar cualquier cambio por variación significativo.

Observación: No se aplica control de zona horaria, esta es definida al momento de la instalación de los equipos.

A.12.5	**Control de Software Operacional**		
Objetivo:	**Asegurarse de la integridad de los sistemas operacionales**		
A.12.5.1	Instalación de software en sistemas Operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	**APLICA** **SI** / **NO** Realizar la aplicación de controles durante la puesta en marcha de software de producción, de esta forma se minimiza el impacto que se pueda causar en los sistemas **IMPLEMENTADO** **SI** / **NO** Todas las aplicaciones desarrolladas al interior de la organización deberán tener un responsable, los desarrolladores no deben tener acceso a los ambientes de producción, todos los cambios u actualizaciones deben estar aprobados por el líder de desarrollo y llevando un registro de los cambios realizados.

Observación: El desarrollador tiene acceso al ambiente de producción, no se le limita el acceso ya que el provee asistencia técnica ante cualquier eventualidad del sistema o si el equipo de soporte no tiene la capacidad de resolver.

A.12.6	Gestión de la vulnerabilidad Técnica		
Objetivo:	**Asegurarse de la integridad de los sistemas operacionales**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	**APLICA** **SI** / **NO** Se tendrá la información oportuna de vulnerabilidades técnicas en los sistemas de información de forma oportuna y se tomaran las medidas para tratar los riesgos que surjan de los análisis de las vulnerabilidades posibles. **IMPLEMENTADO** **SI** / **NO** Identificar las vulnerabilidades técnicas potenciales que se puedan presentar, en el caso de no existir planes contra ciertas vulnerabilidades se deben tener presentes controles alternativos para realizar el seguimiento y gestión de los mismos.

Observación: Se tienen definidos planes de contingencia que apoyen a mitigar cualquier riesgo que se pueda presentar.

A.12.6.2	Restricciones sobre la instalación de software	Control: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	**APLICA** **SI** / **NO** Se deben establecer reglas acerca de la instalación de software por parte de personal no autorizado. **IMPLEMENTADO** **SI** / **NO** Los usuarios que realizan instalaciones sin autorización, generan vulnerabilidades y fugas de información, y otro tipo de incidentes de seguridad.

Observación: A los usuarios que realizan instalaciones sin autorización, se les genera un incidente de seguridad el cual se anexa a la hoja de vida con un llamado de atención, este tipo de incidentes se presentan cuando los usuarios logran captar las credenciales del administrador, cuando realiza labore de mantenimiento del equipo.

A.13	SEGURIDAD EN LAS COMUNICACIONES		
A.13.1	Gestión de la seguridad de las redes		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte			
A13.1.1	Controles de Redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	APLICA SI / NO El área de TI debe gestionar los controles necesarios para resguardar los datos y servicios al interior de la organización. IMPLEMENTADO SI / NO Se establecen los procedimientos para garantizar que la información que viaja por la red cumpla los principios de confidencialidad e integridad, se debe garantizar la disponibilidad del servicio de red, los procedimientos deben aplicarse tanto a la red interna como externas si se comparte algún tipo de información.

Observación: Se implementan mecanismos de protección sobre la red, los canales de transmisión contratados cuentan con servicio de protección de datos.

A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraen externamente.	APLICA SI / NO El líder de proceso en conjunto con el líder de área debe definir los lineamientos para que se garantice la seguridad de la información ya sea al interior de la organización como fuera de ella. IMPLEMENTADO SI / NO Se deben realizar las actualizaciones de seguridad requeridas, instalar y habilitar los servicios que realmente se requieren, verificar que no existan puertos innecesarios abiertos, se deben realizar validaciones de las configuraciones realizadas a fin de encontrar posibles fallas.

Observación: La actualización e instalación de parches de seguridad tanto de sistemas operativos como del resto de las aplicaciones instaladas en la empresa deben ser programadas para no afectar la operación del sistema, se lleva control en hoja de cálculo de las tareas de actualización realizadas, se registra la fecha de ejecución de las mismas, se valida la actualización de navegadores y complementos requeridos.

A.13.1.3	Separación de las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	**APLICA** **SI** / **NO** Los servicios que transitan en la red deben ser separados a fin de optimizar la utilización de los recursos, como ejemplo esta que los servicios de datos para desarrollo y operación de las actividades internas sea diferente al canal que se utiliza para navegar por la Web. **IMPLEMENTADO** **SI** / **NO** La administración de los servicios ya sean datos o internet debe separarse bajo los lineamientos establecidos en las políticas de seguridad para salvaguardar la integridad y confiabilidad de la información.

Observación: La administración de los canales de comunicación es tarea que realiza el proveedor del servicio, si se requiere alguna modificación se agenda la tarea con el centro de soporte y se analiza el impacto que tendrá el cambio al interior de la red.

A.13.2	**Transferencia de Información**		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa			
A.13.2.1	Políticas y procedimientos de transferencia de información.	Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	**APLICA** **SI** / **NO** Se establecen procedimientos, para proteger la transferencia de información en las instalaciones. **IMPLEMENTADO** **SI** / **NO** Los controles y políticas establecidas se implementan considerando que se deben detectar códigos maliciosos, uso adecuado de medios inalámbricos, eliminación de correspondencia mal intencionada, y cualquier tipo de copia o reenvió de mensaje no autorizado

Observación: No se han establecido políticas para actuar ante amenazas de tipo malware o cualquier otro tipo de virus, por medio del firewall y el antivirus se controla el acceso de ataques potenciales que pueden perpetrarse vía correos electrónicos o dispositivos de almacenamiento no autorizados.

A.13.2.2	Acuerdos sobre transferencia de información.	Control: Los acuerdos deben tratar de transferencia segura de información del negocio entra la organización y las partes externas.	**APLICA**	
			SI	**NO**
			La elaboración de acuerdos entre organizaciones para realizar el intercambio de información debe relacionar el grado de sensibilidad de la información que será transmitida.	
			IMPLEMENTADO	
			SI	**NO**
			Se establecen procedimientos de emisión - transmisión y envió - recepción, se deben tener presentes normas técnicas para empaquetado, definir controles especiales para la información sensible.	

Observación: Se tienen procedimientos de envío y recepción de información empaquetada desde y hacia otras entidades las cuales son aliados estratégicos en la operación de las actividades de la empresa, se utilizan mecanismos como sockets para transferir información entre diversos puntos de atención y consultar información en línea.

A.13.2.3	Mensajería Electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica	**APLICA**	
			SI	**NO**
			La implementación de mensajería electrónica ya sea que se hable de correo u cualquier otro medio de intercambio de información deben considerarse los mecanismos para salvaguardar la información.	
			IMPLEMENTADO	
			SI	**NO**
			Se establecen medidas de seguridad para la mensajería electrónica, protección por accesos no autorizados, disponibilidad del servicio, requerimiento de firmas electrónicas, y todos los mecanismos que se puedan implementar ya que la mensajería electrónica y sus vulnerabilidades son diferentes a la mensajería que se plasma en papel.	

Observación: Todos los correos electrónicos salientes y entrantes son filtrados por el firewall que se encuentra instalado en la empresa, adicionalmente el antivirus posee herramientas de filtrado para posibles correos tipo spam, lo cual minimiza el riesgo de ataque por vía de correos electrónicos.

A.14	**Adquisición, desarrollo y mantenimiento de Sistemas**		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	**APLICA** **SI** / **NO** Los nuevos requerimientos de sistemas de información requieren controles específicos, los administradores de sistemas deben tener en cuenta controles automáticos así como el respaldo en apoyos de controles manuales **IMPLEMENTADO** **SI** / **NO** Se deben definir dentro de la etapa de análisis los controles de seguridad correspondientes a nuevos requerimientos, se debe tener presente una etapa de evaluación donde se validen los controles establecidos

Observación: Se implementan controles dentro de la etapa de análisis y desarrollo de software, se evalúan si las medidas que se implementan son eficaces ante eventualidades que se puedan presentar.

A.14.1.2	Seguridad de servicios de las aplicaciones	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas	**APLICA** **SI** / **NO** Se debe contar con mecanismos de protección para los medios por los cuales se transfiere información ya sean documentos, dispositivos móviles, correos, o mensajes de voz, cualquier tipo de medio multimedia, fax etc. **IMPLEMENTADO** **SI** / **NO** Se debe validar las posibles vulnerabilidades de información al interior de la organización, en llamadas telefónicas, video llamadas, distribución de mensajería. Restricción de acceso a información sensible por personas no autorizadas, Realizar la identificación correspondiente por categorías de usuarios ya sean empleados director, terceros contratistas

Observación: No se tienen implementadas restricciones de uso de equipos electrónicos como celulares tabletas, etc.

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	**APLICA** **SI** / **NO** Se deben tomar medidas para proteger la integridad de la información que se publica de forma electrónica, a fin de evitar la modificación por personal o entes no autorizados, se debe implementar mecanismos formales de autorización para la información que se expone al público estas autorizaciones deben estar avaladas por los jefes de área **IMPLEMENTADO** **SI** / **NO** Se debe tener presente para toda la información que se comparte: Toda la información que se comparte al público se debe procesar de forma completa, y oportuna. Se debe vigilar que las redes en las cuales se publica no interactúen con las redes a las cuales se conectan. Se deben tener presentes las normas legales y establecidas al respecto. se debe garantizar la vigencia y validez de la información que se publica

Observación: La información se viaja por medios electrónicos deben contemplar las normativas de ley que aplican a este tipo de servicios de transferencia de información, se definen fechas de publicación de la información a fin que la misma se encuentre actualizada para su consulta.

A.14.2	**Seguridad en los Procesos de desarrollo y de Soporte**		
Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.			
A.14.2.1	Política de Desarrollo seguro	Control: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	**APLICA** **SI** / **NO** Se deben definir lineamientos durante la etapa de diseño del software, se deben aplicar controles que garanticen la integridad de los datos ingresados, todo debe estar controlado de forma permanente. **IMPLEMENTADO** **SI** / **NO** Se debe llevar un control estricto de las aplicaciones, códigos fuentes que estén siendo utilizados, se deben administrar las versiones del software, se debe garantizar la integridad del software desarrollado garantizando que los programas en ambientes de desarrollo pertenezcan a un mismo código fuente.

Observación: Se definen controles de versión por parte del grupo de desarrollo todas las veces que se genera una nueva compilación de cualquiera de los aplicativos, estos se categorizan y marcan con el nombre del aplicativo y fecha de compilación lo que permite al grupo de desarrollo acceder a compilaciones anteriores con mayor facilidad.

A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios	**APLICA**	
			SI	**NO**
			Para minimizar los riesgos en los sistemas de información se establecen controles durante la implementación de cambios haciendo cumplir los lineamientos establecidos.	
			IMPLEMENTADO	
			SI	**NO**
			Se deben validar que los cambios se han presentados con antelación y los mismos estén avalados para su aplicación, se debe llevar un registro de los niveles de autorización estipulados, se deben efectuar los cambios en ambientes de desarrollo, se debe notificar a las áreas de los cambios a los cuales se someterá el sistema de información.	

Observación: Siempre que se realizan cambios en las aplicaciones al interior de la empresa, se les notifica a las áreas que intervengan de las nuevas funcionalidades que se incorporan en el aplicativo, los cambios sobre las aplicaciones se realizan de forma controlada y en horarios que no afecte la operación de la empresa.

A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	**APLICA**	
			SI	**NO**
			Se debe validar la interoperabilidad e las aplicaciones frente a cambios de plataformas que puedan afectar la continuidad de las operaciones al interior de la organización, se deben realizar pruebas en ambientes de desarrollo controlando las posibles vulnerabilidades que se puedan presentar	
			IMPLEMENTADO	
			SI	**NO**
			Se debe implementar mecanismos de validación que constaten la información que genera el sistema, se debe vigilar la integridad de los datos, se establecen procedimientos que aseguren el correcto funcionamiento de las aplicaciones, detección de fallas y seguimiento de las mismas hasta solucionarlo	

Observación: La integridad de y veracidad de los datos es tarea fundamental del DBA designado al interior del área de TI, este se encarga de validar que la información que es procesada por las aplicaciones es información que no es manipulada de forma diferente ni alterada, incluyendo mecanismos de control de cambios a bases de datos, los cuales permiten validar que la información contenida en las DB es veraz.

A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	**APLICA**	
			SI	**NO**
			las modificaciones que se plantean sin una base bien fundamentada se deben descartar ya que simplemente generan procesos de desarrollo que no conllevan a cambios que mejoren el rendimiento de las operaciones de la empresa	
			IMPLEMENTADO	
			SI	**NO**
			La presentación de cambios en las aplicaciones debe estar fundamentada en base a los objetivos de la organización aplicando las técnicas y metodologías para tal fin, se deben controlar que los cambios que se requieran no generen traumatismos en materia de desarrollo y gastos operacionales innecesarios.	

Observación: Algunos de los cambios que se realizan obedecen a cambios generados por otros factores, estos afectan la operación normal de la empresa, los mismos son evaluados y puestos en ambientes de producción a fin de corregir las fallas detectadas.

A.14.2.5	Principios de construcción de los sistemas seguros	Control: Se deben establecer documentar, y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas de información.	**APLICA**	
			SI	**NO**
			Se debe realizar la documentación durante todo el ciclo de vida del desarrollo de aplicaciones, se deben establecer procedimientos para validad que los nuevos sistemas diseñados cumplan con los requisitos de implementación.	
			IMPLEMENTADO	
			SI	**NO**
			Se debe establecer un funcionario que realice el proceso de documentación de las actividades desarrolladas en el desarrollo de software a fin de mantener control del desarrollo del mismo y los posibles cambios a los que se pueda incurrir. Se debe rechazar la implementación del aplicativo software si no existe documentación alguna.	

Observación: No se realiza la documentación dentro del ciclo de vida de software que se diseña en la empresa, no se cuenta con los mecanismos ni recursos humanos suficientes para la realización de actividades de documentación, en algunas ocasiones documentar un procedimiento debe realizarla el mismo grupo de desarrollo.

A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	**APLICA** **SI** / **NO** El líder del área de tecnología debe establecer el perímetro de áreas de desarrollo, en el cual se aseguren los mecanismos e infraestructura para desarrollar las actividades de desarrollo en concordancia de las normas y procedimientos vigentes. **IMPLEMENTADO** **SI** / **NO** Se deben resguardar solo los ejecutables que están aprobados en el ambiente de producción, se debe implementar un registro de las actualizaciones que se realizan al sistema, se deben mantener protegidas las versiones anteriores de las aplicaciones a fin de tener un plan de contingencia.

Observación: Tanto ejecutables como código fuente generados y aprobados para puesta en marcha en ambientes de producción son resguardados en medios ópticos rotulados cada uno con fecha de creación y tipo de archivo, de igual forma se almacenan todas las versiones que se generan en el grupo de desarrollo.

A.14.2.7	Desarrollo controlado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	**APLICA** **SI** / **NO** Todas las aplicaciones que se desarrollan fuera de los ambientes de desarrollo controlado deben tener un estricto seguimiento, pruebas y validación de salida de datos, al igual que su respectiva documentación. **IMPLEMENTADO** **SI** / **NO** todos los desarrollo que son tercer izadas deben estar supervisados por el líder de desarrollo validando que cumplan con los lineamientos establecidos dentro del ciclo de vida del software, aplicando pruebas respectivas e implementando auditorías a los sistemas que están siendo desarrollados por terceros, se debe informar al líder del área de TI sobre los avances y vulnerabilidades a que tengan lugar las aplicaciones desarrolladas

Observación: Las aplicaciones que son diseñadas y adquiridas por la empresa deben cumplir con las especificaciones técnicas y requerimientos específicos que son propios de la operación interna de la empresa. Se realizan pruebas en ambientes controlados de software en los cuales se aplican parámetros específicos de la empresa para determinar si la aplicación cumple con los requisitos aplicables a la organización.

A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad	**APLICA** **SI** / **NO** Todas las aplicaciones software ya sean desarrolladas al interior de la organización o desarrolladas por externos deben cumplir con los estándares de desarrollo establecidos por el área de TI, se deben validar las posibles vulnerabilidades a que tengan lugar al momento de realizar las pruebas de funcionalidad. **IMPLEMENTADO** **SI** / **NO** Se deben ejecutar las pruebas a las aplicaciones software validando que estas cumplan con los lineamientos de seguridad establecidos al interior de la organización. Se debe implementar el plan de pruebas establecido por el área de TI y analizar los resultados de las mismas entregando un informe al responsable del área

Observación: Las aplicaciones que son desarrolladas por el equipo de TI de la empresa, se ciñen a los lineamientos establecidos por la empresa. Se implementan planes de pruebas con usuarios de las áreas donde se realizan modificaciones o nuevas aplicaciones para el desarrollo de las operaciones interna de la empresa.

A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados	**APLICA** **SI** / **NO** Se deben implementar planes de pruebas a todos los sistemas, los planes de pruebas están acordes a los lineamientos y planes de pruebas estándar, junto con la documentación de los procesos respectivamente **IMPLEMENTADO** **SI** / **NO** La persona testeador realiza todas las pruebas bajo una base de datos de pruebas, el testeador ejecuta las rutinas de seguridad que están definidas al interior del área de TI y si no se evidencias falla alguna estas aplicaciones son remitidas al coordinador de desarrollos para realizar el control de versión y documentación respectivo, de no cumplirse se devuelve nuevamente al programador para que este junto con el documento de las falencias encontradas sea evaluado nuevamente.

Observación: No se realizan pruebas bajo ambientes controlados, las pruebas realizadas están definidas utilizando copias de seguridad que reposan en las instalaciones de la empresa.

A.14.3	Datos de Prueba		
Objetivo:	Asegurar la protección de los datos usados para pruebas		
A.14.3.1	Protección de datos de pruebas	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente	APLICA SI / NO Los datos seleccionados están avalados para cumplir con las exigencias de las pruebas de aplicaciones ya sean desarrolladas por el equipo de desarrollo de la organización o por los desarrollados por terceros. IMPLEMENTADO SI / NO Los datos proporcionados para la realización de las pruebas deben ser cuidadosamente seleccionados, los procedimientos a aplicarse deben ser los mismos a fin de que peritan determinar los alcances u modificaciones a que se puedan dar lugar ya sea en el diseño de la base de datos o modificación del código fuente, las pruebas realizadas deben estar debidamente documentadas y deben cumplir con los lineamientos de seguridad ya establecidos.

Observación: Los datos que son utilizados para la realización de las pruebas son tomados de copias de seguridad de fechas anteriores, a fin de que se pueda asegurar que las pruebas realizadas cumplan los requisitos y lineamientos de seguridad establecidos.

A.15	Relaciones con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		
Objetivo:	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores		
A.15.1.1	Política de seguridad de la información para relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar	APLICA SI / NO Se debe garantizar la protección a la información a la cual tienen acceso los proveedores, cumpliendo a cabalidad los lineamientos de seguridad establecidos IMPLEMENTADO SI / NO Se debe tener presente en todo momento los contratos y acuerdos pactados con el proveedor, se deben establecer controles para contemplar de forma específica el acceso a los proveedores, se deben establecer procesos estandarizados para las relaciones con los proveedores, se deben definir cuáles serán los tipos de acceso y cuáles serán los controles que se realizarán a los proveedores. Se deben establecer obligaciones por parte del proveedor para garantizar la protección de la información, todas las políticas lineamientos y acuerdos que se establezcan con el proveedor deben estar debidamente documentados y firmados por las partes.

Observación: Se deben analizar todos los contratos que sean pactados con proveedores, se deben validar que cumplan con los requisitos de ley, los documentos deben ser revisados en conjunto del abogado y el líder del área de TI a fin de garantizar que se establezcan las obligaciones por parte del proveedor y del contratante.

A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	**APLICA** **SI** / **NO** Todos los acuerdos realizados con los proveedores deben estar debidamente documentados, se deben definir dentro de los acuerdos todas las responsabilidades para las partes y mecanismos de seguridad pertinentes. **IMPLEMENTADO** **SI** / **NO** Se deben definir dentro de los acuerdos: la información a la cual tendrán acceso, los requisitos legales a que tenga lugar, se establecen de igual forma los niveles de servicio que serán aceptados, lineamientos en materia de capacitación a los empleados, realizar la auditoria de los procesos que se implementen con los proveedores, solicitudes de cambios y solución de errores.

Observación: Se definen las funciones y responsabilidades a que tienen lugar, los empleados de la empresa se definen los niveles de servicio que se deben prestar a los mismos y como deben proceder cuando identifiquen alguna anomalía del sistema.

A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Loa acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información comunicación	**APLICA** **SI** / **NO** Se realiza la definición de requisitos para la adquisición de tecnologías, productos u cualquier otro servicio de información relacionados a la cadena de suministros de tecnología de información y las comunicaciones. **IMPLEMENTADO** **SI** / **NO** Se deben implementar procesos que apoyen la identificación de componentes tecnológicos que son de importancia al interior de la organización, se deben tener presentes las garantías de los productos en caso alguno uno de estos componentes tecnológicos no opere según lo esperado.

Observación: Las reuniones que se realizan dentro del área de TI, sirven para identificar qué tipos de componentes tecnológicos ya sean Routers, Switch, servidores etc., son requeridos como tal para el desarrollo de las funciones y mantener la operación normal de los procesos de la empresa.

A.15.2	Gestión de la Prestación de servicios de Proveedores		
Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	APLICA SI / NO Se debe realizar un seguimiento a todos los servicios prestados por terceros, verificando que estos se encuentran en línea con las políticas de seguridad de la información. IMPLEMENTADO SI / NO Se deben tener presentes: Los desarrollos que estén implementados por terceros, el soporte respectivo y las actualizaciones a las que tenga lugar sin alterar las operaciones al interior de la organización

Observación: Todas las aplicaciones que sean implementadas por terceros cuentan con el soporte respectivo a fin de que si se presentan problemas el grupo de soporte puede realizar la consulta y si se encuentra dentro de una incidencia que se puede resolver con la consulta esta se realizaría y se dejara constancia del ajuste realizado.

A.15.2.2	Gestión de cambios en los servicios de los proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	APLICA SI / NO Cuando se realizan cambios por parte de los proveedores se debe tener en cuenta que los cambio que se realizan deben ser en beneficio y que aporten funcionalidades dentro de los sistemas ya implementados, se establecen nuevos controles que resuelvan incidentes de seguridad de la información y de esta manera mejorar la seguridad. IMPLEMENTADO SI / NO Se adoptan las nuevas versiones que presentan los proveedores que no afecten y mejoren el desarrollo de las actividades u operaciones al interior de la organización, la implementación de nuevas tecnologías y ambientes de desarrollo, los productos o servicios que el proveedor realice oferta teniendo presente normativas técnicas y legales dentro de los acuerdos ya establecidos

Observación: Las nuevas versiones de software que lanzan los proveedores que ya tienen algún tipo de contratación con la empresa deben garantizar que estas nuevas versiones o actualizaciones de software no generaran cambios que afecten de manera considerable las operaciones de la empresa.

A.16	**Gestión de Incidentes de Seguridad de la Información**		
A.16.1	**Gestión de Incidentes y Mejoras en la Seguridad de la Información**		
Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades.			
A.16.1.1	Responsabilidades y Procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información	**APLICA** **SI** / **NO** Se realiza un análisis de la incidencia presentada para definir el grado de criticidad de la misma y la forma de atención dependiendo del tipo de incidencia. **IMPLEMENTADO** **SI** / **NO** Está definido personal de soporte capacitado para atender los requerimientos que se generan por parte de los usuarios al interior de la organización.

Observación: Al personal que se contrata para temas de soporte a usuarios y otras actividades que designe el líder de área le realiza una evaluación técnica de conocimientos propios de las tareas a realizar, se le realizan adicionalmente pruebas actitudinales a fin de analizar si el perfil que arrojan estas pruebas cumple con el solicitado para el puesto.

A.16.1.2	Reporte de Eventos de Seguridad de la Información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	**APLICA** **SI** / **NO** No se cuentan con los canales de gestión de incidentes de seguridad, se realizan por medio de correo electrónico lo que no respalda de manera formal la presentación de incidentes en seguridad de la información. **IMPLEMENTADO** **SI** / **NO** Se deben aplicar mecanismos que informen de los incidentes de seguridad que se presentan al interior de la organización, existen mecanismos u herramientas que permiten la gestión de incidentes que puedan presentarse.

Observación: No se cuentan con mecanismos por los cuales los diversos usuarios puedan notificar acerca de incidentes relacionados con las aplicaciones que ellos ejecutan en sus labores diarias como por ejemplo que no está realizando el cálculo de cuotas a pagar dentro de una aplicación de ventas.

A.16.1.3	Reporte de Debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios de sistemas de información de la organización que observen y reporten cualquier debilidad de seguridad de la información	**APLICA** **SI** / **NO** Los empleados con capacitados en el uso de las herramientas desarrolladas o contratadas por terceros, estos al momento de detectar debilidades informan al coordinador de área quien a su vez en los comités de áreas expresa este tipo de debilidad para ser tratada por el área **IMPLEMENTADO** **SI** / **NO** Una vez se detecta una debilidad el usuario realiza un informe de la debilidad evidenciada y es reportada a el líder del área vía correo electrónico, no se le permite al usuario que retire el software que presente anomalías sin previa autorización. Se debe tener presente los mensajes de error que aparecen en pantalla

Observación: El usuario identifica una debilidad este genera un informe de anomalía el cual es entregado al líder de área del usuario, este a su vez remite la información al líder de área y al equipo de soporte de la empresa a fin de que se tomen las medidas de protección y corrección necesarias.

A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	**APLICA** **SI** / **NO** Se realiza la evaluación del evento de seguridad de la información, se deben establecer procedimientos para mitigar o evitar que estos ocurran nuevamente, se debe informar a las áreas del incidente y como se recuperan del mismo. **IMPLEMENTADO** **SI** / **NO** Se realiza la definición de las medidas a implementar, se implementan soluciones para evitar que ocurra nuevamente, se les informa a las áreas la solución implementada.

Observación: Las incidencias reportadas por los usuarios son atendidas por el equipo de soporte del área de TI.

A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	**APLICA** **SI** | **NO** Se notifican a las áreas de los incidentes evidenciados, se notifica la corrección al incidente presentado. **IMPLEMENTADO** **SI** | **NO** No se tiene implementados procedimientos documentados que soporten las respuestas a incidentes presentados, la notificación de las incidencias dependiendo del grado de criticidad es notificada a las áreas.

Observación: Las incidencias que son atendidas por el equipo de soporte del área de TI, no son documentadas lo que no permite crear base de conocimiento para atender futuras incidencias que se puedan presentar.

A.16.1.6	Aprendizaje Obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se deben usar para reducir la posibilidad o el impacto de incidentes futuros.	**APLICA** **SI** | **NO** Se define un proceso que permita realizar la documentación y seguimiento de las incidencias que se presentan, este tipo de seguimientos garantizan que se puedan mejorar los controles y reducir los costos de implementación a futuro. **IMPLEMENTADO** **SI** | **NO** La solución a incidencias se realiza por la experiencia que se tiene de experiencias ya vivenciadas, en el caso de no conocer la solución de forma inmediata se realiza el análisis al interior del área de tecnología para encontrar una solución viable y efectiva contra la incidencia presentada

Observación: Todas las incidencias que son resueltas por el equipo de soporte son soluciones basadas en su conocimiento, cuando no pueden realizar una corrección inmediata a la incidencia se apoyan en algún otro integrante del área que tenga el conocimiento de cómo resolver este tipo de incidencias.

A.16.1.7	Recolección de Evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia	**APLICA**	
			SI	**NO**
			La organización debe definir de manera efectiva los procedimientos que permitan manejar las debilidades e incidentes presentados en la organización, se debe realizar la aplicación de procesos de recolección de información oportuna y sin distorsión alguna que garanticen que la incidencia presentada no ha sido manipulada	
			IMPLEMENTADO	
			SI	**NO**
			Se mantienen los registros de auditoria que se ejecuta sobre las transacciones al interior de la organización, estos sirven de evidencia para llevar procesos disciplinarios a que tuviese lugar.	

Observación: Todas las operaciones transaccionales realizadas por los usuarios en las aplicaciones son auditadas esto permite brindar un mejor soporte dado que se presente alguna incidencia.

A.17	**Aspectos de Seguridad de La Información de la Gestión de Continuidad de Negocio**			
A.17.1	**Continuidad de seguridad de la información**			
Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio dela organización.				
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas para la seguridad de la información durante una situación adversa.	**APLICA**	
			SI	**NO**
			Se debe desarrollar e implementar planes de contingencia, deben mantenerse actualizados y deben incorporarse a los procesos administrativos y operativos al interior de la organización para lograr que ante cualquier incidencia esta pueda ser resuelta dentro de los tiempos estipulados.	
			IMPLEMENTADO	
			SI	**NO**
			Se diseñan y aplican planes de contingencia, se realiza un análisis del impacto de la incidencia, se determinan los controles preventivos ante cualquier eventualidad.	

Observación: Se implementan planes de contingencia cuando se requiere realizar labores de mantenimiento a equipos de procesamiento de datos, servidores u otros equipos, se ejecutan planes de contingencia ante eventualidades generadas con las DB transaccionales de la empresa.

A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa	**APLICA** **SI** / **NO** Se debe identificar que puede ocasionar la interrupción de los procesos al interior de la organización, estas actividades se llevan a cabo con la participación de las áreas y los responsables de los procesos sin limitarse simplemente a las áreas de procesamiento de información. **IMPLEMENTADO** **SI** / **NO** Se identifican los elementos preventivos como por ejemplo sistemas de detección de humo, gabinetes resistentes al calor y los medios de respaldo a prueba de agua. A partir de los resultados de estas actividades se crean planes estratégicos para tener en conocimiento el con que se abordara la continuidad de la organización.

Observación: Al interior del área de Ti no se cuentan con dispositivos de detección de humo, ni de control de humedad.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	**APLICA** **SI** / **NO** Se deben establecer cronogramas de pruebas para los controles ya establecidos, donde se enmarquen diversas situaciones que afectan la continuidad de las actividades de la organización. **IMPLEMENTADO** **SI** / **NO** Realización de simulaciones de desempeño de los sistemas, pruebas de servicio en conjunto con los proveedores para garantizar que los servicios prestados operan de la manera con las cuales fueron adquiridos, se debe realizar la documentación de todas las pruebas ejecutadas, ya que son base fundamental para nuevos esquemas y planificaciones de trabajos

Observación: Se realizan pruebas de servicio sobre canales de datos que están contratados por la empresa, las realizaciones de estas pruebas no están sujetos a fechas preestablecidas, se realizan cuando se detectan anomalías de servicio.

A.18	Cumplimiento		
A.18.1	Cumplimiento de Requisitos Legales y Contractuales		
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	**APLICA** **SI** / **NO** Toda la operación y administración de los sistemas de información están avalados por normas legales y contractuales. Todas las normas implementadas deben estar documentadas. **IMPLEMENTADO** **SI** / **NO** Se debe evitar el incumplimiento de las normas legales, se debe verificar que los sistemas establecidos cumplan las políticas y procedimientos, se establecen compromisos de confidencialidad entre la organización y el empleado.

Observación: Se realiza una revisión de forma periódica de los términos de contratación de servicios, cuando se realizan las pruebas **A.17.2.3**y estas no cumplen con lo contratado se hacen valer los compromisos adquiridos con el proveedor del servicio.

A.18.1.2	Derechos de propiedad Intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	**APLICA** **SI** / **NO** Se deben implementar procedimientos que garanticen el cumplimiento de todas las restricciones legales, el no cumplimiento tiene resultados que pueden terminar en sanciones legales o demandas. **IMPLEMENTADO** **SI** / **NO** Se debe realizar la aplicación de normas de propiedad intelectual, protección de marcas, patentes y productos software que son desarrollados al interior de la organización.

Observación: Las aplicaciones que son diseñadas por integrantes del equipo de TI son de propiedad de la empresa, se deja contemplado que la propiedad moral es irrenunciable e intransferible, todas las aplicaciones generadas se registran a nombre de la empresa.

A.18.1.3	Protección de Registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de acuerdo con los requisitos legislativos de reglamentación contractuales y de negocio	**APLICA** **SI** / **NO** Todos los registros generados dentro de la organización se deben proteger contra cualquier tipo de daño físico que puedan sufrir, se debe tener en cuenta la degradación de los materiales que resguardan los registros para evitar daños a futuro ya sea por cambios de tecnología o nuevos lineamientos. **IMPLEMENTADO** **SI** / **NO** Se realiza la clasificación de los registros para determinar el nivel de protección de los mismos y el tiempo de permanencia de los mismos en los archivos de la organización, se consideran las normas legales que amparan la protección de los registros

Observación: Toda la información que se remite al archivo se clasifica y se mantiene durante un periodo de tiempo específico, se tienen presentes las normas de protección en archivo.

A.18.1.4	Privacidad y protección de información de datos personales	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	**APLICA** **SI** / **NO** Se les informa a todos los empleados que existen restricciones para el tema de divulgación de información en el ejercicio de las funciones. Se les explica cuáles son las reglamentaciones legales que existen al respecto. **IMPLEMENTADO** **SI** / **NO** Se debe diligenciar el acuerdo de confidencialidad, tanto para usuarios como para contratistas, este instrumento es utilizado para concientizar a los usuarios que la información solo debe ser utilizada, procesada al interior de la organización.

Observación: Se tramita para todos los usuarios cuando ingresan a laborar en la empresa, se definen dentro de los acuerdos cuales son las causales legales a las que se hace responsable el usuario para manejo de la información de la empresa.

A.18.1.5	Reglamentación de controles criptográficos	Control: Se deben usar controles criptográficos en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes	**APLICA** **SI** / **NO** Para la utilización de firmas digitales o cualquier otro mecanismo criptográfico se debe tener presente la ley 25.506 y sus decretos, que regulan los términos e utilización de este tipo de elementos. **IMPLEMENTADO** **SI** / **NO** La implementación de herramientas criptográficas sin el debido conocimiento de las mismas no garantiza que la información este protegida, se debe contar con la instrucción adecuada y si se transfiere información de forma encriptado entre países se deben tener presentes las normativas legales.

Observación: No se utilizan mecanismos para encriptación de datos.

A.18.2	**Revisiones de Seguridad de la Información**		
Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.			
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos	**APLICA** **SI** / **NO** Se deben crear comités de seguridad, conformado por las áreas, se debe designar un responsable que recopile y realice un informe gerencial de los resultados de la evaluación a los procesos actividades, controles procedimientos, políticas y tratar los temas referente a la seguridad de la información. **IMPLEMENTADO** **SI** / **NO** Es necesario que se contraten agentes externos que realicen una auditoria interna, de esta forma se obtiene un panorama de la calidad de los procedimientos establecidos y que no hacen parte fundamental del SGSI.

Observación: Se realizan auditorias por agentes externos a la empresa, se auditan ciertos procesos del área de TI como es el proceso de copias de seguridad y mantenimientos preventivos de los equipos de cómputo que son propiedad de la empresa, los procesos auditados se ciñen a la norma ISO 9001.

A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad	**APLICA** **SI** / **NO** Se realizan comités de evaluación para verificar que se cumplan los lineamientos y objetivos trazados al interior de la organización. **IMPLEMENTADO** **SI** / **NO** Se realiza el análisis de los procedimientos realizando auditorías a procesos teniendo en cuenta los diversos aspectos que pueden generar debilidades y de esta forma validar la efectividad de controles previamente establecidos durante el diseño de los procedimientos

Observación: Las auditorías realizadas son ejecutadas sobre el proceso de backup, mantenimiento de equipos de cómputo, estas determinan cuales son las no conformidades y productos conformes según el informe de auditoría entregado al líder del área de TI.

A.18.2.3	Revisión del cumplimiento Técnico.	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	**APLICA** **SI** / **NO** El administrador del sistema debe realizar verificaciones a los procesos y sistemas de información, para garantizar que estos cumplen la función para la cual fueron diseñados. **IMPLEMENTA** **SI** / **NO** La validación de los procesos debe ser responsabilidad de la persona que ha sido designada por el líder de área, esta persona tiene como objetivo la detección de posibles vulnerabilidades y la realización de pruebas de penetración que pongan en riesgo la seguridad de la información.

Observación: las vulnerabilidades que se presentan al interior de la empresa son manejadas por el equipo de soporte, dentro del equipo la persona con la experiencia genera controles en los centros de control de antivirus, de esta forma se trata de minimizar el impacto o nuevos ataques de esa índole.

Realizando un análisis del anexo A de la norma ISO 27001 en relación de cuales controles aplica e implementa la oficina de TI de organización la esperanza s.a, se ha evidenciado que muchos de estos controles han sido incorporados, pero sin tener una guía clara, la incorporación de medidas que salvaguarden la información y de cómo se implantan debe ser considerado como uno de las primeras directrices por parte del líder de equipo de TI. De igual forma mantener y apoyar la gestión dado el cambio que genera la adopción e incorporación del Anexo A de la Norma ISO 27001.

La organización debe analizar e identificar las necesidades de seguridad y cuáles de los controles son requisitos fundamentales para garantizar la seguridad de la información al interior del área de TI.

11. ANÁLISIS DE RIESGOS AL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA ORGANIZACIÓN LA ESPERANZA

Todas las organizaciones se encuentran expuestas a riesgos, esto debido a que no existen espacios que sean totalmente seguros, es por ello que cualquier organización debe supervisar cualquier cambio o anomalía presentada ya que pueden afectar el correcto funcionamiento de la organización. Para la realización del análisis emplearemos la metodología MAGERIT.

La metodología MAGERIT permite realizar análisis y gestión de riesgos, la metodología fue elaborada por el *Consejo Superior de Administración Electrónica de España.*[6] La metodología MAGERIT en diversas formas sistémicas permite la realización de análisis de riesgos que le permiten a la empresa implementar controles a fin de que se reduzcan los costos y mitigar en cierta forma los riesgos que se puedan presentar al interior de la organización.

Una vez establecen los activos de la empresa, se deben identificar las amenazas que puedan afectar tales activos, ya que una de estas puede llegar a desencadenas muchas más. Las amenazas son eventos que pueden desencadenar un incidente en la organización ocasionando daños materiales o perdidos de uno de los activos importantes la Información.

Se logra realizar una medición de la degradación causado por algún incidente, este se caracteriza en base a una fracción del valor del activo.

[6] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.V_RRjYjhCUk

Tabla 7 Estimación del Impacto

Impacto		Degradación		
		1%	10%	100%
Valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente Autor

Todos los activos que reciban una calificación del impacto en escala de muy alto deben tratarse de una forma inmediata.

Estimación el Riesgo: se puede definir un riesgo como la posibilidad que se produzca un impacto en los activos de la organización. Realizar el cálculo del riesgo permite tomar decisiones teniendo en cuenta un nivel de riesgo determinado, se puede establecer una relación entre vulnerabilidad sobre el impacto que nos genera una relación entre los activos y las amenazas.

Los niveles de riesgos se pueden representar utilizando una sencilla técnica matricial en la cual son relacionados los niveles de vulnerabilidad y el impacto, la tabla a continuación se tiene como base para realizar los análisis correspondientes.

Tabla 8 Estimación del Riesgo

Riesgo		Frecuencia			
		PF	FN	F	MF
Impacto	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

Fuente Autor

11.1 IDENTIFICACIÓN DE ACTIVOS

Realizamos la recopilación de los activos teniendo como base de referencia el tipo y su función al interior de la organización

TIPO	NOMBRE DEL ACTIVO
DATOS / INFORMACIÓN	1. [BD_DATAJARDES] Base Datos Operacional
	2. [BD_INTEGRITY] Base Datos Contable Progress
	3. [BD_RECAUDO] Base de datos Recaudo Electrónico
	4. [COD_FU] Código Fuente Aplicaciones
SERVICIOS	5. [SERV_DA] Servicio de directorio Activo
	6. [SERV_PLANIL] Formular y elaborar la planilla única de sueldos de personal activo y cesante
	7. [SERV_CONT_INST] Registrar las operaciones contables y patrimoniales de la institución.
	8. [SERV_PRESU] Formular los Estados Financieros y Presupuestarios de periodicidad mensual, trimestral y anual
APLICACIONES	9. [PORT_WEB] Portal Web
	10. [SI_RECEPCION] Sistema de Recepción de Servicios
	11. [SI_VENTAS]
	12. [SI_INTEGRITY] Sistema de Información Contable y Financiera
	13. [SI_NOMINA] Sistema de Información de Nomina

	14. [CORR_ELEC]Correo Electrónico
	15. [SI _CARTERA]
	16. [SI_INVENTARIO] Sistema de Información de Inventario
	17. [SI_TESORERIA] Sistema de Información de Tesorería
	18. [SO] Sistemas Operativos
	19. [HER_OFI] Herramientas de ofimática Office
	20. [ANT_VIR_KASP] Software Antivirus KASPERSKY ANTIVIR
EQUIPAMIENTO INFORMÁTICO	21. [SRV_FIREWAL] Servidor Firewall
	22. [PC] Equipos de Computo
	23. [SRV_DATOS] Servidor para documentos
	24. [SRV_CONTABLE] Servidor de base de datos contable
	25. [SRV_DA] Servidor Directorio Activo
	26. [SRV_WEB] Servidor Web
REDES DE COMUNICACIONES	27. [MPLS] Conexión Datos e Internet
	28. [ADSL] Conexión Servicio Internet
EQUIPAMIENTO AUXILIAR	29. [CAB_ESTRED] Cableado Estructurado de Red
	30. [CAB_ELECTRIC] Cableado eléctrico
INSTALACIONES	31. [SEDE_PRIN] Instalaciones de Empresa
	32. [RACK] Gabinete de Red
PERSONAL	33. [ING_SIST_III] ingeniero de sistemas (Soporte)
	34. [ING_SIST_II] Ingeniero de Sistemas (Desarrollador)
	35. [ING_SIST_I] Ingeniero de Sistemas (Coordinador de Área)
	36. [ADM_EMP] Administrador de Empresas
	37. [ING_INDUS] Ingeniero Industrial
	38. [ESP_FINA] Especialista Financiero
	39. [OPE_ADMIN] Operador Administrativo
	40. [OPE_CARTERA] Operador de cartera
	41. [OPE_RECEPCION] Operador de recepción

Fuente Autor

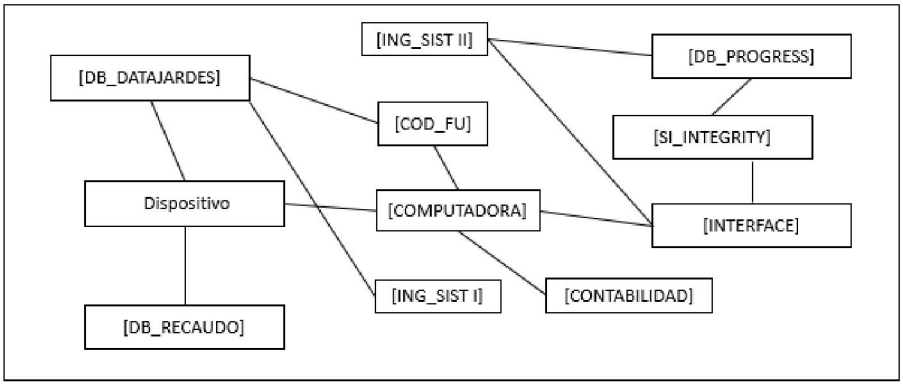
11.2. DEPENDENCIA DE ACTIVOS SEGÚN METODOLOGÍA MAGERIT

Recorrido Top – Down

Se realiza la dependencia de los activos del tipo Datos/ Información

- Las aplicaciones que lo soportan
- Personas que Tienen acceso
- Equipos que interactúan

Figura 3. Dependencia de Activos

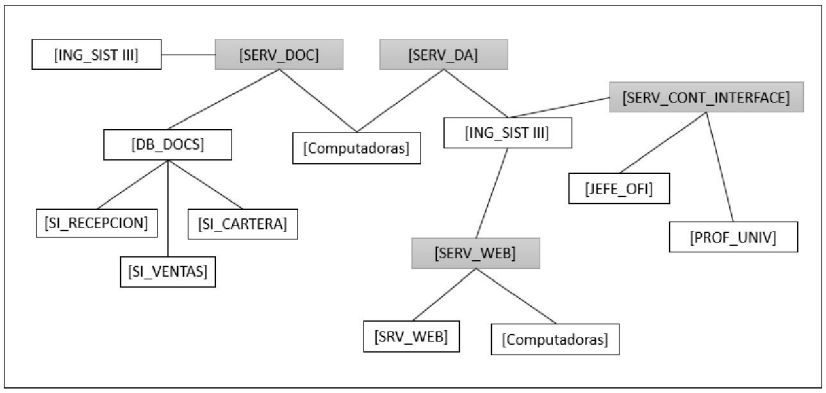


Fuente Autor

Se realiza la dependencia de los activos del tipo Servicios

- Los datos que lo soportan
- Equipos que Personas que Tienen acceso
- Equipos que interactúan
- Personal que interviene

Figura 4. Dependencia de Activo por Servicios

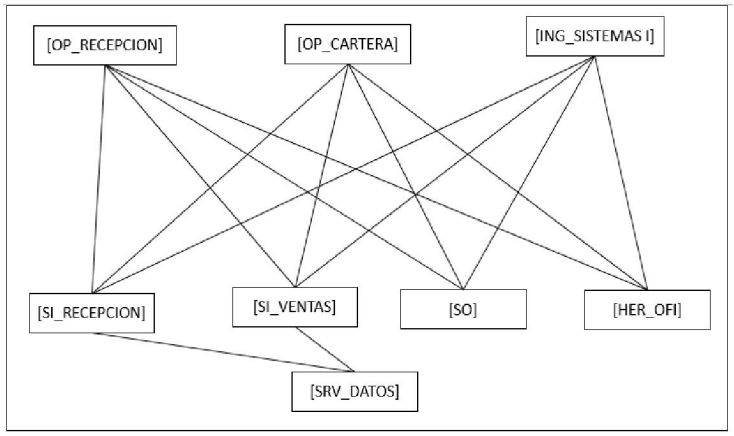


Fuente Autor

Se realiza la dependencia de los activos del tipo Aplicación

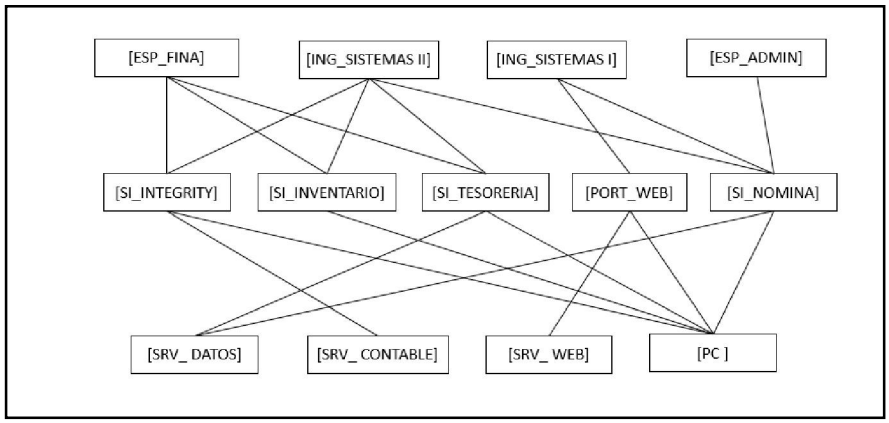
- Los equipos que lo hospedan
- Personal que tiene acceso

Figura 5. Dependencia de activos por Aplicación



Fuente Autor

Dependencia de activos por Aplicación

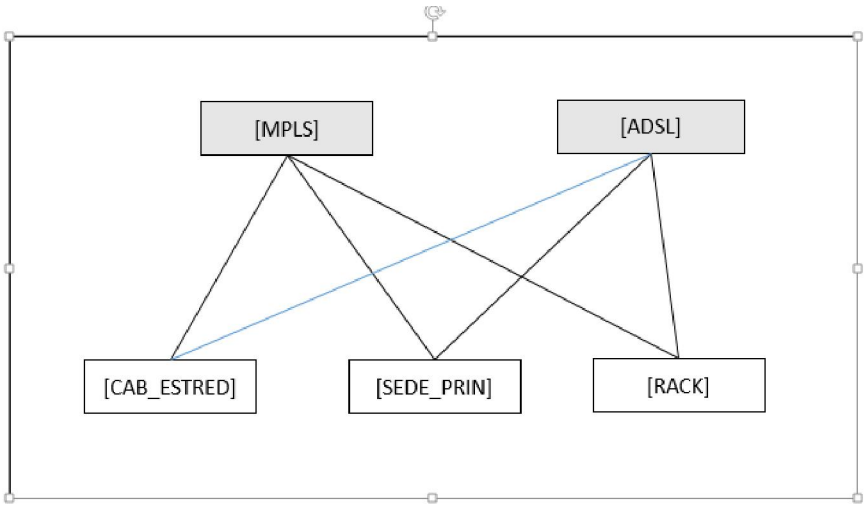


Fuente Autor

Dependencia de tipo Redes De Comunicaciones de:

- Las instalaciones
- El equipamiento auxiliar.

Figura 6. Dependencia de Activos de tipo Comunicación



Fuente: Autor

12. PLAN DE TRATAMIENTO DE RIESGO

Los planes de tratamiento de riesgos son una actividad contemplada dentro de la norma ISO 27001 al momento de implementar y colocar en marcha un SGSI, los planes permiten realizar un análisis de los activos que pueden ser afectados en mayor medida, de esta forma el administrador del sistema logra diseñar, construir e implementar mecanismos que permitan manejar posibles riesgos de seguridad de información.

Tabla Tipos de Activos

Tipos de Activos
[D] Datos Informacion
[S] Servicios
[SW] Software / Aplicaciones
[HW] Hardware
[COM] Redesde comunicaciones
[L] Instalaciones
[P] Personal
[SI] Sistema de informacion

Tabla Dimensiones

Dimensiones	
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
[A]	Autenticidad
[T]	Trazabilidad

Fuente: Autor

Tabla Valoración de Activos

Valor			Criterio
10	Extremo	E	Daño Extremadamente Grave
9	Muy Alto	MA	Daño Muy Grave
6-8	Alto	A	Daño Grave
3-5	Medio	M	Daño Importante
1-2	Bajo	B	Daño Menor
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente: Autor

Tabla Frecuencia de Amenazas

Valor			Criterio
5	Demasiado frecuente	DF	Siempre
4	Muy frecuente	MF	A Diario
3	Frecuente	F	Mensualmente
2	Normal	FN	Una vez al año
1	Poco frecuente	PF	Cada varios años

Fuente Autor

Tabla Valoración de Activos

Activo	Dimensiones de Seguridad				
	[D]	[I]	[C]	[A]	[T]
[BD_DATAJARDES] Base Datos Operacional	[E]	[MA]	[MA]	[MA]	[MA]
[BD_INTEGRITY] Base Datos Contable Progress	[M]	[MA]	[MA]	[MA]	[MA]
[BD_RECAUDO] Base de datos Recaudo Electrónico	[A]	[MA]	[M]	[A]	[A]
[COD_FU] Código Fuente Aplicaciones	[E]			[A]	
[SERV_DA] Servicio de directorio Activo	[A]	[A]	[A]	[A]	[M]
[SERV_PLANIL] Formular y elaborar la planilla única de sueldos de personal activo y cesante	[D]	[A]			
[SERV_CONT_INST] Registrar las operaciones contables y patrimoniales de la institución.	[A]	[MA]	[A]		[A]
[SERV_PRESU] Formular los Estados Financieros y Presupuestarios de periodicidad mensual, trimestral y anual			[A]	[A]	
[PORT_WEB] Portal Web	[D]				
[SI_RECEPCION] Sistema de Recepción de Servicios	[B]	[M]			[B]
[SI_VENTAS]	[A]	[A]		[MA]	[A]
[SI_INTEGRITY] Sistema de Información Contable y Financiera	[E]	[MA]	[MA]		[A]
[SI_NOMINA] Sistema de Información de Nomina	[MA]	[MA]	[A]		
[CORR_ELEC]Correo Electrónico	[M]	[B]	[D]		[B]
[SI _CARTERA]	[MA]		[M]		
[SI_INVENTARIO] Sistema de Información de Inventario	[B]	[M]	[M]		

[SI_TESORERIA] Sistema de Información de Tesorería	[MA]		[M]		
[SO] Sistemas Operativos	[MA]	[A]			
[HER_OFI] Herramientas de ofimática Office	[MA]	[A]			
[ANT_VIR_KASP] Software Antivirus KASPERSKY ANTIVIR	[A]				
[SRV_FIREWAL] Servidor Firewall	[MA]				
[PC] Equipos de Computo	[M]		[A]		
[SRV_DATOS] Servidor para documentos	[E]	[E]			
[SRV_CONTABLE] Servidor de base de datos contable	[E]	[E]			
[SRV_DA] Servidor Directorio Activo	[A]	[M]			
[SRV_WEB] Servidor Web	[M]	[M]	[M]		
[MPLS] Conexión Datos e Internet	[MA]	[A]			
[ADSL] Conexión Servicio Internet	[B]				[B]
[CAB_ESTRED] Cableado Estructurado de Red	[A]	[M]			[M]
[CAB_ELECTRIC] Cableado eléctrico	[MA]				
[SEDE_PRIN] Instalaciones de Empresa					
[RACK] Gabinete de Red	[B]	[D]			
[ING_SIST_III] ingeniero de sistemas (Soporte)	[B]		[MA]		[A]
[ING_SIST_II] Ingeniero de Sistemas (Desarrollador)	[M]		[MA]		[A]
[ING_SIST_I] Ingeniero de Sistemas (Coordinador de Área)	[M]	[A]	[MA]	[A]	[A]
[ADM_EMP] Administrador de Empresas	[B]	[A]		[A]	
[ING_INDUS] Ingeniero Industrial	[D]		[A]		
[ESP_FINA] Especialista Financiero	[B]		[MA]		
[OPE_ADMIN] Operador Administrativo	[B]		[A]	[A]	[A]
[OPE_CARTERA] Operador de cartera	[B]	[A]	[A]	[A]	[A]
[OPE_RECEPCION] Operador de recepción	[B]	[A]	[A]	[A]	[A]

Fuente Autor

Valoración de amenazas / Activos Software

	Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
			D	I	C	A	T
Activos Software	Denegación de Servicio	F					A
	Errores del Administrador	FN	A		A		
	Errores de los usuarios	F	MA	A			
	Errores de Configuración	FN	A				
	Accesos no autorizados	PF		M	M		
	Alteración de información	PF			A		
	Difusión de software malicioso	FN		A	A		
	Abuso de privilegios	PF	A	A			
	Errores de mantenimiento	FN		M			A
	Fugas de información	PF	A		A		
	Interrupción de comunicaciones	F		A			A

Fuente Autor

Valoración amenazas / Servicios

	Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
			D	I	C	A	T
Servicios	Perdida de Datos	F					A
	Caídas de Red	FN	A		A		
	Información errónea	F	MA	A			
	Servidor fuera de servicio	FN	A				
	Denegación de Servicio	PF	A				
	Difusión de software malicioso	FN	A	A	A		
	Abuso de privilegios	PF	A	A			

Fuente Autor

Valoración amenazas / Redes de Comunicación

	Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
			D	I	C	A	T
Redes de Comunicación	Desastres naturales (De cualquier tipo)	PF	MA				MA
	Caídas de Red	FN	A		A		
	Errores de configuración	PF	MA	A			
	Errores del administrador	PF	A		A		
	Análisis de trafico	PF	A				MA
	Errores de tipo físico o lógico	FN	A	A	A		
	Perdida de equipos	PF	A	A			

Fuente Autor

Valoración de amenazas / Equipo Informático

	Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
			D	I	C	A	T
Equipo informático	Fuego	PF	MA	A	MA	MA	MA
	Daños por agua	PF	MA	MA	A	MA	MA
	Errores de equipos	FN		A			
	Errores del administrador	FN	A		A		
	Análisis de trafico	PF			A		MA
	Acceso no autorizado	FN			A		
	Corte de Energía	PF					A
	Condiciones inadecuadas de temperatura	PF		A	A		

Fuente Autor

Valoración amenazas Infraestructura

	Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
			D	I	C	A	T
Infraestructura	Fuego	PF	MA				MA
	Daños por agua	PF	MA				MA

Fuente Autor

Valoración Amenazas /Personal

	Activo / Amenaza	Frecuencia	Dimensiones de seguridad				
			D	I	C	A	T
Equipo informático	Suplantación de identidad	PF	A		A		A
	Abuso de privilegios	PF		MA	MA		
	Alteración de la información	FN		MA	A		
	Destrucción de información	FN	A		A		
	Indisponibilidad del personal	PF			A		MA
	Acceso no autorizado	FN	A		A		
	Extorsión	PF		A		A	A
	Ingeniería social	PF		A			A

Fuente Autor

Tabla de valoración de los activos según amenaza e impacto

ACTIVO	AMENAZA	Impacto				
		D	I	C	A	T
Aplicaciones Informáticas software	Denegación de Servicio					A
	Errores del Administrador	A		A		
	Errores de los usuarios	MA	A			
	Errores de Configuración	A				
	Accesos no autorizados		M	M		
	Alteración de información			A		
	Difusión de software malicioso		A	A		
	Abuso de privilegios	A	A			
	Errores de mantenimiento		M			A
	Fugas de información	A		A		
	Interrupción de comunicaciones		A			A
Servicios	Perdida de Datos					A
	Caídas de Red	A		A		
	Información errónea	MA	A			
	Servidor fuera de servicio	A				
	Denegación de Servicio	A				
	Difusión de software malicioso	A	A	A		
	Abuso de privilegios	A	A			
Redes de Comunicación	Desastres naturales (De cualquier tipo)	MA				MA
	Caídas de Red	A				
	Errores de configuración	MA	A			
	Errores del administrador	A				
	Análisis de trafico	A				MA
	Errores de tipo físico o lógico	A	A	A		
	Perdida de equipos	A	A			
Equipo Informático	Fuego	MA	A	MA	MA	MA
	Daños por agua	MA	MA	A	MA	MA
	Errores de equipos		A			
	Errores del administrador	A		A		
	Análisis de trafico			A		MA
	Acceso no autorizado			A		
	Corte de Energía					A
	Condiciones inadecuadas de temperatura		A	A		
Infraestructura	Fuego	MA				MA
	Daños por agua	MA				MA
Personal	Suplantación de identidad	A		A		A

	Abuso de privilegios		MA	MA		
	Alteración de la información		MA	A		
	Destrucción de información	A		A		
	Indisponibilidad del personal			A		
	Acceso no autorizado	A		A		
	Extorsión		A		A	A
	Ingeniería social		A			A

Fuente Autor

A continuación, se realiza el análisis de riesgos teniendo en cuenta la probabilidad de ocurrencia y el impacto de esta forma se identifican cuáles son los activos que deben ser tratados con mayor prioridad y establecer los mecanismos para minimizar posibles afectaciones a los activos de la empresa.

Tabla de estimación de Impacto

Categoría	Valor de Impacto	Descripción
[E]	5	La materialización de este tipo de riesgos, afecta en gran medida los objetivos y el desarrollo organizacional de la empresa, procesos, servicios e infraestructura.
[MA]	4	La materialización del riesgo afecta de forma directa y en una alta proporción los objetivos de la organización, deterioro patrimonial, deja sin funcionamiento aplicaciones, servicios u infraestructura de la organización
[A]	3	La materialización de este riesgo afecta de forma significativa los objetivos de la organización, deja inoperante parte de la organización, se toma tiempo la detección y corrección de las afectaciones.
[M]	2	La materialización de este tipo de riesgos genera una importante pérdida para la organización, requiere que el equipo de TI y la alta dirección realicen investigaciones para realizar correcciones de las afectaciones.
[B]	1	La materialización de este tipo de riesgos genera daños que se pueden solucionar en espacios de tiempo cortos ya que no afectan los objetivos de la organización.
[D]	0	Este tipo de riesgos no tienen efecto sobre los objetivos de la organización

Fuente: Autor

Tabla de Probabilidad

Categoría	Valor de Probabilidad	Descripción
[E]	5	Riesgo con una probabilidad de ocurrencia extremadamente alta tendencia al 100%
[MA]	4	Riesgo con una alta probabilidad de ocurrencia muy alta, tendencia entre el 81% al 99%
[A]	3	Riesgo con una probabilidad de ocurrencia alta, es decir entre 65% a %80 de que se presente.
[M]	2	Riesgo con una probabilidad de ocurrencia media, es decir entre 41% al 64% de que se presente.
[B]	1	Riesgo con una probabilidad de ocurrencia baja, es decir entre 16% al 40% de que se presente.
[D]	0	Riesgo con una probabilidad de ocurrencia muy baja, es decir entre 1% al 15% de que se presente.

ANALISIS DE RIESGOS

El análisis de riesgos permite definir las políticas de seguridad que deberán ser aplicadas al interior de la organización, de esta forma se generan controles y otros mecanismos para mitigar y dar el manejo adecuado a las posibles amenazas y vulnerabilidades que se puedan presentar al interior del área de TI de la Organización.

TABLA DE EQUIVALENCIAS		
PROBABILIDAD	IMPACTO	VALOR
[E]	[E]	[E]
[E]	[MA]	[MA]
[E]	[A]	[MA]
[E]	[M]	[A]
[E]	[B]	[M]
[E]	[D]	[B]
[MA]	[MA]	[MA]
[MA]	[A]	[A]
[MA]	[M]	[M]
[MA]	[B]	[M]
[MA]	[D]	[B]
[A]	[A]	[A]
[A]	[M]	[M]
[A]	[B]	[M]
[A]	[D]	[B]
[M]	[M]	[M]
[M]	[B]	[B]
[M]	[D]	[B]
[B]	[B]	[B]
[D]	[D]	[D]

Fuente Autor

Tabla de Riesgos

				CRITICIDAD					IMPACTO					RIESGOS				
Ambito	Codigo	Activo	Valor	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
[D]Datos	D1	[BD_DATAJARDES] Base Datos Operacional	[MA]	[E]	[MA]	[MA]	[MA]	[MA]	[MA]	[MA]	[MA]	[MA]	[A]	[MA]	[MA]	[MA]	[MA]	[A]
[D]Datos	D2	[BD_INTEGRITY] Base Datos Contable Progress	[MA]	[M]	[MA]	[MA]	[MA]	[MA]	[MA]	[MA]	[MA]	[MA]	[A]	[MA]	[MA]	[MA]	[MA]	[A]
[D]Datos	D3	[BD_RECAUDO] Base de datos Recaudo Electrónico	[MA]	[A]	[MA]	[M]	[A]	[A]	[A]	[MA]	[A]	[MA]	[A]	[A]	[MA]	[M]	[A]	[A]
[D]Datos	D4	[COD_FU] Código Fuente Aplicaciones	[A]	[E]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[MA]	[A]	[A]	[A]	[A]
[S] Servicios	S1	[SERV_DA] Servicio de directorio Activo	[A]	[A]	[A]	[A]	[A]	[M]	[MA]	[M]	[M]	[M]	[M]	[A]	[M]	[M]	[M]	[M]
[S] Servicios	S2	[SERV_PLANIL] Formular y elaborar la planilla única de sueldos de personal activo y cesante	[M]	[M]	[A]	[MA]	[A]	[A]	[M]	[M]	[M]	[M]	[B]	[M]	[M]	[M]	[M]	[M]
[S] Servicios	S3	[SERV_CONT_INST] Registrar las operaciones contables y patrimoniales de la institución.	[M]	[A]	[MA]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]
[S] Servicios	S4	[SERV_PRESU] Formular los Estados Financieros y Presupuestarios de periodicidad mensual, trimestral y anual	[M]	[A]	[A]	[A]	[B]	[B]	[A]	[MA]	[A]	[M]	[M]	[A]	[A]	[A]	[M]	[M]
[AP]Aplicaciones	AP1	[PORT_WEB] Portal Web	[M]	[M]	[B]	[B]	[M]	[D]	[M]	[M]	[M]	[B]	[B]	[M]	[B]	[B]	[M]	[B]
[AP]Aplicaciones	AP2	[SI_RECEPCION] Sistema de Recepción de Servicios	[MA]	[B]	[M]	[MA]	[MA]	[B]	[M]	[M]	[M]	[MA]	[MA]	[B]	[M]	[A]	[MA]	[M]
[AP]Aplicaciones	AP3	[SI_VENTAS]	[MA]	[A]	[A]	[A]	[MA]	[A]	[M]	[M]	[M]	[MA]	[MA]	[M]	[M]	[M]	[MA]	[A]
[AP]Aplicaciones	AP4	[SI_INTEGRITY] Sistema de Información Contable y Financiera	[E]	[E]	[MA]	[MA]	[MA]	[A]	[MA]	[MA]	[MA]	[E]	[MA]	[MA]	[MA]	[MA]	[MA]	[A]
[AP]Aplicaciones	AP5	[SI_NOMINA] Sistema de Información de Nomina	[MA]	[MA]	[MA]	[A]	[MA]	[MA]	[A]	[A]	[A]	[MA]	[MA]	[A]	[A]	[A]	[MA]	[MA]
[AP]Aplicaciones	AP6	[CORR_ELEC]Correo Electrónico	[A]	[M]	[B]	[D]	[M]	[B]	[A]	[A]	[A]	[A]	[A]	[M]	[M]	[B]	[M]	[M]
[AP]Aplicaciones	AP7	[SI_CARTERA]	[MA]	[MA]	[MA]	[MA]	[M]	[MA]	[MA]	[A]	[A]	[MA]	[MA]	[MA]	[A]	[A]	[A]	[MA]
[AP]Aplicaciones	AP8	[SI_INVENTARIO] Sistema de Información de Inventario	[A]	[B]	[M]	[M]	[M]	[M]	[MA]	[MA]	[MA]	[MA]	[MA]	[M]	[A]	[A]	[A]	[A]
[AP]Aplicaciones	AP9	[SI_TESORERIA] Sistema de Información de Tesorería	[E]	[MA]	[MA]	[M]	[M]	[M]	[E]	[MA]	[MA]	[A]	[A]	[MA]	[MA]	[A]	[M]	[M]
[AP]Aplicaciones	AP10	[SO] Sistemas Operativos	[A]	[MA]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[A]
[AP]Aplicaciones	AP11	[HER_OFI] Herramientas de ofimática Office	[B]	[MA]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[B]	[B]	[A]	[A]	[A]	[M]	[M]
[AP]Aplicaciones	AP12	[ANT_VIR_KASP] Software Antivirus KASPERSKY ANTIVIR	[M]	[A]	[A]	[A]	[A]	[A]	[A]	[A]	[MA]	[B]	[B]	[A]	[A]	[A]	[M]	[M]
[HW] Hardware Informatico	HW1	[SRV_FIREWAL] Servidor Firewall	[A]	[MA]	[MA]	[MA]	[A]	[A]	[MA]	[MA]	[A]	[B]	[A]	[MA]	[MA]	[A]	[M]	[A]
[HW] Hardware Informatico	HW2	[PC] Equipos de Computo	[B]	[M]	[B]	[A]	[B]	[B]	[A]	[M]	[M]	[B]	[B]	[M]	[B]	[M]	[B]	[B]
[HW] Hardware Informatico	HW3	[SRV_DATOS] Servidor para documentos	[E]	[E]	[E]	[E]	[E]	[MA]	[MA]	[A]	[A]	[MA]	[A]	[MA]	[A]	[A]	[MA]	[MA]
[HW] Hardware Informatico	HW4	[SRV_CONTABLE] Servidor de base de datos contable	[E]	[E]	[E]	[E]	[E]	[MA]	[MA]	[A]	[A]	[MA]	[MA]	[MA]	[A]	[A]	[MA]	[MA]
[HW] Hardware Informatico	HW5	[SRV_DA] Servidor Directorio Activo	[MA]	[MA]	[A]	[M]	[MA]	[A]	[MA]	[A]	[A]	[A]	[A]	[MA]	[A]	[M]	[A]	[A]
[HW] Hardware Informatico	HW6	[SRV_WEB] Servidor Web	[A]	[M]	[M]	[M]	[A]	[A]	[A]	[A]	[A]	[B]	[B]	[M]	[M]	[M]	[M]	[M]
[COM]Comunicaciones	COM1	[MPLS] Conexión Datos e Internet	[MA]	[MA]	[E]	[MA]	[MA]	[MA]	[A]	[A]	[A]	[B]	[A]	[A]	[MA]	[A]	[A]	[A]
[COM]Comunicaciones	COM2	[ADSL] Conexión Servicio Internet	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]	[B]
[AUX] Equipamiento Auxiliar	AUX1	[CAB_ESTRED] Cableado Estructurado de Red	[A]	[A]	[M]	[M]	[M]	[M]	[A]	[A]	[A]	[B]	[MA]	[A]	[M]	[M]	[B]	[A]
[AUX] Equipamiento Auxiliar	AUX2	[CAB_ELECTRIC] Cableado eléctrico	[A]	[MA]	[MA]	[MA]	[MA]	[MA]	[A]	[A]	[A]	[B]	[D]	[A]	[A]	[A]	[M]	[B]
[IN]Instalaciones	IN1	[SEDE_PRIN] Instalaciones de Empresa	[B]	[MA]	[M]	[A]	[D]	[D]	[A]	[D]	[D]	[B]	[D]	[A]	[B]	[B]	[B]	[D]
[IN]Instalaciones	IN2	[RACK] Gabinete de Red	[D]	[B]	[D]	[D]	[D]	[D]	[B]	[D]	[D]	[D]	[D]	[B]	[D]	[D]	[D]	[D]
[P] Personal	P1	[ING_SIST_III] ingeniero de sistemas (Soporte)	[MA]	[MA]	[A]	[MA]	[B]	[B]	[A]	[A]	[B]	[B]	[B]	[A]	[A]	[M]	[B]	[B]
[P] Personal	P2	[ING_SIST_II] Ingeniero de Sistemas (Desarrollador)	[A]	[MA]	[MA]	[MA]	[B]	[B]	[A]	[A]	[B]	[B]	[B]	[A]	[A]	[M]	[B]	[B]
[P] Personal	P3	[ING_SIST_I] Ingeniero de Sistemas (Coordinador de Área)	[MA]	[M]	[A]	[MA]	[A]	[A]	[A]	[A]	[B]	[B]	[B]	[M]	[A]	[A]	[M]	[M]
[P] Personal	P4	[ADM_EMP] Administrador de Empresas	[A]	[A]	[A]	[A]	[B]	[B]	[A]	[A]	[B]	[B]	[B]	[A]	[A]	[M]	[B]	[B]
[P] Personal	P5	[ING_INDUS] Ingeniero Industrial	[A]	[A]	[A]	[A]	[B]	[B]	[A]	[A]	[B]	[B]	[B]	[A]	[A]	[M]	[B]	[B]
[P] Personal	P6	[ESP_FINA] Especialista Financiero	[MA]	[M]	[A]	[MA]	[B]	[B]	[A]	[A]	[B]	[B]	[B]	[A]	[A]	[M]	[B]	[B]
[P] Personal	P7	[OPE_ADMIN] Operador Administrativo	[B]	[M]	[A]	[A]	[D]	[D]	[A]	[A]	[B]	[B]	[B]	[M]	[A]	[M]	[B]	[B]
[P] Personal	P8	[OPE_CARTERA] Operador de cartera	[B]	[M]	[A]	[A]	[D]	[D]	[A]	[A]	[B]	[B]	[B]	[M]	[A]	[M]	[B]	[B]
[P] Personal	P9	[OPE_RECEPCION] Operador de recepción	[B]	[M]	[A]	[A]	[B]	[B]	[A]	[A]	[B]	[B]	[B]	[M]	[A]	[M]	[M]	[M]

Fuente Autor

13. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La definición de políticas de seguridad se realiza como guía para la implementación de las medidas de seguridad, estos documentos son la integración y esfuerzo conjunto de los integrantes del área de TI, en la cual se establecen reglas, normas y controles que apoyan a mantener la confidencialidad, integridad y disponibilidad de la información, al igual que los sistemas de comunicación, equipos informáticos y las instalaciones. Actualmente la seguridad de la información en las empresas se ha acrecentado y ha permitido entender cuáles son las posibilidades que albergan las empresas implementando herramientas tecnológicas.

DEFINICIÓN Una política de seguridad es el conjunto de procedimientos que se establecen al interior de una organización para proteger y regular la utilización de los recursos de una empresa, las políticas permiten enmarcar que se puede hacer u está permitido y que no lo está.

CUMPLIMIENTO OBLIGATORIO El cumplimiento de los lineamientos, políticas, normas y estándares de seguridad de la información es de cumplimiento obligatorio, y debe ser tenido en cuenta al momento de realizar la vinculación de nuevo personal a la organización.

13.1 POLÍTICA DE ACCESO A CORREO ELECTRÓNICO

Nombre del documento:	Política de Acceso a correo electrónico
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

El presente documento es propiedad de Organización la Esperanza S.A la utilización del mismo está basado en lo dispuesto en la clasificación del mismo, se prohíbe su divulgación y/o reproducción de forma total o parcial. La utilización y distribución solo está autorizado al interior de Organización La Esperanza S.A y por el personal que esté autorizado.

Descripción de la política:

La política de acceso a correo electrónico define las directrices que deben tenerse en cuenta para el envío y recepción, de información de carácter institucional en Organización la Esperanza S.A.

Alcance:

La presente política aplica para todos los empleados, funcionarios y contratistas.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

Las cuentas de correo electrónico que son creadas y asignadas a los funcionarios y contratistas son de propiedad de Organización la Esperanza S.A, estas son entregadas con la finalidad de enviar y recibir información entre los miembros de la organización, proveedores y demás relacionados con fin institucional.

Las cuentas de correo electrónico son personales e intransferibles, se prohíbe el uso de las cuentas por terceros, el funcionario y/o contratista es el responsable del manejo que se dé a la cuenta de correo electrónico.

Todo el personal debe mantener de forma confidencial la contraseña del correo electrónico que le haya sido asignado.

Si existe sospecha de mala utilización del correo electrónico que afecte el desarrollo de las actividades de la organización, la oficina de tecnologías tendrá la facultad de ingresar y verificar el uso que se le está dando al mismo.

Los mensajes que contengan algún documento adjunto no deberá superar el límite permitido y definido por la oficina de tecnologías de la información.

Formato de Correo Electrónico

Todas las cuentas de correo electrónicas, deben identificar al usuario al cual se le asignan, se debe referenciar con nombre y apellidos seguidos del dominio de la empresa Ejemplo: jose.bautista@organizacionlaesperanza.com .

Todas las cuentas de correo electrónico deberán contener su pie de página la firma del correo que identifica nombres y apellidos, cargo, numero de contacto correo electrónico, y dirección de la empresa. Ejemplo:

Firma de Correo Electrónico

Fuente: Organización la esperanza s.a.

Prohibiciones

Se prohíbe la utilización del correo electrónico para el envío de mensajes masivos (SPAM), imágenes, música etc. Que no tengan relación alguna con los objetivos de la Organización la Esperanza S.A.

Se Prohíbe la distribución de mensajes que discriminen o difamen sobre condiciones sexuales, físicas, psicológicas, religiosas, o destreza alguna que afecten la moral y el buen nombre de las personas.

Se prohíbe el envío de mensajes de carácter político (campañas electorales, comunicados, etc.), religioso o de opinión acerca de terceros, difusión de software ilegal, no licenciado, o cualquier tipo de pornografía y contenido sexual explícito.

Todos los correos electrónicos deben ser validados por software antivirus, esto será responsabilidad del emisor del mensaje, cualquier archivo que se detecte

como infectado no deberá ser abierto y se deberá informar al área de tecnología acerca de su existencia para tratamiento.

En el caso de recibir correos de dudosa procedencia o se sospeche del contenido del mensaje, se debe informar al área de tecnologías sobre este tipo de eventos que puedan afectar la integridad de la información.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.2 POLÍTICA DE ACCESO FÍSICO

Nombre del documento:	Política de Acceso Físico
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

El presente documento es propiedad de Organización la Esperanza S.A la utilización del mismo está basado en lo dispuesto en la clasificación del mismo, se prohíbe su divulgación y/o reproducción de forma total o parcial. La utilización y distribución solo está autorizado al interior de Organización La Esperanza S.A y por el personal que esté autorizado.

Descripción de la política:

La política de acceso físico define las directrices que deben tenerse en cuenta para el ingreso ya sea de personal interno, como externo a zonas en las cuales se procese o almacene información de la Organización la Esperanza S.A.

Alcance:

La presente política aplica para todos los empleados, funcionarios contratistas, proveedores y personal externo.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

Para acceder a las instalaciones los empleados de la organización deben ingresar su huella en el lector biométrico que se encuentra ubicado en la recepción.

Todos los empleados que se encuentran contratados en la Organización la Esperanza S.A deberán tener acceso solo a la información que es estrictamente necesaria para el desarrollo de sus actividades contractuales, en el caso de requerirse algún tipo de permiso excepcional este deberá ser autorizado por el líder de área y el jefe del área tecnologías de la información.

Solo el personal autorizado de la oficina de tecnologías de la información puede acceder a las instalaciones donde se almacena información de la Organización la Esperanza S.A.

Todo el personal ajeno a la Organización la Esperanza S.A debe anunciarse al área a la cual requiere ingresar, el acceso de personal externo debe ser autorizado por el jefe de área o en su defecto por un responsable interno, este responsable deberá responder por las actuaciones que pueda realizar el personal externo.

Las visitas que están autorizadas deben realizar su registro consignando en la recepción de la empresa la hora y fecha de ingreso, nombres completos, motivo de la visita y deberá portar en un lugar visible el documento que lo acredite como visitante en la Organización la Esperanza S.A.

Para ingresar a las instalaciones donde se almacena información este deberá estar acompañado de personal autorizado y solo podrá permanecer en la misma durante cierto periodo de tiempo y de forma justificada.

Cuando un empleado se desvincula de la entidad, se debe reportar a la oficina de tecnologías para que sean revocados los permisos de ingreso a las instalaciones.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.3 POLÍTICA DE COPIAS DE RESPALDO

Nombre del documento:	Política de Copias de Respaldo
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACION

Descripción de la política:

La política copias de respaldo tiene como objetivo mantener el respaldo de la información de forma actualizada de todos los sistemas al interior de la organización.

Alcance:

La presente política aplica para todos los empleados, funcionarios contratistas, proveedores y personal externo.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

Se deben planificar los horarios de ejecución de las copias de seguridad, estas pueden realizarse en cualquier momento, pero siempre deben realizarse en base a un criterio y en concordancia con las áreas en momentos en los cuales el sistema está inactivo, las copias de respaldo deberán en lo posible ser realizadas de forma automática por la aplicación que haya dispuesto la oficina de tecnologías de la organización.

Todas las copias de seguridad realizadas deben ser rotuladas con la fecha, nombre de la información respaldada y se debe incluir el log de la ejecución de la copia almacenada para su consulta de manera posterior. Se debe diligenciar la planilla de copias de seguridad para contar con el registro de ejecución para seguimiento o en el caso de requerirse en alguna auditoria.

Se deben realizar copias de seguridad de todos los servidores y sus configuraciones, por lo menos una vez al mes, de esta manera se rota el medio en el cual se realizan las copias.

Se debe realizar copia de seguridad de toda la información de discos duros, carpetas de red, bases de datos, en dispositivos (Cintas, CD, DVD, Discos duros,

etc.) que permitan su almacenamiento ya sea de forma interna o externa. Todas las copias de seguridad deben estar resguardadas por la oficina de tecnologías de la información de la organización.

El área de tecnología debe garantizar que las copias y los medios de almacenamiento que resguardan información no deberán ser manipulados por agentes externos o por personal no autorizado.

Se deben realizar planes de restauración de copias de seguridad a fin de validar que la información contenida es confiable, y se pueda utilizar posteriormente en el caso de ocurrir cualquier problema.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad.

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.4 POLÍTICA DE ESCRITORIO LIMPIO

Nombre del documento:	Política de Escritorio Limpio
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

El presente documento es propiedad de Organización la Esperanza S.A la utilización del mismo está basado en lo dispuesto en la clasificación del mismo, se prohíbe su divulgación y/o reproducción de forma total o parcial. La utilización y distribución solo está autorizado al interior de Organización La Esperanza S.A y por el personal que esté autorizado.

Descripción de la política:

La política de escritorio limpio busca evitar que tanto a información tanto física como digital se tenga acceso ya sea de forma accidental o mal intencionada.

Alcance:

La presente política aplica para todos los empleados, funcionarios contratistas, proveedores y personal externo.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

La información debe estar disponible para las personas que laboran al interior de la Organización la Esperanza S.A., esto genera que la información pueda encontrarse en ocasiones en los escritorios de los empleados durante su horario laboral, no significa que la información no esté protegida de manera correcta.

Es responsabilidad de cada empleado de la organización mantener segura la información con la cual desempeñan sus labores (CD, DVD, Informes, Memorias USB, Discos Duros, Portátiles), todos los implementos deben estar resguardados en sus puestos de trabajo o de ser el caso disponer de una guaya de seguridad.

No se deben dejar sobre el escritorio de trabajo:

- Contraseñas de inicio de sesión
- Contratos
- Números de Cuenta ya sean personales o de uso institucional
- Listados de Clientes o proveedores
- Documentos que no se deseen publicar
- Documentos con direccionamiento ip
- Llaves o licencias de software

Todos los empleados al momento de culminar su jornada laboral deberán recoger todos los implementos e información sensible al igual que memorias USB, Discos portables, documentos, etc.

Cuando el usuario se encuentre fuera de su estación de trabajo su equipo de cómputo debe estar bloqueado, ya que puede propiciar que otros usuarios utilicen credenciales diferentes a las asignadas y realicen operaciones no autorizadas.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.5 POLÍTICA MANEJO DE MEDIOS REMOVIBLES

Nombre del documento:	Política manejo de medios removibles
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

El presente documento es propiedad de Organización la Esperanza S.A la utilización del mismo está basado en lo dispuesto en la clasificación del mismo, se prohíbe su divulgación y/o reproducción de forma total o parcial. La utilización y distribución solo está autorizado al interior de Organización La Esperanza S. A y por el personal que esté autorizado.

Descripción de la política:

La política de manejo de medios removibles define la manera como deben protegerse los diversos medios de almacenamiento utilizados por los empleados de la organización, de esta forma evitar la publicación, borrado o destrucción de archivos de forma no autorizada.

Alcance:

La presente política aplica para todos los empleados, funcionarios contratistas, proveedores y personal externo.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

Los medios removibles no son opción para respaldar información de la organización la esperanza S.A, esta es responsabilidad de los empleados en mantener la información en los servidores de definidos para esta labor.

Todo medio removible (USB, CD, DVD, Disco duro externo) debe utilizarse solo como medio de transporte de información, estos serán responsabilidad del usuario que tenga asignado tal recurso.

Todos los dispositivos removibles deben ser escaneados por el software antivirus cada vez que sean conectados en cualquier equipo de cómputo de la organización.

Los medios removibles deben ser almacenados en lugares seguros, teniendo en cuenta las especificaciones técnicas que brinda el fabricante.

Al momento de perder vigencia la información almacenada en el medio removible este deberá ser formateado. La información almacenada que necesite estar disponible después de cierto tiempo deberá ser almacenada en medios diferentes al mismo a fin de evitar pérdidas de información que luego pueda ser requerida.

La asignación de los medios removibles debe cumplir con los lineamientos de asignación de equipos la cual requiere el diligenciamiento de una solicitud formal al coordinador de la oficina de tecnologías de la información de la organización justificando por qué y para que será utilizado el medio de almacenamiento.

Los empleados a los cuales se les asigne un medio de almacenamiento removible son responsables del buen uso y cuidado del mismo, en el caso de pérdida o robo este deberá denunciar ante las autoridades competentes e informar al área de tecnologías la pérdida o robo del mismo.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.6 POLÍTICA DE SEGURIDAD DE ANTIVIRUS

Nombre del documento:	Política de seguridad de Antivirus
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S. A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

El presente documento es propiedad de Organización la Esperanza S.A la utilización del mismo está basado en lo dispuesto en la clasificación del mismo, se prohíbe su divulgación y/o reproducción de forma total o parcial. La utilización y distribución solo está autorizado al interior de Organización La Esperanza S.A y por el personal que esté autorizado.

Descripción de la política:

La política de seguridad de Antivirus define las características y aplicaciones que deben tener las aplicaciones antivirus que sean instaladas en la empresa por parte del equipo de tecnologías de la información.

Alcance:

La presente política aplica para todos los empleados, funcionarios y contratistas.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

Todos los equipos que estén conectados a la red de datos de la empresa deben tener instalado el software antivirus que está autorizado por la oficina de Tecnologías de la información.

La instalación del software antivirus debe ser realizada por el personal de la oficina de tecnologías de la información, la desinstalación del mismo se encuentra restringida por medio de solicitud de clave, la cual está bajo conocimiento del personal de soporte.

Una vez instalado la solución antivirus este debe mantenerse activo en todas sus aplicaciones de detección de intrusos, deberá bloquear de forma automática cualquier ataque a la red, navegadores de internet, u archivos que residan en el equipo de trabajo.

Los usuarios no deberán realizar la desinstalación del antivirus ya que pueden generar riesgos de seguridad ante la presencia de virus.

Todos los medios removibles ya sean personales o autorizados deberán ser escaneados por la aplicación antivirus.

Si se presentan problemas de virus en los equipos asignados, el usuario deberá informar al quipo de soporte para que se tomen las medidas correctivas del caso.

Los usuarios serán informados cuando:

- Se detecte cualquier amenaza de virus informático que pueda generar daños al equipo o se propague por medio de la red.
- Al momento de violar las políticas de antivirus
- Cuando a causa de algún virus los archivos sufran daños que no se puedan reparar

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los

lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.7 POLÍTICA DE SEGURIDAD DE BASES DE DATOS

Nombre del documento:	Política de seguridad de bases de datos
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

El presente documento es propiedad de Organización la Esperanza S.A la utilización del mismo está basado en lo dispuesto en la clasificación del mismo, se prohíbe su divulgación y/o reproducción de forma total o parcial. La utilización y distribución solo está autorizado al interior de Organización La Esperanza S.A y por el personal que esté autorizado.

Descripción de la política:

Política de seguridad de bases de datos define los controles que deben tenerse para la instalación, configuración e implementación de los servidores que se encuentran en la empresa. Se define la forma en la cual deben ser creadas las DB y los niveles de permisos que se deben implementar para el acceso tanto de usuarios como de administradores de DB.

Alcance:

La presente política aplica para todos los empleados, funcionarios y contratistas.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

El acceso a los sistemas de base de datos debe ser manejado por un “DBA” Data Base Administrador, quien será el responsable de administrar las bases de datos que estén diseñadas o en ejecución en la empresa. El administrador de la base de datos deberá garantizar la seguridad de la información de la empresa, solo el administrador podrá ingresar a realizar consultas o modificaciones avaladas por el coordinador del área de sistemas.

Se deberá realizar la definición de un perfil con privilegios, que permita realizar acciones cotidianas de soporte de la base de datos. Este perfil deberá tener registro log en el caso de posibles auditorias o la consulta de las operaciones realizadas por este usuario.

La información que reposa en las bases de datos debe ser respaldada, se deben definir mecanismos software que permitan en base a la frecuencia de actualización de la información generar copias de respaldo completos con su respectivo log de registro, las copias de seguridad deben realizarse de forma diaria y deberán ser almacenadas en medios tales como DVD, Cd, Discos Blue Ray. Estos respaldos deberán almacenarse en un lugar restringido para el resto

del personal y las condiciones ambientales deberán ser las más óptimas para evitar deterioro en los medios en los cuales se almacena la información.

No se podrán almacenar copias de respaldo en los equipos de los integrantes del área de tecnologías de la empresa.

El administrador de la base de datos deberá capacitar al área de tecnologías en herramientas manejadoras de la base de datos, que permitan realizar ciertas actividades basadas en privilegios asignados a los usuarios.

Los procedimientos que se generen en la base de datos deberán será analizados por el “DBA”, en conjunto con el coordinador del área de tecnología de la empresa a fin de socializar y aplicar nuevas funcionalidades que surjan de la operación diaria de la empresa.

Todas las bases de datos deben contener registro de auditoría, se deberán implementar rutinas periódicas que permitan verificar la integridad de los datos almacenados.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.8 POLÍTICA DE SEGURIDAD DE LA RED

Nombre del documento:	Política de seguridad de la red
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

Descripción de la política:

La política de seguridad de la red define los controles que deben tenerse en cuenta para la seguridad de la red de comunicaciones de Organización la Esperanza S.A. al igual que la protección de ingresos no autorizados.

Alcance:

La presente política aplica para todos los empleados, funcionarios y contratistas.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

Toda configuración de firewall, Switch, Routers, sistemas de detección de intrusos, y demás equipos de comunicación y protección de la red debe ser soportada en copias de seguridad

Todos los equipos que ingresen a la empresa deben ser verificados y validados por la oficina de tecnologías de la información antes de ser conectados a la red. El área de tecnología debe velar porque no se conecten dispositivos que no estén autorizados.

La conexión por agentes externos a la organización la esperanza s.a debe estar autorizada por la oficina de tecnologías, se debe validar para la conexión del equipo externo que el sistema operativo cuente con las actualizaciones correspondientes, el sistema antivirus actualizados a fin de evitar incidentes de seguridad.

El acceso a servicio de internet debe estar controlado por reglas en el servidor firewall, las reglas deben ser actualizadas y verificadas cada vez que el coordinador de la oficina de tecnologías de la información así lo disponga.

El acceso al servicio de internet al interior de la organización la esperanza s.a debe ser apara los fines previstos; Cualquier solicitud de acceso a este servicio debe estar avalado por la oficina de tecnologías de la organización.

Todas las conexiones remotas hacia los sistemas de información deben estar supervisadas por el responsable designado de la oficina de tecnologías de la información, se deben definir los parámetros de seguridad convenientes para el acceso a la red desde conexiones fuera de la red.

Todos los puertos de aplicaciones que requieran acceder a la red de datos de la organización deben estar avalados y soportados en las reglas del servidor firewall a fin de no permitir ingresos no autorizados.

Las conexiones inalámbricas deben contener reglas de conexión que no permitan el acceso a los dispositivos principales de la red de datos. Se debe mantener listados todos los dispositivos con las claves y ubicación al interior de la organización.

Las contraseñas de conexión a los dispositivos inalámbricos deben tener contraseñas cifradas, no deben contener claves de tipo WEP o WPA, se deben utilizar métodos de encriptación WPA/SDK, WPA2.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

13.9 POLÍTICA DE SEGURIDAD DE INGENIEROS DE SOPORTE

Nombre del documento:	Política de seguridad de Ingenieros de Soporte
Elaborado por:	Ing. Armando Quintero Miranda
Revisado por:	Ing. Rosa Marina Castellanos
Elaborado para la empresa:	Organización La Esperanza S.A
Fecha:	22 de octubre de 2015

NOTA DE CONFIDENCIALIDAD DE ACUERDO A LA CLASIFICACIÓN

El presente documento es propiedad de Organización la Esperanza S.A la utilización del mismo está basado en lo dispuesto en la clasificación del mismo, se prohíbe su divulgación y/o reproducción de forma total o parcial. La utilización y distribución solo está autorizado al interior de Organización La Esperanza S.A y por el personal que esté autorizado.

Descripción de la política:

La política de seguridad de Ingenieros de soporte define las responsabilidades que deben tener los ingenieros de soporte para realización de soporte en la empresa.

Alcance:

La presente política aplica para todos los empleados, funcionarios y contratistas.

Aplicable

La política aplica para todo el personal que es contratado.

La política definida tendrá una duración de carácter interno mientras los empleados estén vinculados a la empresa.

Lineamientos de Seguridad

Los ingenieros de soporte podrán acceder de forma remota a los equipos de cómputo solo para resolver de forma exclusiva y bajo petición del usuario problemas relacionados con el equipo de cómputo asignado.

Los ingenieros de soporte deberán realizar un backup de forma periódica de la información y aplicativos que tengan asignados a su cargo, siempre que cuenten con los medios de almacenamiento correspondientes.

Los ingenieros de soporte deberán validar que todos los equipos de cómputo de la empresa estén registrados en el inventario de equipos e infraestructura de red de la empresa.

Deberán realizar auditorías periódicas sin notificación previa tanto a los equipos de cómputo como a los servicios de la red, de esta forma se identificarán archivos no autorizados, aplicación de configuraciones no permitidas o problemas de vulnerabilidad que puedan colocar en riesgo la información de la empresa.

Los ingenieros de soporte deben realizar la actualización de todos los Sistemas operativos de los equipos registrados en la empresa a fin de evitar posibles brechas de seguridad en base a carencia de actualizaciones por parte del sistema operativo instalado.

Se deben reportar todos los incidentes de seguridad evidenciados, al igual que toda la información que apoye la seguridad de la información de la empresa.

Los ingenieros de soporte no deberán realizar instalaciones no permitidas, aplicación de activadores de paquetes de software, ni la instalación de paquetes de software libre sin la autorización del líder de área, ya que estos podrán ser causales de llamados de atención o sanciones legales.

Los ingenieros de soporte deberán instruir al personal sobre los riesgos que se presentan en materia de información, cuales son las causas que lo generan y cuáles son las políticas de seguridad establecidas para el resguardo de la información.

Responsabilidades

De la dirección:

Promover la divulgación de la política por los canales internos de comunicación (intranet, correo electrónico, boletines internos), a todos los empleados funcionarios y/o contratistas de la empresa. La dirección deberá tomar los correctivos o medidas disciplinarias a que haya lugar por el no cumplimiento de las mismas.

Responsabilidades del área de tecnologías de la información:

El área de tecnologías de la información debe realizar la socialización de la política a los empleados de la Organización la Esperanza. Debe contar con un proceso de que permita la recepción de la política definida.

La política y los lineamientos que conlleva la misma deben informarse al momento que ingresa personal nuevo a la entidad

Responsabilidades de los empleados:

Todos los empleados deben acatar las políticas establecidas, Cualquier forma de obstinación, o de diferencia ante las mismas es considerada como una falta a los lineamientos establecidos y no será tolerada. Este principio deberá ser aplicado a todos los niveles de la organización sin excepción alguna.

NOTA:

Las personas que no estén dispuestas a adherir a la normativa de la empresa no podrán formar parte de la Empresa, dado que esos documentos enuncian sus responsabilidades.

14. CONCLUSIONES

Con el diseño de las políticas de seguridad de la información presentadas a la empresa y ante la alta dirección se logró la aprobación y aplicación de las mismas al interior de la oficina de Tecnologías de la información de organización la esperanza, acompañado de diversos elementos tecnológicos, que les permitirá alcanzar y realizar los objetivos propuestos con la implementación de las políticas de seguridad.

Como consecuencia de la aplicación de políticas de seguridad la empresa debe centrar parte de su actividad en abastecerlos sistemas e infraestructura tecnológica que promuevan e impulsen los mecanismos propuestos para salvaguardar la información de la empresa, el establecimiento de estas políticas en lo necesario debe estar apegado a la ley y la normativa de la empresa.

En otro aparte y teniendo presente las normativas sobre seguridad de la información tema en el cual se basó este documento, el mismo aporta un avance significativo al área de sistemas mediante la adopción de las políticas diseñadas, participa y apoya a minimizar las amenazas y posibles vulnerabilidades.

15. BIBLIOGRAFÍA

GUTIERREZ, Amaya Camilo. Los renovados Anexos de ISO/ IEC 27001-2013 <http://www.welivesecurity.com/la-es/2013/10/18/renovados-anexos iso-iec-27001-2013/> [Citado el 18 de octubre de 2013]

Constitución política de Colombia. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492> [Citado diario oficial 47.223 de enero]

27001 Academy, Una introducción simple a los aspectos básicos.

<http://www.iso27001standard.com/es/que-es-iso-27001/ > [Citado 2016]

RODRIGUEZ, Rico Juan Carlos, Gestión de la Seguridad

<http://www.fundaciondedalo.org/archivos/ACTIVIDADES/SSI07/GestionDeLaSeguridad.pdf> [Articulo Web].

Iso-27001-2013 <http://www.sgs.co/es-ES/Health-Safety/Quality-Health-Safety-and-Environment/RiskAssessment-and-Management/Security-Management/ISO-27001-2013-Information-Security-Management-Systems.aspx> [Artículo Web]

Metodología plan de Seguridad < http://www.youblisher.com/p/588309-Metodologia-plan-de-seguridad/> [Articulo Web]

ISO – SGSI http://www.gesconsultor.com/iso.html [Articulo Web]

Ley 1273 de 2009 <http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm > [Citado Bogotá 05 de enero de 2009]

WILFRED, Uriel García. Políticas, Planes y Procedimientos de Seguridad informática para ElectroSoftSystem. [Citado UNIVERSIDAD FRANCISCO DE PAULA SANTANDER, 2012]

Plan de Seguridad Informática <http://instituciones.sld.cu/faenflidiadoce/files/2014/04/Plan-de-Seguridad-Inform%C3%A1tica-1.pdf> [Articulo Web, Citado 18 de febrero de 2016]

GINA Elizabeth Maza Anton, Plan de contingencia informático y seguridad de información 2009 <http://www.eumed.net/libros-gratis/2009c/605/indice.htm > [Citado 2009]

16. ANEXOS

16.1 ANEXO A

AUTORIZACIÓN DE EJECUCIÓN DE PROYECTO EN EMPRESA

Organización
La Esperanza
Contigo a cada paso.

San Jose de Cúcuta, Marzo 31 de 2015

Ingeniero
ARMANDO QUINTERO
Ciudad

Respetado Ingeniero:

De manera atenta manifestamos nuestro interés y conocimiento de la propuesta de Proyecto de investigación titulada: "PLAN DE SEGURIDAD INFORMATICA (SGSI)" fundamentado en el estándar internacional ISO 27001, y la cual aceptamos se desarrolle para nuestra Organización.

En este sentido, nos comprometemos a participar en este proceso ofreciendo la información y el apoyo necesario para el desarrollo de la propuesta.

Atentamente,

ISABEL CRISTINA RINCON RODRIGUEZ
Gerente General

RAZÓN SOCIAL
Jardines de Esperanza S.A.
NIT. 890.504.437-1

OCAÑA
Calle 12 No. 10-43 B. El Tamaco
Teléfono: 582 57 12
Parque Cementerio
Km 1 Vía al Aeropuerto

BUCARAMANGA
Mayorbo
Km 3.5 Anillo Vial
Floridablanca - Girón
Teléfono: 679 86 21

CÚCUTA
Diagonal Santander No. 8-93
Teléfono: 582 96 66
Parque Camentario
Km 4 Vía Los Patios

ISO 9001
icontec
Certificado SC 4366-1

IQNet

www.organizacionlaesperanza.com

16.2 ANEXO B

ENCUESTA

La encuesta que se presenta a continuación fue efectuada tanto a miembros del equipo de Ti de la empresa como a usuarios que ejercen funciones diferentes a las del equipo del área de tecnología, con el fin de realizar un diagnóstico del estado actual de la seguridad de la información y el conocimiento por parte de empleados de la empresa.

Modelo de encuesta:

CUESTIONARIO Nº 1

DIAGNÓSTICO DEL ESTADO ACTUAL DE LA DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA JARDINES DE ESPERANZA S.A

1. ¿Tiene usted conocimiento sobre lo que significa un plan de seguridad de información? SI ___ NO ___

2. ¿Cree usted que el diseño de un plan de Seguridad de la Información permitirá mejorar la calidad tecnológica de la Empresa Organización La Esperanza S.A.? SI ___ NO ___

3. ¿Cree usted que se logrará un cambio positivo con la aplicación de este plan de seguridad de información en la plataforma tecnológica de la Empresa Organización La Esperanza S.A.?

SI ___ NO ___

4. ¿Aprobaría usted la implementación del plan de Seguridad de la Información para la plataforma tecnológica de la Empresa Organización La Esperanza S.A.?

SI ___ NO ___

5. ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la Seguridad de la Información en la Empresa Organización La Esperanza S.A.?

SI ___ NO ___

6. ¿Estaría usted dispuesto a colaborar para que este plan de seguridad pueda ser llevado a cabo en las instalaciones de la Empresa Organización La Esperanza S.A.?

SI ___ NO ___

7. ¿Sabe usted si existe un plan de recuperación ante desastres en Organización La Esperanza S.A.?

SI ___ NO ___

8. ¿En la Organización La Esperanza S.A. se ha realizado evaluación de riesgos relacionados con la información?

SI ___ NO ___

9. ¿En la Empresa se ha realizado una evaluación de vulnerabilidades de la red?

SI ___ NO ___

10. ¿La Empresa Jardines de Esperanza S.A. cuenta con software antivirus actualizado?

SI ___ NO ___