ESTUDIO DE ANÁLISIS Y GESTIÓN DE RIESGO AL SISTEMA DE INFORMACIÓN DE LA EMPRESA AGESAGRO S.A.S UTILIZANDO LA METODOLOGÍA MAGERIT

JUAN CARLOS VARÓN QUIROGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2017

ESTUDIO DE ANÁLISIS Y GESTIÓN DE RIESGO AL SISTEMA DE INFORMACIÓN DE LA EMPRESA AGESAGRO S.A.S UTILIZANDO LA METODOLOGÍA MAGERIT

JUAN CARLOS VARÓN QUIROGA

Monografía para optar al título de
Especialista en Seguridad Informática

Director de Proyecto
Esp. Ing. Hernando José Peña Hidalgo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2017

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Ibagué 17 de Abril de 2017

DEDICATORIA

A Dios, mi padre Q.E.P.D. a mi madre por su apoyo incondicional, mi hermana y familia que han estado dispuestos a colaborarme en todo lo que he necesitado, a mis amigos que han influido para la continuación de mi formación.

Juan Carlos

AGRADECIMIENTOS

Juan Carlos expresa sus agradecimientos a:

Esp. Ing. Hernando José Peña Hidalgo por su disponibilidad y colaboración en esta monografía y ser de gran ayuda brindando su conocimiento para el enriquecimiento del mismo.

A todos los integrantes de la empresa AGESAGRO S.A.S por todos los recursos e información sin la cual no hubiera sido posible el producto final. A los Ingenieros Agrónomos Juan Rodrigo Alvarado Moreno por permitir el acompañamiento a bancos para conseguir la información, Luis Humberto Lastra por enseñar el manejo de la plataforma Athenea, Rafael Bonilla Ospina por permitir las visitas a los predios y Henry Rivas Escobar por enseñarme términos y formatos manejados, los cuales entre todos permitieron que se conociera el proceso desde el principio todo su desarrollo y finalización del mismo y la información necesaria para poder entender mucho mejor el proceso realizado por la empresa.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág

GLOSARIO

ACTIVO Conjunto de todos los bienes y derechos con valor monetario que son propiedad de una empresa, institución o individuo[1].

AGESAGRO S.A.S: asesorías y gestiones agropecuarias sociedad por acciones simples.

AMENAZA: las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.[2]

ATHENEA: plataforma de visitas usada por FINAGRO para subir información de las mismas.

CONFIDENCIALIDAD: la cualidad de confidencial (que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos). Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas[3].

DISPONIBILIDAD: en la comunidad de IT, la métrica empleada para medir la disponibilidad es el porcentaje de tiempo que un sistema es capaz de realizar las funciones para las que está diseñado[4].

FINAGRO: el Fondo para el Financiamiento del Sector Agropecuario, es una entidad que promueve el desarrollo del sector rural colombiano, con instrumentos de financiamiento y desarrollo rural, que estimulan la inversión.[5]

INTEGRIDAD: la corrección de todos los elementos que presenta una base. Cuando se utilizan sentencias como INSERT, DELETE o UPDATE, la integridad de los datos puede verse afectada. Por ejemplo, se pueden añadir datos no

---

[1] Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). Consultado en http://dle.rae.es/?id=0clfXYb

[2] Departamento de seguridad informática. Amenazas a la Seguridad de la Información. Universidad Nacional de Luján, Luján, Buenos Aires, Argentina. Disponible en Internet: http://www.seguridadinformatica.unlu.edu.ar/?q=node%2F12

[3] PEREZ. Julián. (2013). Definición de confidencialidad. Recuperado de http://definicion.de/confidencialidad/

[4] TechNet. (2005). Descripción de la disponibilidad, la confiabilidad y la escalabilidad. Consultado enhttps://technet.microsoft.com/es-es/library/aa996704(v=exchg.65).aspx

[5] Finagro. ¿Qué es FINAGRO?. Bogotá Colombia. 2013. Disponible en Internet: https://www.finagro.com.co/qui%C3%A9nes-somos/informaci%C3%B3n-institucional

válidos o modificarse datos existentes en forma incorrecta, con lo que la integridad no se cumple[6].

ITIL: un conjunto de libros que ofrecen una guía que constituyen las mejores prácticas en la provisión de servicios TIC en base a los requeridos del cliente.[7]

ITSM: emplea buenas prácticas basadas en procesos para satisfacer los requisitos de los clientes en relación a los servicios TIC.

MAGERIT: es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.[8]

POLÍTICA DE SEGURIDAD: la política de seguridad es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas de información y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.[9]

PROTECCIÓN DE DATOS: sistema legal que garantiza la confidencialidad de los datos personales en poder de las Administraciones públicas u otras organizaciones.[10]

RIESGO: la noción de riesgo suele utilizarse como sinónimo de peligro. El riesgo, sin embargo, está vinculado a la vulnerabilidad, mientras que el peligro aparece asociado a la factibilidad del perjuicio o daño[11].

SEGURIDAD: comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.[12]

---

[6] PEREZ. Julián. (2013). Definición de confidencialidad. Recuperado de http://definicion.de/integridad/

[7] Fernández, V. E. (2009). El gobierno y la gestión de las TIC: una aproximación práctica al ámbito del sector público universitario. Madrid, ES: Dykinson. Retrieved from http://www.ebrary.com

[8] Consejo Superior de Administración Electrónica. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. España. 2012. Disponible en Internet: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VybNzvnhBpg

[9] ROMERO. Luis. Seguridad informática conceptos generales. España. Disponible en Internet: http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

[10] Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). Consultado en http://dle.rae.es/?id=URUdTVs

[11] PEREZ. Julián. (2013). Definición de confidencialidad. Recuperado de http://definicion.de/riesgo/

[12] Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). Consultado en http://dle.rae.es/?id=LXrOqrN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): es un conjunto de procesos que permiten establecer, implementar, mantener y mejorar de manera continua la seguridad de la información, tomando como base para ello los riesgos a los que se enfrenta la organización.[13]

TIC: Tecnologías de la Información y la Comunicación.[14]

VULNERABILIDAD: debilidad de cualquier tipo que compromete la seguridad del sistema informático.[15]

[13] Gómez, F. L., & Fernández, R. P. P. (2015). Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. Madrid, ES: AENOR - Asociación Española de Normalización y Certificación. Retrieved from http://www.ebrary.com

[14] Fernández, V. E. (2009). El gobierno y la gestión de las TIC: una aproximación práctica al ámbito del sector público universitario. Madrid, ES: Dykinson. Retrieved from http://www.ebrary.com

[15] MIFSUD. Elvira. Introducción a la seguridad informática - Vulnerabilidades de un sistema informático. España. 2012. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

RESUMEN

El propósito de este documento es aplicar el método MAGERIT a la empresa AGESAGRO S.A.S, con la finalidad de analizar amenazas, vulnerabilidades y riesgos en el manejo de la información.

Primero se identifica el estado actual de la empresa historia, misión, visión, ubicación geográfica y estructura organizacional. Luego se identifican los activos informáticos para poder realizar luego el análisis de la información que manejan. Se determinan las amenazas encontradas al analizar cada uno de los activos informáticos.

Se realiza un cuadro de análisis de riesgos con los incidentes encontrados y finalmente se realizan unas sugerencias frente a los hallazgos encontrados revisando los puntos críticos y recomendaciones para poder contrarrestar la posibilidad de fuga de la información.

Palabras clave: AGESAGRO S.A.S, amenaza, Finagro, MAGERIT, riesgo, vulnerabilidad.

ABSTRACT

The purpose of this document is to apply the MAGERIT method to the company AGESAGRO S.A.S, in order to analyze threats, vulnerabilities and risks in the management of information.

First identify the current state of the company history, mission, vision, geographical location and organizational structure. Then the computer assets are identified to be able to then carry out the analysis of the information they manage. The identified threats are determined when analyzing each of the computer assets.

A table of risk analysis is carried out with the incidents found and finally some suggestions are made against the findings found by reviewing the critical points and recommendations to be able to counteract the possibility of information leakage.

Keywords: Agesagro, threat, FINAGRO, magerit, risk, vulnerable.

TITULO

ESTUDIO DE ANÁLISIS Y GESTIÓN DE RIESGO AL SISTEMA DE INFORMACIÓN DE LA EMPRESA AGESAGRO S.A.S UTILIZANDO LA METODOLOGÍA MAGERIT

INTRODUCCIÓN

Al contar con acceso a información de los usuarios que han realizado créditos de inversión, aplicando a la empresa AGESAGRO S.A.S. la metodología MAGERIT se realiza una verificación del estado actual de la empresa verificando y analizando los activos con los que cuenta para poder determinar los riesgos, amenazas y vulnerabilidades.

Al utilizar la metodología que incluye el análisis de riesgos y vulnerabilidades del manejo de la información sensible de usuarios y bancos por terceros. Se pueden establecer controles y políticas para mejorar el nivel de seguridad de la información manejada por la empresa, un conjunto de reglas claras, y bien definidas, para denegar el acceso a los datos de los usuarios a personas mal intencionadas que puedan buscar hacer mal uso de esa misma información.

1. DEFINICIÓN DEL PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

Asesorías y gestiones agropecuarias sociedad por acciones simples - AGESAGRO S.A.S, es una sociedad encargada de apoyar el acceso a los créditos en el sector rural de Colombia por medio de programas de capacitación, consultorías, asesorías y auditorias en el beneficio de empresarios agropecuarios, ofreciendo monitoreo de proyectos aplicando tecnologías en informática y comunicación, se utilizan equipos informáticos para el manejo de la información.

Se maneja la información de 1600 usuarios, por lo tanto es una cantidad considerable de información de usuarios con créditos que maneja, frente a consultas de buenas prácticas y sobre el nivel de seguridad que se utiliza para el manejo de la información no hay una capacitación clara sobre mucha información que deberían manejar y poder asegurar la integridad, confidencialidad y disponibilidad de la información.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo diseñar un sistema de seguridad y sus correspondientes controles de riesgos basados en la norma ISO 27002:2013 para reducir las vulnerabilidades, riesgos y amenazas a la seguridad en la información administrada por la empresa AGESAGRO S.A.S?

2. JUSTIFICACIÓN

El uso de tecnologías en AGESAGRO S.A.S. en la actualidad es fundamental para un ágil uso de la misma, pero por falta de conocimiento de ciertos parámetros que se deban seguir la información y confiabilidad se puede ponerse en riesgo, el desconocimiento de buenas prácticas en el uso de controles puede hacer que el buen nombre de la empresa no pierda credibilidad en caso de una fuga de información sensible y esto puede llegar a ser la muerte para la empresa que debe mantener uno de sus bienes más importantes que es la seguridad de su información.

El uso de controles, capacitaciones y buenas practicas es el paso necesario para poder dar solución o tener una contramedida frente a los riesgos y vulnerabilidades que pueda contar la empresa para que la información activo fundamental pueda mantener un mayor nivel de disponibilidad, integridad, confidencialidad y confiabilidad en este caso el beneficiario seria la empresa AGESAGRO S.A.S.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar controles de seguridad de la información y control de riesgos para la empresa AGESAGRO S.A.S, bajo la norma ISO 27002:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar un informe del estado actual del sistema de información de la empresa AGESAGRO S.A.S.
- Identificar los activos de información que pertenecen a la empresa AGESAGRO S.A.S. y clasificarlos a acuerdo a la metodología MAGERIT.
- Identificar las amenazas y riesgos de los activos de información en la empresa AGESAGRO S.A.S.
- Proponer controles basados en la norma ISO 27002:2013 a los riesgos identificados en la empresa AGESAGRO S.A.S.
- Diseñar políticas de seguridad, con base a los controles propuestos.

4. ALCANCES Y LIMITACIONES

4.1 ALCANCES:

La presente monografía se encuentra entre los proyectos de investigación proyectiva y lo que pretende es proponer un conjunto de políticas de seguridad utilizando la metodología MAGERIT basada en la norma ISO 27001:2013 donde se realizará un análisis de riesgos y posteriormente diseñar una propuesta, pero de la implementación se hace cargo la institución.

4.2 LIMITACIONES:

Es conveniente resaltar que el desarrollo de la presente monografía no abarcará temas como los que se definen a continuación:

1. No se realizará Análisis de algoritmos o arboles de ataque de la metodología MAGERIT.
2. No se realizarán las Técnicas gráficas, sesiones de trabajo, valoración Delphi.
3. No se mostrarán resultados de aplicar los consejos establecidos.
4. Se realizarán políticas de seguridad para el área de gerencia de la empresa AGESAGRO S.A.S. proponiendo un conjunto de
5. No se realizara implementación, sino una propuesta de conjuntos de controles y políticas de seguridad que quedará a cargo de la empresa.

5. MARCO DE REFERENCIA

5.1 MARCO TEÓRICO

La investigación proyectiva tiene como objetivo diseñar o crear propuestas dirigidas a resolver determinadas situaciones. Los proyectos de arquitectura e ingeniería, el diseño de maquinarias, la creación de programas de intervención social, el diseño de programas de estudio, los inventos, la elaboración de programas informáticos, entre otros, siempre que estén sustentados en un proceso de investigación, son ejemplos de investigación proyectiva. Este tipo de investigación potencia el desarrollo tecnológico[16].

El ciclo PHVA o ciclo de Deming fue dado a conocer por Edwards Deming en la década del 50, basado en los conceptos del estadounidense Walter Shewhart. PHVA significa: Planificar, hacer, verificar y actuar. En inglés se conoce como PDCA: Plan, Do, Check, Act. Este ciclo constituye una de las principales herramientas de mejoramiento continuo en las organizaciones, utilizada ampliamente por los sistemas de gestión de la calidad (SGC) con el propósito de permitirle a las empresas una mejora integral de la competitividad, de los productos ofrecidos, mejorado permanentemente la calidad, también le facilita tener una mayor participación en el mercado, una optimización en los costos y por supuesto una mejor rentabilidad[17].

El SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información e ISMS son las siglas equivalentes en ingles a Information Security Management System. Podemos entender por información todo el conjunto de datos que se organizan en una organización y otorgan valor añadido para ésta, de forma independiente de la forma en la que se guarde o transmita, el origen que tenga o la fecha de elaboración. El Sistema de Gestión de Seguridad de la Información, según ISO 27001 consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización[18].

Según el especialista de Awareness & Research H. Camilo Gutiérrez Amaya menciona “En este sentido fue desarrollado MAGERIT una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta

---

[16] HURTADO DE BECERRA, Jacqueline. Guía para la comprensión Holística de la Ciencia. Caracas Venezuela, Edit. Sypal. 2010.

[17] SANCHEZ MORENO. Yuli. Ciclo PHVA. Diciembre 2014. Disponible en Internet: http://www.gerencie.com/ciclo-phva.html

[18] ¿Qué es un SGSI?. 2012, http://www.iso27000.es/sgsi.html [Consulta: Sábado, 12 de Noviembre de 2016]

forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos."[19]

Miguel Ángel Mendoza menciona en el artículo ¿Cuál es la idea central de aplicar ISO 27001? "en la realidad difícilmente se pueden evadir todas las amenazas y ataques, por lo que en caso de que sucedan, uno de los propósitos es corregir los errores y evitar que vuelvan a presentarse, a través de lecciones aprendidas y las acciones correctivas."[20]

5.2 MARCO CONCEPTUAL

5.2.1. Amenaza. Es la probabilidad de pérdida material o inmaterial, frente a un peligro o riesgo de factor externo. En el factor matemático es una probabilidad de exceder un nivel en que esta pérdida ocurra. Pueden ser de índole personal, de programación o un factor externo como naturaleza o incendios. Frente a las amenazas informáticas afectan la disponibilidad, integridad, confidencialidad y confiabilidad, o autenticación de los datos.

5.2.1.1 Tipos de amenazas en informática. Se pueden clasificar según el daño causado a los sistemas clasificados en:

- Intercepción: cuando una persona, programa o proceso logra el acceso a una parte del sistema a la que no está autorizada. Por ejemplo, la escucha de una línea de datos, o las copias de programas o archivos de datos no autorizados. Estas son más difíciles de detectar ya que en la mayoría de los casos no alteran la información o el sistema.
- Modificación: este tipo de amenaza se trata no sólo de acceder a una parte del sistema a la que no se tiene autorización, sino también de cambiar su contenido o modo de funcionamiento. Por ejemplo, el cambiar el contenido de una base de datos, o cambiar líneas de código en un programa.
- Interrupción: se trata de la interrupción mediante el uso de algún método el funcionamiento del sistema. Por ejemplo, la saturación de la memoria o el

[19] GUTIERREZ, Camilo, MAGERIT: metodología práctica para gestionar riesgos, 2013, http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/ [Consulta: Sábado, 22 de Agosto de 2015]

[20] MENDOZA, Miguel, ¿Cuál es la idea central de aplicar ISO 27001?, 2015, http://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/ [Consulta: Sábado, 22 de agosto de 2015]

máximo de procesos en el sistema operativo o la destrucción de algún dispositivo hardware de manera malintencionada o accidental.

- Generación: generalmente se refiere a la posibilidad de añadir información a programas no autorizados en el sistema. Por ejemplo, el añadir campos y registros en una base de datos, o adicionar código en un programa (virus), o la introducción de mensajes no autorizados en una línea de datos[21].

5.2.2. Vulnerabilidad. Es un grado de pérdida o elementos que pueden estar bajo un riesgo dentro de una escala que es afectado por el fenómeno que caracteriza la amenaza.

5.2.2.1 Tipos de Vulnerabilidad informática. Se pueden agrupar en función de:

- Vulnerabilidad Física: Es la posibilidad de ingresar directamente al sistema para robar, manipular o destruir el sistema de forma física.
- Vulnerabilidad Natural: El daño en el sistema afectado por desastres naturales, ambientales, dañando el sistema como lo es el fuego, inundaciones, rayos, terremotos o fallos de electricidad, el polvo. Humedad y temperatura excesiva.
- Vulnerabilidad de hardware y software: Frente a hardware o dispositivos según el material que son elaborados pueden ser más delicados que otros, esto es frente al material. Algunos fallos o debilidades del software pueden hacer que sean menos fiables y confiables para su intrusión.
- Vulnerabilidad de medios o dispositivos: Peligro frente al robo o daños de discos o impresiones.
- Vulnerabilidad por emanación: Los dispositivos electrónicos emiten radiaciones electromagnéticas, y también existen equipos o dispositivos para descifrar o reconstruir la información almacenada o que se trasmite.
- Vulnerabilidad de las comunicaciones: Las computadoras en red suponen una vulnerabilidad al sistema, ya que el riesgo es mayor, porque se aumenta el nivel de acceso al mismo, y con ello también la intercepción de las comunicaciones, penetrando al sistema, interceptando la información entre terminales.
- Vulnerabilidad humana: La mayor vulnerabilidad en el sistema se encuentra entre los administradores y usuarios del mismo, ya que pueden acceder al

[21] BENAVIDES, Mirian. SOLARTE, Francisco. (2012). Módulo de riesgos y control informático, (pp 18). Pasto, Colombia.

sistema de forma física o por conexión para ello deben realizarse y adoptar medidas de seguridad[22].

5.2.3. Riesgos. Es la exposición de adversidad junto a circunstancias del entorno, que generan una posibilidad de perdidas, generando una falla en las organizaciones o pérdidas por diversas causas. Su diferenciación es de acuerdo a las causas y efectos.

5.2.3.1 Tipos de riesgos. Los riesgos se pueden clasificar en:

- Riesgos Financieros: los riesgos financieros incluyen la relación entre una organización y una ventaja que puede ser pérdida o perjudicada. De este modo el riesgo financiero contiene tres elementos que son la organización que está expuesta a pérdidas, los elementos que conforman las causas de pérdidas financieras y el peligro que puede causar la perdida (amenaza a riesgo).
- Riesgos Dinámicos: generalmente son el resultado de cambios en la economía que surgen de dos conjuntos de factores externos como la economía, la industria, competidores y clientes, además de otros factores que pueden producir las pérdidas que constituyen las base del riesgo especulativo y están relacionadas con las decisiones de la administración de la organización.
- Riesgos Estáticos: las causas de estos riesgos son distintas a las de la economía y generalmente se deben a la deshonestidad o fallas humanas.
- Riesgo Especulativo: Describe una situación que espera una posibilidad de pérdida o ganancia.
- Riesgo Puro: son aquellas situaciones que solamente generan pérdida o ganancia, un ejemplo es la posibilidad de pérdida en la compra de un bien (automóviles, casas, etc.). Dentro de los riesgos puros están los siguientes:
    - Riesgo personal, relacionado con la posibilidad de pérdida por muerte prematura, enfermedad e incapacidades
    - Riesgos de las posesiones, donde la pérdida puede ser directa por destrucción de bienes, e indirectas causados por las consecuencias de las pérdidas directas o gastos adicionales.

[22] BENAVIDES, Mirian. SOLARTE, Francisco. (2012). Módulo de riesgos y control informático, (pp 17). Pasto, Colombia.

- Riesgos de Responsabilidad, relacionadas con el perjuicio de otras personas o daño de una propiedad por negligencia o descuido.
- Riesgos físicos, por ejemplo el exceso de ruido, iluminación inadecuada, exposición a radiaciones, instalaciones eléctricas inadecuadas.
- Riesgos químicos, por ejemplo la exposición a vapores de los solventes, humo de combustión y gases.
- Riesgos biológicos, como hongos y bacterias.
- Riesgos psicosociales como bajos ingresos económicos, la falta de incentivos y motivación.
- Riesgos ergonómicos tales como puesto de trabajo incomodo, posición corporal forzada, movimiento repetitivo al operar máquinas, hacinamiento.

- Riesgo Fundamental: incluye las pérdidas que son impersonales en origen y consecuencia. La mayor parte son causados por fenómenos económicos, sociales que pueden afectar a parte de una organización.
- Riesgo Particular: generalmente son pérdidas que surgen de eventos individuales, antes que surjan de un grupo completo tales como desempleo, el incendio de una casa, el robo a una persona, son todos riesgos fundamentales ya que son particulares.
- Riesgos específicos: como el grado de pérdidas esperadas u ocurrencias para un caso particular.
- Elementos de riesgo: la población, edificios u obras civiles dentro de la estructura e infraestructura.
- Riesgo total: es el número de pérdidas tanto humanas como daño a la propiedad dentro de la actividad económica y ocurrencia al desastre[23].

5.3. ESTADO ACTUAL DE LA EMPRESA AGESAGRO S.A.S

5.3.1 INTRODUCCIÓN. Para conocer estado actual de la empresa se revisa desde su formación hasta los servicios que presta, con el propósito de poder analizar la información que maneja y para fortalecerla con recomendaciones de integridad, confidencialidad y confiabilidad de la información.

[23] BENAVIDES, Mirian. SOLARTE, Francisco. (2012). Módulo de riesgos y control informático, (pp 19-20). Pasto, Colombia.

5.3.2 DESCRIPCIÓN DE LA EMPRESA

5.3.2.1 Historia. La empresa Asesoría y Gestiones Agropecuarias (AGESAGRO) se fundó en 29 de Mayo de 2009, los señores Juan Rodrigo Alvarado Moreno, Luis Humberto Lastra, Rafael Bonilla Ospina y Henry Rivas Escobar, su concepción desde sus inicios tiene como objetivo principal la gestión asesorías y servicios relacionados con las actividades agrícolas, pecuarias, agroindustriales, forestales y ambientales.

AGESAGRO S.A.S. es un equipo interdisciplinario con experiencia basada en la capacidad de trabajo de profesionales, los cuales suman más de 15 años apoyando integralmente el acceso a los créditos en el sector rural de nuestro país. Desarrollando con profesionalismo las actividades que demanda el sector productivo y de comercialización con valores agregados a través de programas de capacitación, consultorías, asesorías y auditorias que se ejecutan para el beneficio de los empresarios agropecuarios.

5.3.2.2 Misión. Desarrollar con profesionalismo las actividades que demanda el sector productivo con valores agregados a través de programas de capacitación, consultorías, asesorías y auditorias que se ejecutan para el beneficio de los empresarios agropecuarios y del sector financiero[24].

5.3.2.3 Visión. AGESAGRO S.A.S. en el 2015 se consolidará como una organización líder a nivel nacional en el sector agropecuario ofreciendo alternativas de planificación y monitoreo de proyectos de la mano de nuestros aliados financieros, con talento humano capacitado aplicando tecnologías en informática y comunicación. Integrando nuevos productos permanentemente a nuestro portafolio de servicios[25].

5.3.2.4 Ubicación geográfica. AGESAGRO S.A.S tiene como domicilio principal la ciudad de Ibagué, no obstante, está en capacidad de realizar un cubrimiento a nivel nacional. La empresa cuenta con asignación preferencial por parte de FINAGRO, adquiriendo una muestra a cubrir concentrada en un área geográfica cerca de la ciudad. AGESAGRO S.A.S es una empresa en crecimiento, esta asignación es una oportunidad, esto permite incurrir en menos costos de funcionamiento.

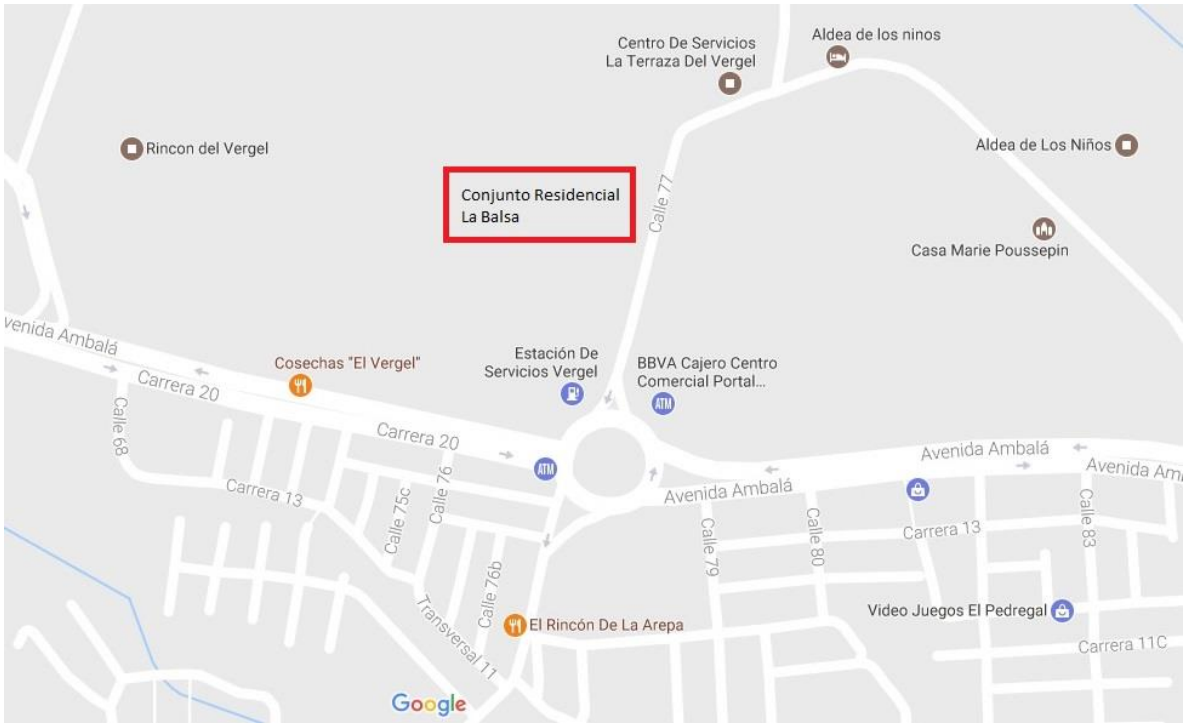
---

[24] AGESAGRO S.A.S. (2009). MISIÓN Y VISIÓN. Disponible en: https://biodomo2.wixsite.com/agesagro/mision-y-vision

[25] AGESAGRO S.A.S. (2009). MISIÓN Y VISIÓN. Disponible en: https://biodomo2.wixsite.com/agesagro/mision-y-vision

Dirección: Conjunto Residencial la Balsa Casa 18.

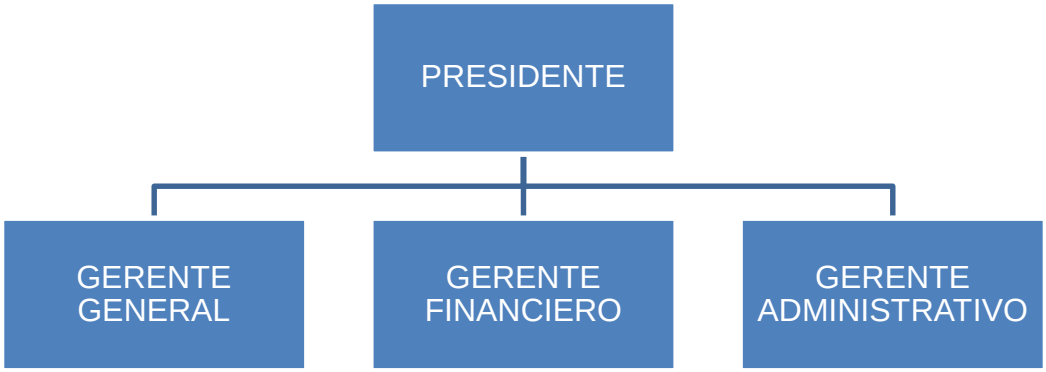
Figura 1. Ubicación Geográfica de AGESAGRO S.A.S



Fuente: Google Maps

5.3.3 Estructura Organizacional

Figura 2. Organigrama



Fuente: Autor

5.3.4. Control interno:

5.3.4.1 Funciones: A continuación vamos a describir las funciones de la Gerencia.

PRESIDENTE

a. Elegir a los miembros de la Junta Directiva con sus respectivos suplentes, y señalarles su remuneración;
b. Darse su propio reglamento;
c. Reformar los estatutos;
d. Ampliar, restringir o modificar el objeto de la sociedad;
e. Decretar el aumento de capital y la capitalización de utilidades;
f. Resolver sobre la disolución de la sociedad;
g. Decidir sobre el cambio de razón social, su transformación en otro tipo de sociedad, la fusión con otra u otras sociedades, la incorporación en ellos de otra u otras sociedades, o sobre las reformas que afecten las bases fundamentales del contrato, o que aumenten las cargas de los accionistas;
h. Reglamentar lo relativo al derecho de preferencia de las acciones que sean creadas; i. Decretar la enajenación o el gravamen de la totalidad de los bienes de la empresa, autorizado para ello al gerente;
j. Aprobar o improbar las cuentas, el balance y el estado de pérdidas y ganancias;
k. Decretar la distribución de utilidades, la cancelación de pérdidas y creación de reservas no previstas en la ley o en estos estatutos;
l. Remover libremente a cualquiera de sus empleados o funcionarios de la entidad, cuya designación le corresponda;
m. Decretar la compra de sus propias acciones con sujeción a la ley y a los presentes estatutos;
n. Autorizar la emisión de bonos industriales;
o. Estatuir y resolver sobre los asuntos que le correspondan como suprema autoridad directiva de la sociedad y que no hayan sido atribuidos a ninguna otra autoridad o persona

GERENTE GENERAL

1) Representar a la sociedad ante los accionistas, ante terceros y ante toda clase de autoridades de orden administrativo y jurisdiccional.
2) Ejecutar todos los actos u operaciones correspondientes al objeto social, de conformidad con lo previsto en las leyes y en estos estatutos.

3) Autorizar con su firma todos los documentos públicos o privados que deban otorgarse en desarrollo de las actividades sociales o en interés de la sociedad.
4) Presentar a la Asamblea de accionistas en sus reuniones ordinarias, un inventario y un balance de fin del ejercicio, junto con un informe escrito sobre la situación de la sociedad, un detalle completo de la cuenta de pérdidas y ganancias y un proyecto de distribución de utilidades obtenidas,
5) Nombrar y remover los empleados de la sociedad cuyo nombramiento y remoción le delegue a Junta Directiva.
6) Tomar todas las medidas que reclame la conservación de los bienes sociales. Vigilar la actividad de los empleados de la administración de la sociedad e impartirles las órdenes e instrucciones que exija la buena marcha de la compañía.
7) Convocar la Asamblea de Accionistas a reuniones extraordinarias cuando lo juzgue conveniente o necesario y hacer las convocatorias del caso cuando lo ordenen los estatutos o la Junta Directiva de la sociedad.
8) Convocar la Junta Directiva cuando lo considere necesario o conveniente y mantenerla informada del curso de los negocios sociales,
9) Cumplir las órdenes e instrucciones que le impartan la Asamblea de accionistas o la Junta Directiva, y. en particular, solicitar autorizaciones para los negocios que deben aprobar previamente la Asamblea o Junta Directiva según lo disponen las normas correspondientes del presente estatuto.
10) Cumplir o hacer que se cumplan oportunamente todos los requisitos o exigencias legales que se relacionen con el funcionamiento y actividades de la sociedad.

GERENTE FINANCIERO

BALANCES: El último día de cada mes, se producirá un balance de prueba pormenorizado de las cuentas de la compañía, que será presentado por el Gerente a la Junta Directiva.
INVENTARIO Y ESTADO DE RESULTADOS: El 31 de diciembre de cada año se verificarán los asientos contables correspondientes al balance de prueba de esa misma fecha, se cortarán las cuentas y se producirá el inventario general y el estado de resultados correspondiente al año fiscal, concluido en esa fecha. Para determinar los resultados definitivos de las operaciones realizadas, será necesario que se hayan apropiado previamente, de acuerdo con la ley, y las normas de contabilidad y con la reglamentación de la Junta Directiva las partidas necesarias para atender el deprecio, desvalorización y garantía del patrimonio social.
BALANCE GENERAL: Determinados los resultados finales del ejercicio se procederá a la elaboración del balance general al 3l de diciembre de cada año, el

cual se someterá a la aprobación de la Asamblea de Accionistas, junto con el estado de resultados del ejercicio.
RESERVA LEGAL: De las utilidades liquidas determinadas por los estados financieros se destinará un 10% para la formación e incremento de la reserva legal.
RESERVAS ESPECIALES. La Asamblea de Accionistas podrá crear, si lo estima conveniente, cualquier clase de reservas, tomadas de las utilidades líquidas y una vez deducida la suma necesaria para la reserva legal, siempre que tengan una destinación especial y justificada conforme a la ley.
DIVIDENDOS: La Asamblea de accionistas, una vez aprobado el balance, el estado de resultados y destinadas las sumas correspondientes a la reserva legal y a la que ella misma estime conveniente. Fijará el monto del dividendo.
APROBACIÓN DE ESTADOS FINANCIEROS. Tanto los estados financieros de propósito general o especial, como los informes de gestión y demás cuentas sociales deberán ser presentadas por el representante legal a consideración de la asamblea de accionistas para su aprobación.

GERENTE FINANCIERO

BALANCES: El último día de cada mes, se producirá un balance de prueba pormenorizado de las cuentas de la compañía, que será presentado por el Gerente a la Junta Directiva.
INVENTARIO Y ESTADO DE RESULTADOS: El 31 de diciembre de cada año se verificarán los asientos contables correspondientes al balance de prueba de esa misma fecha, se cortarán las cuentas y se producirá el inventario general y el estado de resultados correspondiente al año fiscal, concluido en esa fecha. Para determinar los resultados definitivos de las operaciones realizadas, será necesario que se hayan apropiado previamente, de acuerdo con la ley, y las normas de contabilidad y con la reglamentación de la Junta Directiva las partidas necesarias para atender el deprecio, desvalorización y garantía del patrimonio social.
BALANCE GENERAL: Determinados los resultados finales del ejercicio se procederá a la elaboración del balance general al 3l de diciembre de cada año, el cual se someterá a la aprobación de la Asamblea de Accionistas, junto con el estado de resultados del ejercicio.
RESERVA LEGAL: De las utilidades liquidas determinadas por los estados financieros se destinará un 10% para la formación e incremento de la reserva legal.
RESERVAS ESPECIALES. La Asamblea de Accionistas podrá crear, si lo estima conveniente, cualquier clase de reservas, tomadas de las utilidades líquidas y una

vez deducida la suma necesaria para la reserva legal, siempre que tengan una destinación especial y justificada conforme a la ley.

DIVIDENDOS: La Asamblea de accionistas, una vez aprobado el balance, el estado de resultados y destinadas las sumas correspondientes a la reserva legal y a la que ella misma estime conveniente. Fijará el monto del dividendo.

APROBACIÓN DE ESTADOS FINANCIEROS. Tanto los estados financieros de propósito general o especial, como los informes de gestión y demás cuentas sociales deberán ser presentadas por el representante legal a consideración de la asamblea de accionistas para su aprobación.

GERENTE ADMINISTRATIVO

RESOLUCION DE CONFLICTOS SOCIETARIOS. Las diferencias que ocurran a los accionistas entre sí, o con la sociedad o sus administradores, en desarrollo del contrato social o del acto unilateral, incluidos la impugnación de determinaciones de asamblea o junta directiva con fundamento en cualquiera de las causas legales, se someterán a decisión arbitral o de amigables componedores.

UNANIMIDAD PARA LA MODIFICACION DE DISPOSICIONES ESTATUTARIAS. Las cláusulas consagradas en los estatutos conforme a lo previsto en los artículos 13. 14; 39 y 40 de la ley 1258 de2008 sólo podrán ser incluidas o modificadas mediante la determinación de los titulares del ciento por ciento (100%) de las acciones suscritas.

ABUSO DEL DERECHO. Los accionistas deberán ejercer el derecho de voto en el interés de la compañía. Se considerará abusivo el voto ejercido con el propósito de causar daño a la compañía o a otros accionistas o de obtener para si o para una tercera ventaja injustificada, así como aquel voto del que pueda resultar un perjuicio para la compañía o para los otros accionistas. Quien abuse de sus derechos de accionista en las determinaciones adoptadas en la asamblea, responderá por los daños que ocasione, sin perjuicio que la Superintendencia de Sociedades pueda deparar la nulidad absoluta de la determinación adoptada, por la ilicitud del objeto. La acción de nulidad absoluta y la de indemnización de perjuicios de la determinación respectiva podrán ejercerse tanto en los casos de abuso de mayoría, como en los de minoría y de paridad. El trámite correspondiente se adelantará ante la Superintendencia de Sociedades mediante el proceso verbal sumario.

ATRIBUCION DE FACULTADES JURISDICCIONALES. Las funciones jurisdiccionales a que se refieren los artículos 24, 40. 42 y 43. DE LA LEY 1258 DE 2008, serán ejercidas por la Superintendencia de Sociedades, con fundamento en lo previsto en el artículo 116 de la Constitución Política de Colombia.

REMISION. En lo no previsto en los presentes estatutos, la sociedad se regirá por las disposiciones contenidas en la ley 1258 de 2008, por las normas legales que rigen a la sociedad anónima y, en su defecto, en cuanto no resulten contradictorias, por las disposiciones generales que rigen a las sociedades previstas en el Código de Comercio, así mismo, la sociedad estará sujeta a la inspección, vigilancia o control de La Superintendencia de Sociedades, según las normas legales pertinentes.

5.3.5 SISTEMAS DE INFORMACIÓN Los listados de visitas son enviados por FINAGRO por medio de la plataforma ATHENEA, luego se revisa la información de las visitas y se buscan los valores de los créditos en las bases de los Bancos en los cuales hayan realizado el crédito, se procede a realizar la visita de campo para dar el visto favorable o negativo del uso del dinero para el crédito realizado.

5.3.6 SERVICIOS QUE PRESTAN. Planificación de Proyectos Agropecuarios bajo las normas de FINAGRO: Se le facilita al empresario del sector rural, el desarrollo y estructuración de proyectos agropecuarios bajo las directrices de FINAGRO, lo cual permite adquirir créditos oportunos con los intermediarios financieros que garantizan el establecimiento y sostenimiento de sus negocios agropecuarios.

Control de Inversión: Prestando servicio en el acompañamiento y vigilancia a las inversiones ejecutadas en el sector agropecuario, para garantizar el éxito y rentabilidad de los proyectos desarrollados. Ayudando a los clientes a organizar rápidamente su información para la obtención de los subsidios estatales, como el Incentivo a la capitalización rural (ICR), el Certificado de Incentivo Forestal (CIF) y otros.

Avalúos de predios rurales y urbanos, muebles e inmuebles y maquinaria agrícola: Le ayudan a los productores agropecuarios a determinar el valor real de sus activos que vayan a constituir garantías reales ante los intermediarios financieros. Contando con los requerimientos y certificados que exige FEDELONJAS para el desarrollo de esta labor.

Asistencia Técnica Agropecuaria: Asesorando al productor agropecuario con asistencia técnica especializada cumpliendo con las exigencias del ministerio de agricultura y demás entes que regulan el desarrollo de las labores agropecuarias.

5.3.7 PROCEDIMIENTOS ACTUALES. Actualmente la empresa cuenta con mecanismos de protección de la información al momento de realizar la descarga de los listados ya que utilizan usuarios de autenticación, como al momento de realizar el cargue de las visitas que también requieres un ingreso con usuario y contraseña.

5.4 REFERENTES HISTORICOS

En el año 2013 se realiza el análisis de gestión de riesgos de la empresa "Pesquera e Industrial Bravito S.A." en el cual se identifican que no tiene medidas de seguridad guiados y documentados, por lo cual ese estudio será de gran beneficio para minimizar riesgos en el futuro. Gracias a la metodología MAGERIT donde se consiguió una serie de pasos estructurados para el análisis y gestión de riesgos, fase fundamental en este estudio ya se obtuvo resultados realistas del estado de riesgos actual e la empresa donde se supo escoger que medidas serán necesarias para mitigar el riesgo, utilizaron la herramienta PILAR 5.2.9 y por medio de este software se supo de manera directa que mecanismos de seguridad tienen que implementar en la empresa, y después de realizar el proyecto se obtuvo un documento encaminado a la seguridad y será el punto de partida para creación de normativas de seguridad para los recursos informáticos y para los empleados que laboran en la empresa[26].

En el año 2012 en Ecuador se realiza el Análisis y Gestión de Riesgos de los Sistemas de la Cooperativa de Ahorro y Crédito Jardín Azuayo utilizando la metodología MAGERIT para contribuir a que la institución posea un conocimiento claro sobe los riesgos que puedan presentarse en sus sistemas de información, junto a los objetivos, estrategia y políticas de la organización, las actividades de gestión de riesgos permitiendo elaborar un plan de seguridad que implantado y operando satisfaga los objetivos propuestos con el nivel de riesgo que acepta la dirección[27].

En la ciudad de Ibagué ya se puede ver que se implementa el SGSI y políticas de seguridad. Las políticas de seguridad definidas en el presente documento están dirigidas a los servidores públicos de la Alcaldía de Ibagué, las cuales serán de

---

[26] GAONA, Karina del Rocio. APLICACION DE LA METODOLOGIA MAGERIT PARA EL ANALISIS Y GESTION DE RIESGOS DE LA SEGURIDD DE LA INFORMACIÓN APLICADO A AL EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A. EN LA CIUDAD DE MACHALA. 2013. http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf [Consulta: Sábado, 12 de noviembre de 2016]

[27] Gomez, A.J., & Valverde, J.O. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO, UTILIZANDO LA METODOLOGÍA MAGERIT. (2011-2012), http://dspace.ucuenca.edu.ec/bitstream/123456789/1342/1/tcon640.pdf [Consulta: Sábado, 12 de noviembre de 2016]

obligatorio cumplimiento, a fin de proteger la información y otros activos informáticos de amenazas y vulnerabilidades y garantizar la integridad, confidencialidad y disponibilidad de la información. Con la definición de las políticas y estándares de seguridad informática, se busca establecer en el interior de la Alcaldía Municipal de Ibagué una cultura de calidad operando en una forma confiable[28].

[28] Alcaldía de Ibagué-Tolima. (2016). SGSI. Ibagué, Colombia. Recuperado el 09 de agosto de 2016 de: http://www.alcaldiadeibague.gov.co/portal/seccion/contenido/index.php?type=3&cnt=10

6. DISEÑO METODOLÓGICO

6.1 UNIDAD DE ANÁLISIS. AGESAGRO S.A.S

6.1.1 Población y muestra.

6.1.1.1 Población. Empleados que forman la empresa AGESAGRO S.A.S. Juan Rodrigo Alvarado Moreno, Luis Humberto Lastra, Rafael Bonilla Ospina y Henry Rivas Escobar. En el área de Gerencia.

6.1.1.2 Muestra. 100% de la población ya que representa la totalidad de la Gerencia.

6.1.2 Estudio metodológico. Investigación proyectiva. Este tipo de investigación, consiste en la elaboración de una propuesta, un plan, un programa o un modelo, como solución a un problema o necesidad de tipo práctico, ya sea de un grupo social, o de una institución, o de una región geográfica, en un área particular del conocimiento, a partir de un diagnóstico preciso de las necesidades del momento, los procesos explicativos o generadores involucrados y de las tendencias futuras, es decir, con base en los resultados de un proceso investigativo[29].

6.1.3. Marco legal
Ley Estatutaria 1273

“La cual determina el acceso abusivo a un sistema informático u obstaculiza ilegítimamente sistemas informáticos o redes de telecomunicación, la interceptación de datos informáticos, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte. Dentro de los daños informáticos se encuentran destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos. Y en la parte de software Quien produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas

[29] HURTADO DE BECERRA, Jacqueline. 2008. Metodología de la investigación, una comprensión holística. Caracas Venezuela, Edit. Sypal.

de computación, como también uso de software malicioso o violación de datos personales" [30].

Ley Estatutaria 1341

"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones". Se protegen los derechos de los usuarios, velando por la calidad, eficiencia y adecuada provisión de los servicios, promover el acceso a las Tecnologías de la Información y las Comunicaciones, promover el desarrollo de contenidos y aplicaciones, oferta de mayores capacidades en la conexión, la libre y leal competencia, el uso eficiente de infraestructura, e igualdad de oportunidad en el acceso[31].

Ley Estatutaria 527

"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones". Definiciones de mensaje de datos, comercio electrónico, firma digital, entidad de certificación, intercambio de datos y sistema de información[32].

Ley Estatutaria 1266

"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" [33].

---

[30] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (Enero 05 de 2009). Diario Oficial 47.223 del 05 de enero de 2009. p. 1-4.
[31] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341. (Julio 30 de 2009). Diario Oficial 47.426 del 30 de julio de 2009. p. 1-15.
[32] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (Agosto 18 de 1999). Diario Oficial 43.673 del 21 de agosto de 1999. p. 1-15.
[33] COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. P. 1-15.

7. IDENTIFICACIÓN DE ACTIVOS TECNOLOGICOS

Al realizar la identificación der los activos podemos lograr un mejor criterio para identificar las amenazas potenciales como salvaguardas para proteger esos activos.

7.1 CLASIFICACIÓN DE LA INFORMACIÓN

La siguiente clasificación es determinada de acuerdo a la metodología MAGERIT en el libro II – Catálogo de elementos de la página 8 a 13.

7.1.1 [D] Datos / Información La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos[34].

7.1.2 [K] Claves criptográficas. La criptografía se emplea para proteger el secreto o autenticar a las partes. Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos[35].

7.1.3 [S] Servicios. Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema[36].

7.1.4 [SW] Software. – Aplicaciones informáticas Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios[37].

---

[34] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[35] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[36] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[37] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.

7.1.5 [HW] Equipamiento informático (hardware). Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos[38].

7.1.6 [COM] Redes de Comunicaciones. Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro[39].

7.1.7 [Media] Soportes de información. En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo[40].

7.1.8 [AUX] Equipamiento auxiliar. En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos[41].

7.1.9 [L] Instalaciones. En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones[42].

7.1.10 [P] Personal. En este epígrafe aparecen las personas relacionadas con los sistemas de información[43].

---

[38] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[39] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[40] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[41] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[42] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[43] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.

7.2 ACTIVOS DE LA INFORMACIÓN

Hacer un inventario de servicios de red asociándolos con los respectivos activos u equipamiento de hardware y software, vinculando si son propios de empresa o son de terceros (proveedores, outsorcing).

Celulares: lumia 820 4 unidades. Equipos telefónicos con sistema operativo Windows phone mango.
Portátiles: Lenovo z40 1 unidad, Propio

Tabla 1. Portátil z40

Especificaciones técnicas	
Procesador	• Intel® Core™ i7- 4500U 4° generación (3 GHz 1600 MHz 4MB) • Intel® Core™ i5- 4200U 4° generación (2,60 GHz 1600 MHz 3MB)
Sistema operativo	Windows 8,1 64
Gráficos	Hasta gráficos NVIDIA® GeForce® GT 820M 2GB
Memoria	Hasta 8 GB de memoria PC3-12800 DDR3L SDRAM 1600 MHz
Cámara Web	Cámara HD 720p (1M píxel)
Almacenamiento	SSHD de hasta 1 TB + unidad de estado sólido de 8 GB
Audio	Parlantes estéreo con Dolby® Home Theater®
Batería	Hasta 5 horas
Pantalla	• Pantalla HD de 14” (1366 x 768) • Pantalla ancha de 16:9
Unidad óptica	Unidad óptica integrada (DVD-R)
DIMENSIONES (A X P X A)	13,74" x 9,6" x 0,97"
Peso	2.10 Kg
Conexión Inalámbrica	• Bluetooth® 4.0 • Lenovo BGN Wireless • LAN 10 / 100 / 1000M
Puertos	• 1 puertos USB 3,0 • 2 puertos USB 2.0 • Conector para combo de audio • Salida HDMI • Lector de tarjetas 2 en 1 (SD/MMC)

Fuente: Autor

Portátil hp pavillion dv4 propio

Tabla 2. Portátil hp pavillion dv4

Especificaciones Técnicas	
Sistema Operativo	El sistema operativo es responsable por la administración de los recursos de su computador y permite que el software y el hardware trabajen juntos. • Windows Vista Home Basic
Webcam	Haz conferencias en vivo de video o audio con tus familiares y amigos. • Web Cam y micrófono integrado. Cámara VGA
Procesador	Un procesador más rápido le permite terminar sus tareas en menos tiempo. • AMD Athlon 64 X2 Dual-Core Mobile con tecnología QL-62 (2.0 GHz, 1MB L2 Cache)
Caché	Aumente el rendimiento de su equipo. • 1 MB Cache L2
Memoria	Más memoria le permite ejecutar más programas de software al mismo tiempo. Nota: Aquellos sistemas que no incluyen tarjeta de video, comparten la memoria principal con la memoria de video. • 2048MB 800MHz DDR2 (1 Dimm), expandible a 8GB
Pantalla	Una pantalla clara y brillante donde quiera que la lleve. El tamaño de la pantalla esta dado en pulgadas. • Pantalla de 14.1" TFT/WXGA Widescreen con tecnología BrightView High-Definition, resolución 1280 x 800
Gráficas	El controlador de gráficas acelera el procesamiento de las imágenes, ofreciéndole una alta calidad y mejor nitidez. • ATI Mobility Radeon HD 3200
Disco Duro	Discos duros le dan el espacio de almacenamiento para sus datos y programas. • Disco Duro de 250GB SATA (5400 rpm)
Disco Óptico	Obtenga lo máximo de la multimedia con un disco óptico en su computadora portátil. • Super Multi DVD±RW Drive con soporte para doble capa y lightScribe
Audio	Viva la experiencia del sonido en el Internet y en los más populares programas de hoy. • Altec Lansing con Audio Playback SRS Premium Sound
Interface	Permite la conexión de los periféricos. • 3 USB 2.0 (3er combo USB + eSATA); 2 s/audífono; 1 /micrófono; 1 puerto VGA, 1 RJ-11, 1 RJ-45, 1 Expansión, 1 Consumer IR, 1 HDMI

Tabla 3. (Continuación)

Especificaciones Técnicas	
Medio Digital	Para utilizar la tarjeta de memoria de otro dispositivo (como una cámara digital o un MP3) para acceder a fotos, películas, archivos, música, etc. • Lector 5 en 1 de memoria digital Secure Digital, MultiMedia, Memory Stick, Memory Stick Pro y xD
Conectividad	Permite conectar su notebook a Internet y ambientes de red. • Conexión de red 10/100 BASE-T Ethernet LAN
Módem	Conéctese al mundo a gran velocidad. • Módem de 56K de alta velocidad
Bluetooth	Dispositivo de conexión inalámbrica. • Conexión de Bluetooth integrada
Conexión inalámbrica	Conexión inalámbrica. • 802.11b/g
Ranuras de expansión	Ranuras de expansión. • Una ranura para ExpressCard/54, incluye soporte para ExpressCard/34
Batería	Mantenga su sistema encendido, aun cuando este desconectado del toma de corriente. • Batería de Lithium-ion de 6 células (47Whr)
Adaptador de corriente alterna	Conecte su notebook a la red eléctrica para recargar su batería o trabajar de esta forma según su conveniencia. • Adaptador de corriente alterna de 65W
Teclado	Teclado Integrado. • Teclado compatible 101 teclas
Mouse	Use su computadora de la forma más fácil. • Touch Pad integrado con boton de encendido/apagado y pad dedicado de desplazamiento vertical
Controles	Controles de encendido, media, musica, red inalámbrica y DVD. • 1 par de audífonos Stereo, control remoto (Versión Express Card), 1 botón Quick Launch
Características de Seguridad	Compaq le brinda seguridad adicional y reforzada para mantener la calidad de su trabajo y data. • Cerradura Kensington MicroSaver (acepta candados de seguridad de terceras marcas), password de encendido, lector de Huellas Digitales
Mantenimiento y seguridad	Programas de software para la seguridad y mantenimiento de su PC. • Symantec Norton Security 2009 (60 días); Adobe Acrobat Reader; HP Ayuda y Soporte; HP Pc Recovery (SoftThinks); Digital Persona

Tabla 3. (Continuación)

Especificaciones Técnicas	
Software	Software pre-instalado para que su experiencia sea de lo mejor. • Microsoft Office 2007 Home and Student Edition (60 días de prueba)
Software de entretenimiento	Juegos, fotografía, edición de películas y más. • Media Smart 2.0,Cyberlink DVD Suite Deluxe, HP Games Powered by Wild Tangent con Spore Creature Creator, Muvee Reveal Basic (20 días de prueba)
Software de productividad	Aplicaciones y software de productividad. • Microsoft Works 9.0
Dimensiones y Peso	Las dimensiones estan dadas en centímetros (alto, ancho y profundidad) y el peso en kilogramos. • 24.0 x 33.4 x 3,4-4.0 (cm). Peso: 2.2 kg

Fuente: Autor

Samsung mini np-n150 propio

Tabla 3. Samsung mini np-n 150

Especificaciones Técnicas	
Sistema Operativo	• Windows 7 Starter (32 Bits)
Procesador	• Intel Atom N450 (1.66 GHz, 667 MHz, 512 KB)
Chipset	• Intel NM10 Express Chipset
Memoria RAM	• 1GB, DDR2
Disco Duro	• 160 GB, SATA (5400 rpm)
Pantalla	• 10.1" WSVGA (1024 x 600), Retroiluminación LED
Video	• Intel Graphics Media Accelerator 3150
Audio	• Audio de Alta Definición Realtek - 2 x Bocinas de 1.5 Watts c/u - Micrófono integrado - Efecto de sonido SRS TruSurround XT
Red	• Fast Ethernet 10/100 LAN
Red Inalámbrica	• 802.11 b/g/n
Cámara Web	• Digital LiveCam (SCB-0340N). Integrada a la Pantalla
Lector de Memorias	• 3-en-1 (SD, SDHC, MMC)
Puertos	• 1 x VGA • 3 x USB 2.0 (1 x USB recargable) • 1 x Red (RJ-45) • 1 x Entrada para Micrófono • 1 x Entrada para Audífonos • 1 x Alimentación de Energía (DC-In)

Tabla 3. (Continuación)

Especificaciones Técnicas	
Seguridad	• 1 x Ranura Kensington
Adaptador de Corriente	• 40 Watts
Batería	• 6 celdas de Ion-Litio
Dimensiones	• 264 x 188 x 25.3 ~ 34.7 mm (Ancho x Profundo x Alto)
Peso	• 1.24 Kg
Fuente: Autor	

Fuente: Autor

Software: Sistema operativo Windows 7, sistema operativo Windows 8, cada sistema operativo con su programa ofimático Office, Athenea encargado de recibir la información de las visitas que se encuentra en todos los equipos telefónicos.

7.3 CLASIFICACION DE LOS ACTIVOS DE ACUERDO A LOS CRITERIOS DE LA INFORMACIÓN

Tabla 4. Tipos de activo y descripción

Tipos de activos	Descripción
[D] Datos / información	Bases de datos del listado de visitar a realizar por FINAGRO, manual de usuario de la plataforma athenea, Contrato de los empleados de AGESAGRO S.A.S, Visitas realizadas por AGESAGRO S.A.S.
[SW]Software – Aplicaciones informáticas	Windows 7 SP1, Windows 8, aplicación athenea, programas ofimáticos como Office, sistema operativo Windows phone versión mango.
[HW] Equipamiento informático (Hardware)	Equipos celular lumia 820 4 unidades, portatiles Lenovo z40, hp pavillion dv4, Samsung mini np-n150. Equipo de escritorio clon.
[COM] Redes de comunicaciones	Modem movistar modelo modem mini BHS, modem claro Thomson digital/Broadband, Claro Ubee 2110, modem claro Thomson dwg849. Conectividad a internet movil por medio de los proveedores, claro y movistar.
[Media] Soportes de información	Tarjetas de memoria, discos, memorias usb, material impreso.
Tipos de activos	Descripción
[AUX]Equipamiento auxiliar	UPS poweback 1000.
[L] Instalaciones	Cableado de red y servicio wifi, instalaciones eléctricas de los hogares de los usuarios.
[P] Personal	Ingenieros Agrónomos: Juan Rodrigo Alvarado Moreno, Luis Humberto Lastra, Rafael Bonilla Ospina, Henry Rivas Escobar

Fuente: Autor

7.4 DIMENSIONES DE VALORACIÓN

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión[44].

7.4.1 De acuerdo al impacto

7.4.1.1Criterios de valoración. Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

MB: muy bajo
B: bajo
M: medio
A: alto
MA: muy alto

Tabla 5. Criterios de valoración de acuerdo al 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: Tomado del Libro III Magerit versión 3 p.6

7.4.1.2 Valoración de los activos. En la siguiente tabla se va a ofrecer una calificación cualitativa de los activos de acuerdo al impacto.

[44] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.

Tabla 6. Valoración de activos de acuerdo al impacto

ACTIVO	AMENAZA	IMPACTO
ACTIVO DE LA INFORMACION	Corrupción de la información	A
	Destrucción de información	A
	Interceptación de información (escucha)	A
	Robo	A
HARDWARE	Desastres naturales	A
	Corte del suministro eléctrico	B
	Condiciones inadecuadas de temperatura o humedad	M
	Pérdida de equipos	A
	Robo	A
	Errores de mantenimiento / actualización de equipos (hardware)	M
	Degradación de los soportes de almacenamiento de la información	M
	Errores de configuración	M
SOFTWARE	Caída del sistema por sobrecarga	B
	Fallo de servicios de comunicaciones	B
	Difusión de software dañino	M
	Errores de mantenimiento / actualización de programas (software)	M
	Errores de configuración	A
ACTIVO	AMENAZA	IMPACTO
REDES	Errores de configuración	A
EQUIPAMIENTO AUXILIAR	Corte del suministro eléctrico	B
	Robo	M
INSTALACION	Configuraciones predeterminadas de la red	B
SERVICIOS	Fallo de servicios de comunicaciones	B
	Denegación de servicio	B
PERSONAL	Introducción de falsa información	M
	Indisponibilidad del personal	M
	Abuso de privilegios de acceso	M
	Acceso no autorizado	M
	Errores de los usuarios	M
	Errores del administrador	M
	Extorsión	A
	Ingeniería social	A

Fuente: Autor

7.4.2 De acuerdo a las dimensiones de seguridad. Dentro de la dimensión de seguridad se definen la disponibilidad, integridad de los datos, confidencialidad de la información, autenticidad y trazabilidad.

7.4.2.1 Criterios de valoración

Tabla 7. Criterios de valoración de activos

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

Fuente: Tomado del Libro II Magerit versión 3 p.19

[D] Disponibilidad Propiedad o característica de los activos: consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008][45]

[I] Integridad de los datos Propiedad o característica: consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004][46]

[C] Confidencialidad de la información: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007][47]

[45] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[46] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.
[47] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.

[A] Autenticidad Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008][48]

[T] Trazabilidad Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008][49]

7.4.2.2 Valoración de los activos

Tabla 8. Valoración de las 5 dimensiones de seguridad

Activos esenciales	[D]	[I]	[C]	[A]	[T]
Expedientes administrativos		[6]	[6]	[6]	[5]
Atención presencial	[6]			[7]	[7]
Tramitación remota	[3]			[7]	[6]
Fuente: Autor					

[48] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.

[49] AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.

8. ANALISIS DE AMENAZAS CON METODOLOGIA MAGERIT

La siguiente información es realizada determinando los tipos de activos que pueden ser afectados por los diversos tipos de amenazas, y una descripción para cada tipo de amenaza hacia la empresa.

8.1 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

AMENAZAS[50]

[N]Desastres naturales
Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

[N.1]Fuego
Tipos de activos: Equipos informáticos, soportes de información, equipos auxiliares, instalaciones
Descripción: No se encuentran extintores en la oficina o lugares de trabajo y posibilidad que un incendio acabe con los recursos del sistema como documentación de la empresa.

[N.2]Daños por agua
Tipos de activos: Equipos informáticos, soportes de información, equipos auxiliares, instalaciones
Descripción: La posibilidad que una inundación acabe con los recursos del sistema, es baja porque la oficina y lugar de trabajo no se encuentran en la primera planta.

[N.*] Desastres naturales
Tipos de activos: Equipos informáticos, soportes de información, equipos auxiliares, instalaciones
Descripción: Se producen sin intervención humana como son el rayo, tormenta eléctrica, terremoto, avalancha, corrimiento de tierras, actualmente no cuenta con compartimentos de seguridad para la información archivada.

[I] De origen Industrial
Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada

---

[50] AMUTIO, Miguel. CANDAU, Javier. MAÑAS, José. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*, (pp 25-47). España, Madrid.

[I.5] Avería de origen físico o lógico
Tipos de activos: Aplicaciones (software), equipos informáticos (hardware), soportes de información, equipamiento auxiliar.
Descripción: Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema, los equipos de equipo celular instalan aplicaciones adicionales sin ninguna asesoría y algunos equipos portátiles son usados por la familia que tienen completo manejo de instalación de programas.

[I.6] Corte del suministro eléctrico
Tipos de activos: Equipos informáticos, soportes de información (electrónicos), equipamiento auxiliar.
Descripción: Cese de la alimentación de potencia, solo se cuenta con una fuente de respaldo de energía.

[I.7] Condiciones inadecuadas de temperatura o humedad
Tipos de activos: Equipos informáticos, soportes de información, equipamiento auxiliar.
Descripción: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad. , los equipos se encuentran a temperatura ambiente, y no hay algún tipo de protección adicional para evitar las condiciones naturales, los equipos celulares reciben sin ningún tipo de protección el ambiente de las zonas a las cuales tienen que hacer las visitas.

[I.8] Fallo de servicios de comunicaciones
Tipos de activos: Redes de comunicaciones
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente, en algunas zonas la señal del proveedor de telefonía celular no tiene cobertura.

[I.10] Degradación de los soportes de almacenamiento de la información
Tipos de activos: Soportes de información
Descripción: como consecuencia del paso del tiempo, no hay ninguna forma de protección a este tipo de degradación.

[I.11] Emanaciones electromagnéticas
Tipos de activos: Equipos informáticos (hardware), media, equipamiento auxiliar, instalaciones
Descripción: hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser

interceptadas por otros equipos (receptores de radio) derivándose una fuga de información, no hay ninguna forma de aislamiento a las ondas de radio o dispositivos electrónicos, y los equipos de telefonía celular se mantienen cerca de los funcionarios.

[E] Errores y fallos no intencionados
Fallos no intencionales causados por las personas.
[E.1] Errores de los usuarios
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), soportes de información.
Descripción: equivocaciones de las personas cuando usan los servicios, datos, etc. Se han realizado en ocasiones el ingreso de datos erróneos al momento de ingresar la información de la visita, pero esta se puede volver a ingresar si se percatan del error.

[E.2] Errores del administrador
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones, soportes de información.
Descripción: Equivocaciones de personas con responsabilidades de instalación y operación. En el momento no se han obtenido errores al momento de manejar la plataforma Athenea.

[E.3] Errores de monitorización (log)
Tipos de activos: Registros de actividad
Descripción: Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos. Los permisos a usuarios en la plataforma Athenea no han permitido hasta el momento un rol distinto al destinado.

[E.4] Errores de configuración
Tipos de activos: Datos de configuración
Descripción: Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Los equipos de cómputo pueden estar mal configurados y no tienen algún tipo de configuración establecida para evitar pérdidas de información.

[E.8] Difusión de software dañino
Tipos de activos: Aplicaciones (software)
Descripción: propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. Los equipos, aunque cuentan con antivirus, no tienen alguna limitación a la instalación de programas que puedan contener software malicioso.

[E.15] Alteración accidental de la información
Tipos de activos: datos / información, claves criptográficas, servicios, aplicaciones, comunicaciones (tránsito), soportes de información, instalaciones.
Descripción: alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. Los usuarios de la plataforma Athenea solo pueden ingresar información sobre la visita realizada.

[E.18] Destrucción de información
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones, comunicaciones (tránsito), soportes de información, instalaciones
Descripción: pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas. No hay algún tipo de soporte a la información guardada en los equipos de cómputo como a los equipos de telefonía.

[E.19] Fugas de información
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones, comunicaciones (tránsito), soportes de información, instalaciones, personal (revelación).
Descripción: revelación por indiscreción. No se cuenta con algún tipo de manual de seguridad de información.

[E.20] Vulnerabilidades de los programas (software)
Tipos de activos: Aplicaciones (software)
Descripción: defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario, pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar. Hasta el momento en la plataforma Athenea no se han encontrado problemas de vulnerabilidad, pero los equipos de cómputo o celular son vulnerables a violación de la información.

[E.21] Errores de mantenimiento / actualización de programas (software)
Tipos de activos: aplicaciones (software)
Descripción: defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante. La actualización de la plataforma Athenea es realizada en las oficinas de Bogotá de soporte técnico, pero las actualizaciones de sistema operativo se realizan automáticamente y de igual forma el firmware de los equipos telefónicos.

[E.23] Errores de mantenimiento / actualización de equipos (hardware)
Tipos de activos: Equipos informáticos (hardware), soportes electrónicos, equipamiento auxiliar
Descripción: defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

Hasta el momento no se han realizado las modificaciones de hardware de ninguno de los equipos.

[E.24] Caída del sistema por agotamiento de recursos
Tipos de activos: Servicios, equipos informáticos (hardware), redes de comunicaciones
Descripción: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Frente a la plataforma no ha habido problema de caída del sistema por carga de trabajo.

[E.25] Robo
Tipos de activos: equipos informáticos (hardware), soportes de información, equipamiento auxiliar
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información. Todos los equipos cuentan con contraseñas, pero la información no se encuentra encriptada, y la información en físico como papelería no está protegida.

[E.28] Indisponibilidad del personal
Tipos de activos: Personal interno
Descripción: ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, inconformidad laboral. Muchos de los lugares de visita se encuentran en lugares de zona roja, y al momento de recibir las visitas ya se tiene conocimiento de esta situación.

[A] Ataques intencionados
Fallos deliberados causados por las personas.
La numeración no es consecutiva para coordinarla con los errores no intencionados, muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.
[A.3] Manipulación de los registros de actividad (log)
Tipos de activos: Registros de actividad. Actualmente no se sabe si hay un manejo de log en la plataforma Athenea ya que es un servicio externo a la empresa.

[A.4] Manipulación de la configuración
Tipos de activos: Registros de actividad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc. Los manejos de privilegios de los usuarios pueden ser realizados en los equipos de cómputo como equipos de telefonía móvil.

[A.5] Suplantación de la identidad del usuario
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), redes de comunicaciones
Descripción: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente. Actualmente no hay personal contratado temporalmente, y para poder tener acceso a la plataforma, se debe acceder primero a la contraseña del dispositivo móvil y luego al ingresar al teléfono móvil deben ingresar otro usuario y contraseña.

[A.6] Abuso de privilegios de acceso
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones
Descripción: cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas. Los permisos de usuarios no tienen más privilegios para modificar otra información sensible.

[A.7] Uso no previsto
Tipos de activos: Servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc. Los equipos de cómputo como teléfonos también son de uso personal, por lo tanto, albergan información ajena a las visitas.

[A.8] Difusión de software dañino
Tipos de activos: aplicaciones (software)
Descripción: propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. No hay programas instalados o no se tiene protección frente a la instalación de alguna aplicación que pueda tener un spyware.

[A.11] Acceso no autorizado
Tipos de activos: Datos / información, claves criptográficas, servicios, aplicaciones (software), equipos informáticos (hardware), redes de comunicaciones, soportes de información, equipamiento auxiliar, instalaciones
Descripción: el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización. Para poder ingresar a los recursos del sistema debe tener acceso a dos sistemas de información independientes para poder lograr la información, el sistema operativo y el usuario y contraseña de la plataforma

Athenea, pero de tener usuario y contraseña de Athenea solo podría modificar la información de la visita.

[A.14] Interceptación de información (escucha)
Tipos de activos: Redes de comunicaciones
Descripción: el atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada. Se puede llegar a tener información si se llega a hacer uso de las redes WIFI que no sean de plena confianza.

[A.15] Modificación deliberada de la información
Tipos de activos: Datos / información, claves criptográficas, servicios (acceso), aplicaciones (SW), comunicaciones (tránsito), soportes de información, instalaciones.
Descripción: alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Se deben elaborar medios de protección.

[A.18] Destrucción de información
Tipos de activos: Datos / información, claves criptográficas, servicios (acceso), aplicaciones, soportes de información, instalaciones
Descripción: eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Se pueden llegar a instalar en los equipos aplicaciones que pueden llegar a destruir la información ya que son también de uso personal.

[A.19] Revelación de información
Tipos de activos: datos / información, claves criptográficas, servicios (acceso), aplicaciones, comunicaciones (tránsito), soportes de información, instalaciones
Descripción: revelación de información. Se puede llegar a revelar información si se instalan spyware y no hay mecanismos para evitarlos.

[A.22] Manipulación de programas
Tipos de activos: aplicaciones (software)
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. La plataforma Athenea no puede ser modificada por terceros, pero el demás programa no tiene control.

[A.23] Manipulación de los equipos
Tipos de activos: Equipos, soportes de información, equipamiento auxiliar
Descripción: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza. Los equipos no se encuentran inventariados o estipulados para no realizar un cambio en el hardware.

[A.24] Denegación de servicio
Tipos de activos: Servicios, equipos informáticos (hardware), redes de comunicaciones.
Descripción: La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada. Los servidores no han presentado problemas de sobrecarga, pero los demás equipos pueden sufrir la denegación del servicio.

[A.25] Robo
Tipos de activos: Equipos informáticos (hardware), soportes de información, equipamiento auxiliar
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.
El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales.
El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.
En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.

[A.29] Extorsión
Tipos de activos: Personal interno
Descripción: Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido. No hay un manual o mecanismo de prevención frente a casos de extorsión.

[A.30] Ingeniería social (picaresca)
Tipos de activos: Personal interno
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero. Se deben realizar manuales para evitar caer en ingeniería social.

Posibles vulnerabilidades en la empresa: Los ordenadores pueden no tener actualizado el antivirus, o pueden contener spyware, No todos los equipos cuentan con sistemas de alimentación ininterrumpida, la falta de un área especializada en el área de sistemas, solo teniendo soporte sobre la aplicación Athenea por parte de FINAGRO, los equipos como los equipos de cómputo portátiles son usados por familiares, los cuales pueden infectar los computadores, falta un mayor conocimiento de parte de los usuarios sobre la seguridad informática, Se imprimen los documentos de las visitas las cuales pueden ser obtenidas por terceros, en el momento que pueda existir un robo de los equipos tanto de computo como telefónicos se pierde la información sin tener un sistema de respaldo.

El siguiente análisis de riesgo es realizado por medio de la versión Magerit.

8.1.1 Criterios de evaluación. Los criterios de evaluación van a ser determinados de acuerdo a su valor los cuales son:

MB: muy bajo
B: bajo
M: medio
A: alto
MA: muy alto

8.1.2 Evaluación de las amenazas a los activos

Tabla 9. Evaluación de las amenazas a los activos

ACTIVO	AMENAZA	PROBABILIDAD
ACTIVO DE LA INFORMACION	Corrupción de la información	B
	Destrucción de información	B
	Interceptación de información (escucha)	B
	Robo	B
HARDWARE	Desastres naturales	MB
	Corte del suministro eléctrico	B
	Condiciones inadecuadas de temperatura o humedad	B
	Pérdida de equipos	B
	Robo	B
	Errores de mantenimiento / actualización de equipos (hardware)	B
	Degradación de los soportes de almacenamiento de la información	B
	Errores de configuración	B
SOFTWARE	Caída del sistema por sobrecarga	B
	Fallo de servicios de comunicaciones	B
	Difusión de software dañino	B
	Errores de mantenimiento / actualización de programas (software)	B
	Errores de configuración	B

Tabla 9. (Continuación)

ACTIVO	AMENAZA	PROBABILIDAD
REDES	Errores de configuración	M
EQUIPAMIENTO AUXILIAR	Corte del suministro eléctrico	B
	Robo	B
INSTALACION	Configuraciones predeterminadas de la red	M
SERVICIOS	Fallo de servicios de comunicaciones	B
	Denegación de servicio	B
PERSONAL	Introducción de falsa información	B
	Indisponibilidad del personal	MB
	Abuso de privilegios de acceso	MB
	Acceso no autorizado	MB
	Errores de los usuarios	B
	Errores del administrador	MB
	Extorsión	B
	Ingeniería social	B

Fuente: Autor

ACTIVO DE LA INFORMACION: La corrupción de la información es baja por que la información se encuentra en dispositivos que poseen baterías de respaldo por si se llega a haber un corto en el fluido eléctrico, para ello se pueden apagar los equipos y evitar la pérdida de la información.

HARDWARE: El uso de los equipos es en recintos cerrados y de los equipos móviles son en las fincas los cuales se realizan las visitas junto con el cliente.

SOFTWARE: Los equipos de escritorio solo realizan funciones básicas de ofimática por lo cual no se estresan o sobrecargan, las configuraciones básicas no se modifican, pero si se deben verifica que se encuentren en configuraciones seguras.

REDES: Las configuraciones de las redes deben ser verificadas ya que se encuentran con la configuración básica sin ningún dispositivo que evite el acceso a la información con un firewall.

EQUIPAMIENTO AUXILIAR: Se encuentran ups y baterías de respaldo para los equipos móviles.
INSTALACION: Se deben verificar las configuraciones predeterminadas de red para configurar con más seguridad.

SERVICIOS: Son casos aislados los de fallo en los servicios con la plataforma Athenea, y los cuales prestan asesoría en caso de presentar fallo.

PERSONAL: Se deben realizar capacitaciones a todos los empleados sobre buenas prácticas de la información para así evitar que se pueda hacer mal uso de los sistemas de información y equipos tanto de escritorio como móviles.

8.2 RIESGO POTENCIAL

8.2.1 Criterios de Evaluación

Tabla 10. Criterios de aceptación de riesgo.

RANGO	DESCRIPCION
RIESGO <=M	La organización considera el riesgo poco reseñable
RIESGO>M	La organización considera el riesgo reseñable y debe proceder con su tratamiento

Fuente: Autor

8.2.2 Evaluación del riesgo potencial a los activos

Tabla 11. Análisis de riesgo

ANALISIS DE RIESGO				
ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
ACTIVO DE LA INFORMACION	Corrupción de la información	B	A	A
	Destrucción de información	B	A	A
	Interceptación de información (escucha)	B	A	A
	Robo	B	A	A
HARDWARE	Desastres naturales	MB	A	M
	Corte del suministro eléctrico	B	B	B
	Condiciones inadecuadas de temperatura o humedad	B	M	M
	Pérdida de equipos	B	A	A
	Robo	B	A	A
	Errores de mantenimiento / actualización de equipos (hardware)	B	M	M
	Degradación de los soportes de almacenamiento de la información	B	M	M
	Errores de configuración	B	M	M
SOFTWARE	Caída del sistema por sobrecarga	B	B	B
	Fallo de servicios de comunicaciones	B	B	B
	Difusión de software dañino	B	M	M
	Errores de mantenimiento / actualización de programas (software)	B	M	M
	Errores de configuración	B	A	A
REDES	Errores de configuración	M	A	A
EQUIPAMIENTO AUXILIAR	Corte del suministro eléctrico	B	B	B
	Robo	B	M	M
INSTALACION	Configuraciones predeterminadas de la red	M	B	B

Tabla 11. (Continuación)

ACTIVO	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
SERVICIOS	Fallo de servicios de comunicaciones	B	B	B
	Denegación de servicio	B	B	B
PERSONAL	Introducción de falsa información	B	M	M
	Indisponibilidad del personal	MB	M	B
	Abuso de privilegios de acceso	MB	M	B
	Acceso no autorizado	MB	M	B
	Errores de los usuarios	B	M	M
	Errores del administrador	MB	M	B
	Extorsión	B	A	A
	Ingeniería social	B	A	A

Fuente: Autor

9. APLICACIÓN DE CONTROLES

9.1 CONTROLES ANEXO A.

Los controles están basados en el Anexo A de la norma ISO 27001:2013 los cuales son fundamentales para poder gestionar un Sistema de Gestión de la Seguridad de la Información.

Tabla 12. Anexo A norma ISO 27001:2013

Núm.	Nombre	Selección /Excepción	Descripción / Justificación
1	Objeto y campo de aplicación		Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas		La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones		Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma		La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35
A.5	Políticas de seguridad de la información		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	X	Objetivo: Brindar orientación y apoyo 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.
A.5.1.1	Políticas para la seguridad de la información	X	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información	X	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
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 información	X	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes		Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades		Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	X	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección /Excepción	Descripción/Justificación
A.6.1.5	Seguridad de la información en la gestión de proyectos		Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2.1	Política para dispositivos móviles	X	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		Control: Se deberían 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.
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo	X	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los
A.7.1.1	Selección	X	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos
A.7.1.2	Términos y condiciones del empleo	X	Control: Los acuerdos contractuales con empleados y contratistas deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo		Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección	X	Control: La dirección debería 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
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	X	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	X	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados
A.7.3	Terminación o cambio de empleo		Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	X	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos	X	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	X	Control: Los activos mantenidos en el inventario deberían tener un propietario.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección /Excepción	Descripción/Justificación
A.8.1.3	Uso aceptable de los activos	X	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de
A.8.1.4	Devolución de activos	X	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a
A.8.2	Clasificación de la información	X	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	X	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información		Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información
A.8.2.3	Manejo de activos		Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de
A.8.3.1	Gestión de medios removibles	X	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación
A.8.3.2	Disposición de los medios		Control: Se debería disponer en forma segura de los medios cuando
A.8.3.3	Transferencia de medios físicos	X	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción
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	X	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red	X	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
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 debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	X	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de
A.9.2.3	Gestión de derechos de acceso privilegiado	X	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	X	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	X	Control: Los propietarios de los activos deberían revisar los derechos

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección /Excepción	Descripción/Justificación
A.9.3	Responsabilidades de los		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de
A.9.3.1	Uso de la información de autenticación secreta	X	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de
A.9.4	Control de acceso a sistemas y aplicaciones	X	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información	X	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la
A.9.4.2	Procedimiento de ingreso seguro	X	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso
A.9.4.3	Sistema de gestión de contraseñas	X	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	X	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas		Control: Se debería restringir el acceso a los códigos fuente de los programas.
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
A.10.1.1	Política sobre el uso de controles criptográficos	X	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de
A.10.1.2	Gestión de llaves	X	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
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	X	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada	X	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	X	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	X	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras		Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga		Control: Se deberían 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
A.11.2	Equipos	X	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección /Excepción	Descripción/Justificación
A.11.2.2	Servicios de suministro	X	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de
A.11.2.3	Seguridad del cableado	X	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar
A.11.2.4	Mantenimiento de equipos	X	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos		Control: Los equipos, información o software no se deberían retirar de
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		Control: Se deberían 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
A.11.2.7	Disposición segura o reutilización de equipos	X	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido
A.11.2.8	Equipos de usuario desatendidos	X	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia		Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política
A.12	Seguridad de 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 deberían documentar y poner a disposición de todos los usuarios que los
A.12.1.2	Gestión de cambios		Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad		Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	Protección contra códigos maliciosos		Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	X	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos
A.12.3	Copias de respaldo		Objetivo: Proteger contra la perdida de datos.
A.12.3.1	Respaldo de información	X	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección /Excepción	Descripción/Justificación
A.12.4.1	Registro de eventos		Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro		Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador		Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y
A.12.4.4	sincronización de relojes	X	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional		Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos	X	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica		Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas	X	Control: Se debería 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
A.12.6.2	Restricciones sobre la instalación de software	X	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información		Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas	X	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		Objetivo: Asegurar la protección de la información en las redes, y sus
A.13.1.1	Controles de redes	X	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	X	Control: Se deberían 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 servicios de red, ya sea que los servicios se presten internamente o se contraten
A.13.1.3	Separación en las redes		Control: Los grupos de servicios de información, usuarios y sistemas
A.13.2	Transferencia de información	X	Objetivo: Mantener la seguridad de la información transferida dentro
A.13.2.1	Políticas y procedimientos de transferencia de información	X	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de
A.13.2.2	Acuerdos sobre transferencia de información	X	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
A.13.2.3	Mensajería electrónica	X	Control: Se debería proteger adecuadamente la información incluida

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección	Descripción/Justificación
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	X	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización
A.14	Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1.1	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
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	X	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	X	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	X	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería 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.
A.14.2	Seguridad en los procesos de desarrollo y soporte		Objetivo: Asegurar de que la seguridad de la información esté 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 deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
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 deberían controlar mediante el uso de procedimientos formales de control de cambios.
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 deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software		Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los
A.14.2.5	Principios de construcción de sistemas seguros		Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de
A.14.2.6	Ambiente de desarrollo seguro		Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente		Control: La organización debería supervisar y hacer seguimiento de la
A.14.2.8	Pruebas de seguridad de sistemas		Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas		Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para
A.14.3	Datos de prueba		Objetivo: Asegurar la protección de los datos usados para pruebas.

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección	Descripción/Justificación
A.14.3.1	Protección de datos de prueba		Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15	Relación 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 las relaciones con proveedores	X	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 deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	X	Control: Se deberían 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.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	X	Control: Los acuerdos con proveedores deberían 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 y comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores		Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores
A.15.2.2	Gestión de cambios en los servicios de proveedores	X	Control: Se deberían 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 revaloración de los riesgos.
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	X	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación
A.16.1.1	Responsabilidad y procedimientos	X	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la
A.16.1.2	Reporte de eventos de seguridad de la información	X	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	X	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de
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 deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	X	Control: Se debería dar respuesta a los incidentes de seguridad de la

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Tabla 12. (Continuación)

Num	Nombre	Selección	Descripción/Justificación
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	X	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la
A.16.1.7	Recolección de evidencia	X	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
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 debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	X	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	X	Control: La organización debería 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.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	X	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
A.17.2	Redundancias	X	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.		Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
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
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	X	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	X	Control: Se deberían 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
A.18.1.3	Protección de registros	X	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales	X	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en
A.18.1.5	Reglamentación de controles criptográficos	X	Control: Se deberían usar controles criptográficos, en cumplimiento de

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

A.18.2	Revisiones de seguridad de la información	X	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	X	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 seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	X	Control: Los directores deberían 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
A.18.2.3	Revisión del cumplimiento técnico	X	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y

Fuente: Ministerio TIC. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

9.2. POLITICAS DE SEGURIDAD

Sobre la asignación y el uso de los recursos

Cada empleado que hace uso de un equipo de cómputo debe ingresar con usuario y contraseña.

Los empleados deben hacer uso adecuado de los equipos informáticos. Además, deberán informar a los demás sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, o en la plataforma para un adecuado seguimiento.

Todos los empleados tendrán una cuenta de correo electrónico, que les permita recibir y enviar información indispensable para sus actividades. En estas cuentas de correo, se deben evitar abrir correos electrónicos de los cuales no se conozca el remitente.

El uso de internet debe ser precavido cuando se realicen las actividades de trabajo que así lo requieran. Evitar descargar programas o aplicaciones de fuentes desconocidas.

Sobre la seguridad de la información

Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 1 minuto para evitar accesos no autorizados, al momento de retirarse del equipo deben bloquear la cuenta.

Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña, así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.

Los usuarios deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows, no se deben tener nombres de usuario o contraseña en papeles o visibles para evitar el acceso a los mismos.

Se deben asignar periódicamente nuevas contraseñas tanto para el acceso a las sesiones Windows como para el acceso a los programas.

Todos los archivos que se envíen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.

Los equipos que cuenten con puertos USB, CD o Discos duros externos. Deben contar con antivirus actualizados para lograr los siguientes 2 objetivos:

Evitar ataques de virus en los equipos y el servidor.
Evitar extracciones no autorizadas.

Los equipos autorizados para el uso de dispositivos de almacenamiento externos están bajo la responsabilidad del usuario para la entrada y salida de información.

A todos los equipos se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades.

Actualizar su base de firmas de virus (actualización de la lista de amenazas)
Búsqueda de virus (análisis del equipo)
Eliminación de virus si fue detectado.

En caso autorizado de memorias USB y discos, es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados.

Sobre el mantenimiento y buen uso de la infraestructura

Todos los equipos deberán presentar las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.

Los equipos de toda la agencia deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad.

Si se presentara una suspensión de servicio eléctrico, se tendrán que apagar todos los equipos de la empresa, para evitar perdida de la información.

Se debe verificar que las ups estén funcionando correctamente en caso de que no estén en óptimas condiciones, se deben cambiar para evitar la pérdida de información en los equipos por variaciones o fallas de energías.

Una vez al año se realizará una revisión en la red para detectar desperfectos y dar así mantenimiento a la empresa.

Periódicamente, por espacio de 4 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por personal capacitado.

Toda actividad elaborada por personal contratado de sistemas deberá de estar debidamente documentada para darle seguimiento.

9.3. RECOMENDACIONES

Inversión en herramientas antivirus para garantizar la seguridad de la información en todos los equipos para evitar la fuga de la misma.

Instalar en todos los equipos de cómputo sistemas de alimentación ininterrumpida, hacer uso de fuentes de poder alterna.

Asesoramiento de especialistas de información para evitar instalación de programas que puedan vulnerar información sensible.

Crear manuales de confidencialidad para evitar brindar información sensible sin percatarse.

Los equipos no deberían instalar programas adicionales que puedan llegar a instalar programas adicionales que puedan obtener información de los procesos o usuarios y contraseñas.

Mecanismos de seguridad en caso de robo de los equipos.

Mecanismos de seguridad en caso de extorsión.

Evitar al máximo la impresión de los documentos con información sensible y confidencialidad en el uso de los mismos.

Crear sistemas regulares de respaldo de la información.

Almacenar la información en lugares donde no puedan tener acceso personal no autorizado y que estén protegidos de factores ambientales que deterioren los mismos.

Capacitaciones permanentes en buenas prácticas y uso de los sistemas de información para así evitar que el eslabón más débil pueda incurrir en una falla para la empresa de forma inconsciente.

10. CONCLUSIONES

Se encuentran bastantes fallos de seguridad en la empresa y falta de capacitación en los empleados, los recursos y activos se deben de cuidar en almacenamiento y ambiente que pueda dañar los mismos, la disminución de riesgos podrá lograr que la información sea integra, confiable y disponible.

Se deben crear manuales de seguridad para diferentes casos de posible fuga de información, la dirección debe estar un paso adelante en el caso de una auditoría, y así mismo generar confianza para la organización.

Se realiza el análisis de las fallas de la empresa y se invitan a sus funcionarios a implementar un SGSI ya que por ahora solo se ha hecho la identificación de amenazas, riesgos y vulnerabilidades, los controles y recomendaciones deben ser tenidos en cuenta para poder mejorar la calidad como empresa, y así mismo ser más competitiva en el mercado actual.

Saber que incluso al aplicar un SGSI se debe tener el compromiso que debe estar en continuo mejoramiento y aprendizaje, para poder tomar las mejores de medidas para poder funcionar la empresa con normalidad.

BIBLIOGRAFÍA

AGESAGRO S.A.S. (2009). MISIÓN Y VISIÓN. {En línea} {22 de abril de 2017} Disponible en: https://biodomo2.wixsite.com/agesagro/mision-y-vision

Alcaldía de Ibagué-Tolima. (2016). SGSI. Ibagué, Colombia. {En línea} {09 de agosto de 2016} Disponible en: http://www.alcaldiadeibague.gov.co/portal/seccion/contenido/index.php?type=3&cnt=10

AMUTIO, Miguel. CANDAU, Javier. MAÑAS, José. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*, (pp 25-47). España, Madrid.

AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, Madrid, España, 2012.

AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012.

AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas, Madrid, España, 2012.

CARVAJAL. A. (2008). Analisis y gestion de riesgos, base fundamental del SGSI Caso: Metodologia Magerit. {En línea} {12 de noviembre de 2016} Disponible en: http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (Agosto 18 de 1999). Diario Oficial 43.673 del 21 de agosto de 1999. p. 1-15.

COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. P. 1-15.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (Enero 05 de 2009). Diario Oficial 47.223 del 05 de enero de 2009. p. 1-4.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341. (Julio 30 de 2009). Diario Oficial 47.426 del 30 de julio de 2009. p. 1-15.

Consejo Superior de Administración Electrónica. (2012) MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea} {22 de agosto de 2015} Disponible en:

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VybNzvnhBpg

Departamento de seguridad informática. (2016). Amenazas a la Seguridad de la Información. {En línea} {09 de agosto de 2016} Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node%2F12

DIAZ, David. (2009). Políticas informáticas para tu empresa. {En línea} {12 de noviembre de 2016} Disponible en: https://daviddiazdelacruz.wordpress.com/2009/05/12/politicas-informaticas-para-tu-empresa/

ESPAÑA, Ley Orgánica 15/1999, de 13 de noviembre. de protección de datos de carácter personal. P.111-114.

ESPAÑA, Ley 11/2007, de 22 de junio. de acceso electrónico de los ciudadanos a los Servicios Públicos. P.111-114.

ESPAÑA, Real Decreto 3/2010, de 8 de enero. por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín oficial del Estado 30 de Enero de 2010. P.1-49.

Fernández, V. E. (2009). El gobierno y la gestión de las TIC: una aproximación práctica al ámbito del sector público universitario. Madrid, ES: Dykinson. Retrieved from http://www.ebrary.com

Finagro. (2013). ¿Qué es FINAGRO?. {En línea} {09 de agosto de 2016} Disponible en: https://www.finagro.com.co/qui%C3%A9nes-somos/informaci%C3%B3n-institucional

GAONA, Karina del Rocio. APLICACION DE LA METODOLOGIA MAGERIT PARA EL ANALISIS Y GESTION DE RIESGOS DE LA SEGURIDD DE LA INFORMACIÓN APLICADO A AL EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A. EN LA CIUDAD DE MACHALA. 2013. http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf [Consulta: Sábado, 12 de noviembre de 2016]

Gomez, A.J., & Valverde, J.O. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO, UTILIZANDO LA METODOLOGÍA MAGERIT. (2011-2012), http://dspace.ucuenca.edu.ec/bitstream/123456789/1342/1/tcon640.pdf [Consulta: Sábado, 12 de noviembre de 2016]

Gómez, F. L., & Fernández, R. P. P. (2015). Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad.

Madrid, ES: AENOR - Asociación Española de Normalización y Certificación. Retrieved from http://www.ebrary.com

GUTIERREZ, C. (2013) MAGERIT: metodología práctica para gestionar riesgos. {En línea} {22 de agosto de 2015} Disponible en: http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

HURTADO DE BECERRA, Jacqueline. Guía para la comprensión Holística de la Ciencia. Caracas Venezuela, Edit. Sypal. 2010.

Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior. (2014). Manual de políticas de seguridad de la información. {En línea} {25 de marzo de 2017} Disponible en: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

ISO27000 (2012). ¿Qué es un SGSI? {En línea} {12 de Noviembre de 2016} Disponible en: http://www.iso27000.es/sgsi.html

MARCIAL, Noel. CIENCIAS DE LA INFORMACION. Información: Una nueva propuesta conceptual. vol.27. Ciudad de la habana Cuba: Acimed,1996. 193 p.

MARTINEZ, J. (2012) Colombia, el primer país que penaliza los delitos informáticos. {En línea} {2 de abril de 2016} Disponible en: http://www.lapatria.com/tecnologia/colombia-el-primer-pais-que-penaliza-los-delitos-informaticos-1980

MENDOZA, M. (2015) ¿Cuál es la idea central de aplicar ISO 27001? {En línea} {22 de agosto de 2015} Disponible en: http://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/

MIFSUD. E. (2012) Introducción a la seguridad informática - Vulnerabilidades de un sistema informático. {En línea} {22 de agosto de 2015} Disponible en: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

Ministerio Tecnologías de la Información y las Comunicaciones. (2014) Sistemas de Gestión de la Seguridad de la Información (SGSI). {En línea} {9 de abril de 2016} Disponible en: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

Ministerio TIC. (2014). MODELO DE SEGURIDAD. {En línea} {12 de noviembre de 2016} Disponible en: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

PACHECO, F. (2010) La importancia de un SGSI, {En línea} {2 de abril de 2016} Disponible en: http://www.welivesecurity.com/la-es/2010/09/10/la-importancia-de-un-sgsi/

PEÑA, C. (2016) Los principales retos que afronta el país en seguridad informática. {En línea} {12 de noviembre de 2016} Disponible en: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/desafios-que-afronta-colombia-en-seguridad-informatica-/16714536

PEREZ, J. (2013). Definición de confidencialidad. {En línea} {12 de noviembre de 2016} Disponible en: http://definicion.de/confidencialidad/

PEREZ, J. (2013). Definición de integridad. {En línea} {12 de noviembre de 2016} Disponible en: http://definicion.de/integridad/

PEREZ, J. (2013). Definición de Riesgo. {En línea} {12 de noviembre de 2016} Disponible en: http://definicion.de/riesgo/

Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). {En línea} {12 de noviembre de 2016} Disponible en: http://dle.rae.es/?id=0clfXYb

Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). {En línea} {12 de noviembre de 2016} Disponible en: http://dle.rae.es/?id=LXrOqrN

Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). {En línea} {12 de noviembre de 2016} Disponible en: http://dle.rae.es/?id=URUdTVs

ROMERO, L. (2002) Seguridad informática conceptos generales. España. {En línea} {12 de noviembre de 2016} Disponible en: http://campus.usal.es/~derinfo/Activ/Jorn02/Pon2002/LARyALSL.pdf

SANCHEZ, Y. (2014) Ciclo PHVA. {En línea} {12 de noviembre de 2016} Disponible en: http://www.gerencie.com/ciclo-phva.html

Superintendencia Financiera de Colombia. (2006) Circular externa 048 de 2006. {En línea} {12 de noviembre de 2016} Disponible en: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=20144

TechNet. (2005). Descripción de la disponibilidad, la confiabilidad y la escalabilidad. {En línea} {12 de noviembre de 2016} Disponible en: https://technet.microsoft.com/es-es/library/aa996704(v=exchg.65).aspx

ANEXOS

Anexo A. Política global de seguridad de la información

En AGESAGRO S.A.S la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad[51].

Consciente de las necesidades actuales, AGESAGRO S.A.S implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información del AGESAGRO S.A.S, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

[51] Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior, 2014, https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf [Consulta: Sábado, 25 de marzo de 2017]

Anexo B. Sanciones para las violaciones a las políticas de seguridad de la información

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores del AGESAGRO S.A.S. Por tal razón, es necesaria que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

Anexo C. Política para uso de dispositivos móviles

AGESAGRO S.A.S determinará las condiciones para el manejo de los dispositivos móviles y personales que hagan uso de servicios de la empresa. Igualmente vigilará para que los empleados hagan un uso responsable de los servicios y equipos proporcionados por la empresa.

La GERENCIA debe investigar y probar las opciones de protección de los dispositivos móviles empresariales, como personales que hagan uso de los servicios provistos por la empresa.

La GERENCIA debe determinar que configuraciones son admisibles para los dispositivos móviles empresariales o personales que hagan uso de los servicios suministrados por AGESAGRO S.A.S

La GERENCIA debe instaurar un método de bloqueo para los dispositivos móviles empresariales que sean entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad, automáticamente entren a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual solicitará el método de desbloqueo nuevamente.

La GERENCIA debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles empresariales evitando la copia de datos si no se conoce el método de desbloqueo.

La GERENCIA debe configurar la opción de borrado remoto de información en los dispositivos móviles empresariales, con el fin de eliminar la información contenida en los mismos, evitando así el flujo no autorizado de información en caso de pérdida o hurto.

La GERENCIA debe contar con una copia de seguridad de la información contenida en los dispositivos móviles institucionales de AGESAGRO S.A.S.

La GERENCIA debe instalar un software de antivirus tanto en los dispositivos móviles empresariales como en los personales para evitar la propagación de virus en la empresa.

Los empleados deben evitar usar los dispositivos móviles en lugares que no les brinden garantías de seguridad necesarias para evitar pérdida o robo de los mismos.

Los empleados no deben modificar las configuraciones de seguridad de los dispositivos móviles empresariales, tampoco desinstalar el software provisto con ellos al momento de su entrega.

Los empleados deben evitar la instalación de programas de fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles empresariales.

Los empleados deben, cada vez que el dispositivo móvil empresarial notifique de una actualización disponible, aceptar y aplicar la nueva versión.

Los empleados deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

Los empleados deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros, también pasar el antivirus a la memoria USB antes de ingresar a los equipos.

Anexo D. Política de seguridad personal

AGESAGRO S.A.S reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

La Gerencia debe certificar que los funcionarios del instituto firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

La GERENCIA debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de AGESAGRO S.A.S.

El personal provisto por terceras partes que realicen labores en o para AGESAGRO S.A.S, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad de la Información del instituto.

La GERENCIA debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer el instituto.

La Alta Dirección debe promover la importancia de la seguridad de la información entre los funcionarios de AGESAGRO S.A.S y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

La GERENCIA debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente el instituto, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Anexo E. Política de uso de periféricos y medios de almacenamiento

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de AGESAGRO S.A.S será reglamentado por la Dirección de Tecnología, junto con la Oficina de Riesgos, considerando las labores realizadas por los funcionarios y su necesidad de uso.

La GERENCIA debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de AGESAGRO S.A.S.

La GERENCIA debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica del instituto, de acuerdo con los lineamientos y condiciones establecidas.

La GERENCIA debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento del instituto, ya sea cuando son dados de baja o re-asignados a un nuevo usuario

La GERENCIA debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica del instituto de acuerdo con el perfil del cargo del funcionario solicitante.

Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Los funcionarios de AGESAGRO S.A.S y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Los funcionarios y personal provisto por terceras partes son responsables por el custodio de los medios de almacenamiento institucionales asignados. ϖ Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de AGESAGRO S.A.S.

Anexo F. Política de acceso a redes y recursos de red

La GERENCIA de AGESAGRO S.A.S, como responsables de las redes de datos y los recursos de red de la empresa, debe asegurarse que las redes estén debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

La GERENCIA debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de AGESAGRO S.A.S.

La GERENCIA debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que evite accesos no autorizados.

La GERENCIA debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red del AGESAGRO S.A.S, así como velar por la aceptación de las responsabilidades de dicho tercero. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

La GERENCIA debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Los funcionarios y personal provisto por terceras partes, antes de contar con acceso por primera vez a la red de datos de AGESAGRO S.A.S., deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la empresa deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

Anexo G. RAE

Fecha de Realización: 17/04/2017
Título: ESTUDIO DE ANÁLISIS Y GESTIÓN DE RIESGO AL SISTEMA DE INFORMACIÓN DE LA EMPRESA AGESAGRO S.A.S UTILIZANDO LA METODOLOGÍA MAGERIT
Autor: VARÓN, Juan
Palabras Claves: AGESAGRO S.A.S, amenaza, Finagro, MAGERIT, riesgo, vulnerabilidad.
Descripción: Monografía de estudio sobre la implementación de la Metodología MAGERIT analizando los riesgos y vulnerabilidades, presentando políticas de seguridad para mejorar el nivel de seguridad de la información de AGESAGRO S.A.S de Ibagué
Fuentes: AGESAGRO S.A.S. (2009). MISIÓN Y VISIÓN. {En línea} {22 de abril de 2017} Disponible en: https://biodomo2.wixsite.com/agesagro/mision-y-vision AMUTIO, Miguel. CANDAU, Javier. MAÑAS, José. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, (pp 25-47). España, Madrid. AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, Madrid, España, 2012. AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II – Catálogo de Elementos, Madrid, España, 2012. AMUTIO, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III – Guía de Técnicas, Madrid, España, 2012. COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (Agosto 18 de 1999). Diario Oficial 43.673 del 21 de agosto de 1999. p. 1-15. COLOMBIA, CONGRESO DE LA REPUBLICA. Ley 1266. Bogotá. (Diciembre 31 de 2008). Diario Oficial 47.219 de diciembre 31 de 2008. P. 1-15. COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (Enero 05 de 2009). Diario Oficial 47.223 del 05 de enero de 2009. p. 1-4. COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341. (Julio 30 de 2009). Diario Oficial 47.426 del 30 de julio de 2009. p. 1-15.

Departamento de seguridad informática. (2016). Amenazas a la Seguridad de la Información. {En línea} {09 de agosto de 2016} Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node%2F12

Finagro. (2013). ¿Qué es FINAGRO?. {En línea} {09 de agosto de 2016} Disponible en: https://www.finagro.com.co/qui%C3%A9nes-somos/informaci%C3%B3n-institucional

GAONA, Karina del Rocio. APLICACION DE LA METODOLOGIA MAGERIT PARA EL ANALISIS Y GESTION DE RIESGOS DE LA SEGURIDD DE LA INFORMACIÓN APLICADO A AL EMPRESA PESQUERA E INDUSTRIAL BRAVITO S.A. EN LA CIUDAD DE MACHALA. 2013. http://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf [Consulta: Sábado, 12 de noviembre de 2016]

Gomez, A.J., & Valverde, J.O. ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO, UTILIZANDO LA METODOLOGÍA MAGERIT. (2011-2012), http://dspace.ucuenca.edu.ec/bitstream/123456789/1342/1/tcon640.pdf [Consulta: Sábado, 12 de noviembre de 2016]

HURTADO DE BECERRA, Jacqueline. Guía para la comprensión Holística de la Ciencia. Caracas Venezuela, Edit. Sypal. 2010.

ISO27000 (2012). ¿Qué es un SGSI? {En línea} {12 de Noviembre de 2016} Disponible en: http://www.iso27000.es/sgsi.html

MARCIAL, Noel. CIENCIAS DE LA INFORMACION. Información: Una nueva propuesta conceptual. vol.27. Ciudad de la habana Cuba: Acimed,1996. 193 p.

MENDOZA, M. (2015) ¿Cuál es la idea central de aplicar ISO 27001? {En línea} {22 de agosto de 2015} Disponible en: http://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/

PEREZ, J. (2013). Definición de confidencialidad. {En línea} {12 de noviembre de 2016} Disponible en: http://definicion.de/confidencialidad/

PEREZ, J. (2013). Definición de integridad. {En línea} {12 de noviembre de 2016} Disponible en: http://definicion.de/integridad/

PEREZ, J. (2013). Definición de Riesgo. {En línea} {12 de noviembre de 2016} Disponible en: http://definicion.de/riesgo/

Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). {En línea} {12 de noviembre de 2016} Disponible en: http://dle.rae.es/?id=0clfXYb

Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). {En línea} {12 de noviembre de 2016} Disponible en: http://dle.rae.es/?id=LXrOqrN

Real Academia Española. (2014). Diccionario de la lengua española (23.a ed.). {En línea} {12 de noviembre de 2016} Disponible en: http://dle.rae.es/?id=URUdTVs

Contenido del documento:

La metodología MAGERIT como análisis y gestión de riesgos determina el nivel de riesgo de la información en la empresa, los cuales pueden ser causados por hardware, software o inexperiencia en seguridad de la información, para lo cual se deben contar con ciertas pautas para poder proteger la información de la empresa.

La monografía intenta presentar las vulnerabilidades y riesgos a los cuales está expuesta la empresa y se deben determinar qué medidas se pueden aplicar para poder proteger los sistemas de información para prevenir ataques latentes por medio de ataques de software, hardware o por falta de conocimiento de buenas prácticas para proteger la información.

Se debe determinar en el trabajo cuales son los puntos cruciales y neurálgicos a proteger para evitar la fuga de la información, dando soluciones o propuestas para que AGESAGRO S.A.S. de Ibagué pueda evitar que la información sea accedida por terceros mal intencionados.

Se presentan políticas y sugerencia para evitar que la información sea accedida por personas mal intencionadas tomando en cuenta que se deben realizar medidas preventivas e implementación de buenas prácticas para que se cree una conciencia de seguridad en la información.

Las medidas de seguridad en la información para AGESAGRO S.A.S, es fundamental para evitar que las vulnerabilidades puedan causar un gran daño en la empresa.

Metodología:

La investigación es proyectiva, ya que se realiza la elaboración de una propuesta

de seguridad de la información basado en el análisis de los riesgos amenazas y vulnerabilidades actuales, para evitar que a futuro se pueda exponer la información de los usuarios de la empresa, basado en los resultados del proceso investigativo, para que se puedan generar buenas prácticas en el uso de la información. La fuente de la información es obtenida directamente de los empleados de la empresa AGESAGRO S.A.S, se establecieron como objetivos Realizar un informe del estado actual del sistema de información de la empresa AGESAGRO S.A.S. Se realizan los siguientes objetivos: Identificar los activos de información que pertenecen a la empresa AGESAGRO S.A.S. y clasificarlos a acuerdo a la metodología MAGERIT. Identificar las amenazas y riesgos de los activos de información en la empresa AGESAGRO S.A.S. Proponer controles basados en la norma ISO 27002:2013 a los riesgos identificados en la empresa AGESAGRO S.A.S.
Conceptos nuevos: Metodología MAGERIT, ISO 27001, AGESAGRO S.A.S, riesgos, amenazas, vulnerabilidad.
Conclusiones: Se encuentran bastantes fallos de seguridad en la empresa y falta de capacitación en los empleados, los recursos y activos se deben de cuidar en almacenamiento y ambiente que pueda dañar los mismos, la disminución de riesgos podrá lograr que la información sea integra, confiable y disponible. Se deben crear manuales de seguridad para diferentes casos de posible fuga de información, la dirección debe estar un paso adelante en el caso de una auditoría, y así mismo generar confianza para la organización. Se realiza el análisis de las fallas de la empresa y se invitan a sus funcionarios a implementar un SGSI ya que por ahora solo se ha hecho la identificación de amenazas, riesgos y vulnerabilidades, los controles y recomendaciones deben ser tenidos en cuenta para poder mejorar la calidad como empresa, y así mismo ser más competitiva en el mercado actual. Saber que incluso al aplicar un SGSI se debe tener el compromiso que debe estar en continuo mejoramiento y aprendizaje, para poder tomar las mejores de medidas para poder funcionar la empresa con normalidad.
AUTOR: JUAN CARLOS VARÓN QUIROGA