# RESUMEN – TRABAJO DE GRADO

| | |
|---|---|
| **AUTORES** | Jefferson Farelo Páez, Jenis Del Carmen Sagbini Echavez. |
| **FACULTAD** | Ingeniería. |
| **PLAN DE ESTUDIOS** | Especialización en Auditoria de Sistemas. |
| **DIRECTOR** | Ana Melissa Rodríguez Chinchilla. |
| **TÍTULO DE LA TESIS** | Diseño del Sistema de Gestión de la Seguridad de la Información SGSI basado en el Estándar ISO 27001, en Ultraline Electrónica S.A.S en la Ciudad de Barranquilla. |
| **TITULO EN INGLES** | Design of the SGSI Information Security Management System based on the ISO 27001 Standard, at Ultraline Electrónica S.A.S in the City of Barranquilla. |


## RESUMEN
**(70 palabras)**

El Sistema de Información es el recurso más valioso dentro de la cadena productiva de las organizaciones; el buen uso, puede significar la diferencia entre el éxito o el fracaso para una empresa. es por ello, que es importante la administración de la información, la preservación de la confidencialidad, la integralidad y la disponibilidad de la misma; a través de herramientas como el ciclo de Deming PHVA como mejora continua de la calidad.

## RESUMEN EN INGLES

The Information System is the most valuable resource within the productive chain of organizations; Good use can mean the difference between success or failure for a business. That is why the administration of the information, the preservation of the confidentiality, the integrity and the availability of the same is important; through tools such as the Deming PHVA cycle as continuous quality improvement.



| | |
|---|---|
| **PALABRAS CLAVES** | Sistema, Gestión, Monitoreo, Control, Norma, Riesgos, Auditoria, Autenticación, Evaluación de Riesgos, Firewall. |
| **PALABRAS CLAVES EN INGLES** | System, Management, Monitoring, Control, Standard, Risks, Audit, Authentication, Risk Assessment, Firewall. |


## CARACTERÍSTICAS

| | | | |
|---|---|---|---|
| PÁGINAS: 104 | PLANOS: | ILUSTRACIONES: 19 | CD-ROM: 1 |

# DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI BASADO EN EL ESTÁNDAR ISO 27001, EN ULTRALINE ELECTRÓNICA S.A.S., EN LA CIUDAD DE BARRANQUILLA

**Autores**
**JEFFERSON FARELO PAEZ**
**JENIS DEL CARMEN SAGBINI ECHÁVEZ**

**Trabajo de Grado presentado como requisito para optar al título de Especialista en Auditoría de Sistemas**

**Director**
**Ing. ANA MELISSA RODRIGUEZ CHINCHILLA**
**Especialista en Auditoria de Sistemas**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**
**FACULTAD DE INGENIERÍAS**
**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**

**Ocaña, Colombia** **Septiembre, 2021**

# Índice

# Lista de tablas

# Lista de figuras

# Lista de apéndices

# Introducción

Es bien conocido hoy, que las Tecnologías de la Información y la Comunicación (TIC) ha transformado vidas humanas y empresariales. Cada día las empresas dependen de las TIC y sus procesos se basan en sistemas que están interconectados al mundo del internet, por lo que su información está expuesta. Cuanto mayor sea el uso de la Informática y las redes de comunicación, su información estará más expuesta a incidentes de seguridad.

Un 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. Su implantación supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada. Fundamentalmente se distinguirán dos tipos de procesos: 1. Procesos de gestión. Controlan el funcionamiento del propio sistema de gestión y su mejora continua. 2. Procesos de seguridad. Se centran en los aspectos relativos a la propia seguridad. (Gómez, 2015)

En el presente proyecto se da a conocer la elaboración de un Diseño de Sistemas de Gestión de Seguridad de la Información (SGSI) para la empresa Ultraline Electrónica S.A.S. en la ciudad de Barranquilla. El primer capítulo describe los componentes iniciales del proyecto, donde se define el problema y objetivos. En el segundo capítulo se establecen los Marcos Teóricos y Conceptuales para seguir con el marco metodológico en el tercer capítulo. Finalmente, se establecen los resultados de la investigación.

# 1.Diseño del Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el estándar ISO 27001, en Ultraline Electrónica S.A.S., en la ciudad de Barranquilla

## *1.1.Planteamiento del problema*

Ultraline Electrónica S.A.S., anteriormente Ultraline de la Costa S.A., es una empresa industrial tipo pyme, cuyas operaciones comerciales iniciaron en el año 1999 en la ciudad de Barranquilla. Ultraline Electrónica S.A.S. se dedica a producir y comercializar equipos electrónicos tipo reguladores, elevadores de voltajes, multitomas, protectores de neveras, inversores, convertidores, transformadores de aislamientos, ups, baterías para ups, cargadores de baterías, entre otros.

Desde su fundación, los procesos de Ultraline Electrónica S.A.S., fueron creciendo de forma consistente, por lo que, su estructura organizacional y número tanto de clientes y consumidores, fueron testigos de su exitosa y dinámica posición en el mercado actual. De 5 personas que iniciaron laborando y 15 clientes comercializando sus productos; hoy, 20 años después, se pueden calcular 250 clientes y 20 empleados directos. Sus productos son conocidos en toda la Costa Atlántica de Colombia generando ingresos y recursos para muchas familias de la región norte Colombiana.

Para lograr ese posicionamiento en el mercado, Ultraline Electrónica S.A.S., aplicó muchas estrategias administrativas y utilizó información basada en innovaciones de carácter tecnológicas permitiendo mejorar el recurso humano e implementando sistemas de información que mejoraran la productividad volviéndola más competitiva y de esta forma poder enfrentar los retos del nuevo milenio. En este sentido, la utilización de las Tecnologías de la Información y la Comunicación

(TIC) ha sido un factor clave en el interior de la organización, generando muchas ventajas competitivas en cada una de las metas trabajadas. Su uso y aplicación en las actividades diarias y cotidianas, han permitido incrementar la eficiencia, rentabilidad, efectividad y aprovechamiento de los recursos. Tener sistemas de cómputo, una red interna, unos procesos administrativos sistematizados, han sido decisivos en las tomas de decisiones.

A pesar de lo anterior y de los cambios dinámicos, Ultraline Electrónica S.A.S. no cuenta con una oficina de sistemas consolidada, oficializada y organizada que permita brindar un soporte tecnológico apropiado basado en unos estándares vigentes y en una normatividad. Lo anterior se debe a que las diferentes áreas de la empresa trabajan con recursos de internet, cableado estructurado, con varios sistemas de cómputo e impresoras pero todas esas operaciones se hacen de forma aislada, con la carencia de unas políticas de seguridad de la información implementadas y asimiladas por cada trabajor, con usuarios que desconocen por completo las normas básicas en el uso de los equipos y realización de copias de seguridad, con poca protección a la seguridad de la información, con procesos que comprometen y ponen en riesgo la confidencialidad, integridad, disponibilidad, el no repudio y autenticidad de la información.

Todos los procesos que Ultraline Electrónica S.A.S. lleva a cabo no se encuentran definidos en un estándar específico que permita satisfacer las necesidades totales de la organización; ocasionando de esta manera, que los sistemas de información utilizados sean susceptibles a múltiples amenazas poniendo en riesgo activos críticos bajo muchas formas que los delincuentes utilizan como el sabotaje, delitos informáticos, fraudes, daños en equipos de cómputo, servidores y otros elementos informáticos. Los sistemas de información utilizados en Ultraline Electrónica

S.A.S., se convierten en un blanco debido a que presentan altos índices de vulnerabilidades al tener un alto e importante flujo de información en las operaciones cotidianas productivas y comerciales de la organización.

## *1.2. Formulación del problema*

¿El diseño de un Sistema de Gestión de Seguridad de la Información SGSI con base en el estándar ISO 27001, proveerá a Ultraline Electrónica S.A.S. los elementos y mecanismos adecuados para mejorar la seguridad de la información y la gestión de los riesgos que se asocian al tratamiento y uso de la misma?

## *1.3. Objetivos*

### *1.3.1. Objetivo general*

Diseñar el Sistema de Gestión de Seguridad de la Información SGSI con base en el estándar ISO27001, en Ultraline Electrónica S.A.S, en la ciudad de Barranquilla.

### *1.3.2. Objetivos específicos*

Diagnosticar el estado de la seguridad de la información en Ultraline Electrónica S.A.S., en la ciudad de Barranquilla, para conocer sus amenazas, vulnerabilidad e impactos.

Determinar los elementos del estándar ISO 27001, que puedan ser aplicados en Ultraline Electrónica S.A.S., en la ciudad de Barranquilla.

Establecer el Sistema de Gestión de la Seguridad de la Información (SGSI) para Ultraline Electrónica S.A.S., en la ciudad de Barranquilla.

Realizar una prueba utilizando las Políticas del Sistema de Gestión de la Seguridad de la Información (SGSI) en la oficina de Sistemas de Ultraline Electrónica S.A.S., en la ciudad de Barranquilla.

### *1.4.Justificación*

La información es considerada como el elemento más importante dentro de la cadena productiva de las organizaciones. Es un recurso vital, y el buen uso de ésta puede significar la diferencia entre el éxito o el fracaso para una empresa. El éxito de una organización ya no depende sólo de la manera en que cada persona maneja sus recursos materiales, sino que es más importante el buen aprovechamiento de los activos intangibles tales como el know-how (hacer como), el conocimiento de cliente y de mercado, entre otros. (blogs.eusto.es, 2015)

Un SGSI, Sistema de gestión de la seguridad de la información basado en la norma ISO 271001, es una herramienta sencilla que permite a cualquier Pyme utilizar para conocer, gestionar y lograr minimiza los riesgos posibles que atenten contra la seguridad de la información en el interior de su empresa. Es una metología sencilla y barata que donde la implantación y posterior certificación de los sistemas, supone la implicación de toda la empresa. (cic.es, 2019)

Ultraline Electrónica S.A.S., durante los últimos años ha crecido de manera vertiginosa permitiéndole asegurar una proyección como marca posicionada en un mercado dinámico y

cambiante. Para ello, sus operaciones están basadas en una infraestructura física que han estado en un constante mejoramiento en el ámbito tecnológico permitiendo a sus clientes una atención adecuada y eficiente.

De acuerdo a lo anterior, se hace necesario realizar el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) para Ultraline Electrónica S.A.S. que se basó en el estándar ISO 27001. Este SGSI está enmarcado en una política de la seguridad de la información que permitirá identificar, estudiar y evaluar grandes riesgos a los que está expuesta; tales como la pérdida total o parcial de datos, el sabotaje en los sistemas de información y comunicación, cambios o alteración de información que posee la entidad y que de alguna manera contribuyen al desarrollo adecuado de los procesos productivos, administrativos y comerciales de la organización.

No existe un entorno 100% seguro en un Sistema de Información, los incidente existirán siempre, aún sin importar los controles que se lleguen a implementar en el interior de las organizaciones. Sin embargo, con estes SGSI, Ultaline Electrónica S.A.S. podrá conocer cuáles son los incidentes más comunes que se llegaren a presentar; lo que permitirá a la Gerencia, orientar de forma eficiente las inversiones en seguridad hacia las brechas que podrían llegar a generar un mayor impacto en caso que llegase a materializarse un incidente en la organización. Lo importante de todo es que se puedan detectar a tiempo y poder mitigarlos a través de controles eficientes.

### *1.5.Hipótesis*

El presente proyecto permitirá conocer cuáles son las vulnerabilidades, riesgos y amenazas

que tiene la empresa Ultraline Electrónica S.A.S. en la ciudad de Barranquilla en el uso y aplicación de la infraestructura tecnológica y por ende, en sus sistemas de información. Con la prueba piloto que se realizará a través del área de Sistemas, se podrá determinar la manera de implementar las políticas del sistema de seguridad de la información basadas en la norma ISO27001. Todo lo anterior permitirá obtener un porcentaje mayor de confianza en el manejo de los sistemas de información y comunicación (TIC) de las diferentes áreas existentes en Ultraline Electrónica S.A.S.

Establecer el Sistema de Gestión de la Seguridad de la Información (SGSI) para Ultraline Electrónica S.A.S., en la ciudad de Barranquilla, permitirá que los procesos sean más confiables y eficientes debido a que todos los sistemas de información que se manejan en su interior, contarán con parámetros que suplirán las necesidades del personal administrativo y de todos sus clientes.

### *1.6.Delimitaciones*

#### *1.6.1.Delimitación geográfica*

El presente proyecto se desarrolló en la ciudad de Barranquilla, departamento del Atlántico, específicamente en las instalaciones de la empresa Ultraline Electrónica S.A.S. que está ubicada en Cra. 45 #60 -37.

Desde el punto de vista geográfico, Barranquilla se encuentra al norte de América del Sur y de la República de Colombia, ocupa la parte más septentrional del Departamento del Atlántico, del cuál es su capital. La ciudad se levanta en la margen izquierda del río grande de La Magdalena y a 22 kilómetros aguas arriba de su desembocadura en el mar Caribe, sitio conocido como Bocas

de Ceniza en una amplia zona donde la mayor parte es plana con algunas ondulaciones en un área de 154 kilómetros cuadrados. Barranquilla está situada a 74° 50' 43" o sea casi 11 grados latitud boreal. (www.arroyosdebarranquilla.co, 2013)

El departamento del Atlántico presenta un clima tropical de tipo estepa y sabana de carácter árido en la desembocadura del río Magdalena y alrededores de Barranquilla; semi-árido en las fajas aledañas al litoral y al río Magdalena y semihúmedo desde Sabanalarga hacia el sur. El departamento del Atlántico tiene una extensión de 3.386 Kms.² (Atlántico, 2010)

### *1.6.2.Delimitación temporal*

El proyecto tuvo una duración de tres meses, a saber: octubre, noviembre y diciembre. Todo de acuerdo al cronograma pre-establecido especificado por fases.

### *1.6.3.Delimitación conceptual*

La cobertura del presente proyecto fue la empresa Ultraline Electrónica S.A.S., donde se desarrolló un sistema de gestión de seguridad de la información basado en el estándar ISO 27001.

Desde el punto de vista académico, el marco de desarrollo del proyecto fue el del área de la Ingeniería de Sistemas debido a que se aplicaron conocimientos en las siguientes:

- Formulación de proyectos
- Metodología de la investigación

- Estadística
- Tecnologías de la información y la comunicación
- Redes y telecomunicaciones

### *1.6.4.Delimitación operativa*

El presente proyecto se desarrolló para el mejoramiento y mayor productividad de todas las áreas operativas y administrativas pertenecientes a la empresa Ultraline Electrónica S.A.S., entre ellas: área de producción, financiera, recursos humanos y gerencia y sistemas.

Dentro de los factores que pudieron obstruir el avance y el oportuno desarrollo de la presente investigación estuvieron, el desplazamiento de ciudad porque los autores se encuentran residenciados en Valledupar. Igualmente, la disponibilidad del tiempo, la información que se pudo encontrar referente a la temática investigada y aquella que los funcionarios de forma virtual y presencial pudieron entregar en el momento de aplicar la metodología de la investigación (entrevista, encuesta).

# 2.Marco referencial

## *2.1.Marco histórico*

### *2.1.1.Antecedentes*

Hoy en día, con el impulso acelerado que despliegan las organizaciones en sus diferentes campos de acción, la información se ha evolucionado en el activo más valioso e importante para el desempeño adecuado de sus acciones diarias. Es tal su importancia que se recomienda establecer Sistemas de Gestión de Seguridad de la Información (SGSI) para su resguardo y protección. Así mismo, el análisis y la evaluación de riesgos, la verificación de la existencia de controles de seguridad existentes, las pruebas con software y el monitoreo de los sistemas de información han permitido establecer un diagnóstico efectivo para visualizar y establecer el estado actual de la organización, logrando identificar las causas de sus posibles amenazas y vulnerabilidades, para proponer soluciones de control que permitan la mitigación del riesgo planteado. (http://video.anetcom.es/editorial/, 2015)

En este orden de ideas, discutir sobre la seguridad de la información es pensar en muchos puntos, pero el más importante de todos es desviarse hacia el futuro y establecer directrices que podría acontecer en un mañana, qué efecto o pérdidas causaría si la información que manipula la organización a diario cae en manos de personas malintencionadas, que pasaría si mediante algún tipo de ataque o daño se perdieran los procesos y la información de la organización. (http://video.anetcom.es/, 2015)

De igual modo, con el crecimiento tecnológico, abordar la implementación de un sistema de gestión de seguridad es extremadamente complejo para una pequeña o mediana empresa, ya que

la tendencia inicial en el campo de la seguridad informática de la empresa es migrar gradualmente su cultura hacia la creación de un sistema de gestión de seguridad de la información (SGSI), a pesar de que esta progresión es bastante lenta y requiere tanto tiempo como esfuerzo físico y económico por parte de la organización. Incluso, este sistema de gestión de seguridad de la información, puede tener varios niveles de exigencia, y sus recursos limitados. Además, la mayor problemática es que el proceso casi siempre llega al punto en que la empresa se ve obligada a correr el riesgo de no tener un sistema de gestión de seguridad de la información por no poder implementarlo. (AS/NZS 4360, 2004)

Por lo tanto, autores como René Sant-Germain (Sant-Germain 2005) Estimaron que, con los modelos actuales, solo para 2009, 35% de las empresas en el mundo que emplean más de 2000 personas habrán implementado un SGSI, y que las cifras para las PYME serán mucho peor, ya que con el avanzar tecnológico el mercado exige que las empresas y organizaciones garanticen que las tecnologías de información y comunicación sean seguras, rápidas y fáciles de interactuar con los clientes. (Sant-Germain, 2005)

No obstante, en orden de cumplir estos requisitos, los directivos de distintas organizaciones, han descubierto dos problemas sin solución satisfactoria: el primero, la falta de herramientas para enfrentar la gestión de la seguridad de la información en forma centralizada, y simple acorde a cualquier tipo o tamaño de empresa y el segundo problema es la elaboración de un conjunto de reglas o buenas prácticas que definan y certifiquen la gestión de la seguridad, mediante controles y reglas a nivel nacional e internacional. (Josef Pieprzyk, 2003)

Por otro lado, la sociedad de la información depende cada vez más de los sistemas de gestión de seguridad de la información (SGSI), y estos sistemas han expandido y han llenado de vitalidad a las pequeñas y medianas empresas (PYME). Sin embargo, una característica primordial de los SGSI es que deben adaptarse a las características específicas de estas empresas, al punto de ser optimizados desde el área de recursos, para lograr instalarlos y mantenerlos, centrándolos en las técnicas y la gestión institucional de forma progresiva y sostenible. (http://168.243.33.153/infolib/tesis/50107386.pdf)

Análogamente, el objetivo de la institucionalización en los SGSI es construir una cultura de seguridad de la información en de tal manera que la seguridad de la información se convierta en un aspecto natural de toda la organización e involucre todas las actividades diarias de los empleados, para desarrollar y controlar el uso indebido de toda la información que circula en el entorno empresarial en que se encuentra la organización, contribuyendo de forma parcial a la protección de los datos, la información y la gestión del conocimiento empresarial. (Normas ISO/iec 27001, 2013)

En otro orden de cosas, numerosos casos de estudio han demostrado que la implementación de estas buenas prácticas en las organizaciones puede reducir los riesgos, amenazas y vulnerabilidades, por esto mismo, han sido creados numerosos estándares internacionales, tales como: ISO/IEC 27001, COBIT, etc.; que han servido como ayuda y soporte a las organizaciones en los procesos de implementación y gestión de seguridad de información, y activos como: hardware y software, pero sobre todo el más importante de todos: la información. (www.iso27000.es, 2008).

Sumando esto, muchos países han sido conscientes del contexto tecnológico que se está presentando con el crecimiento y han tenido en cuenta que cualquier riesgo o amenaza que se presente en la organización puede ocasionar pérdidas reales, legales y económicas, ya que con el acceso no permitido a la parte tecnológica de cualquier organización es ampliamente vulnerable a una infinidad de ataques tanto dentro como fuera del entorno laboral. (www.iso27000.es, 2008)

Por consiguiente, de acuerdo a lo anterior **a nivel internacional** se han implementado los siguientes casos:

En la ciudad de Madrid (España), el autor Cestero, desarrolló e implementó para la universidad politécnica de Madrid, una metodología de análisis y gestión de riesgos en sistemas de información, reguladas por las normativas internacionales de la serie ISO/IEC 27000, sugiriendo definir relaciones entre los activos del sistema, de modo que el ataque sobre uno de ellos se puede transmitir con cierta probabilidad a lo largo de toda la red, llegando a alcanzar a los activos más valiosos para la organización. (cestero, 2016)

Por otro lado, se realizó una consideración del valor de los activos, estableciendo indicadores de impacto y riesgo a partir de las variables objeto de estudio, tomando como metodología principal MAGERIT ya que está establecida para adoptar las normas ISO/IEC 27000, mediante la construcción de algoritmos que permiten establecer, bajo este tratamiento, los indicadores de impacto y riesgo para las amenazas que se ciernen sobre los activos de información. Así mismo, con el modelo resultante, los expertos valoraron las probabilidades de fallo, utilizando el diálogo

metódico con el analista, así como los valores de los activos y las probabilidades de materialización de las amenazas y la degradación. (Cestero, 2016)

Finalmente, se presentó un modelo de selección de salvaguardas de reducción de riesgos en los sistemas de información consistente en la reducción de las dependencias entre los activos de soporte y los activos terminales, minimizando costos, utilizando programación dinámica en ambiente borroso, de modo que los expertos pueden asignar probabilidades de transmisión de fallos de modo impreciso. Una vez reducidas las probabilidades de transmisión de fallos se seleccionaron las salvaguardas preventivas sobre los activos de soporte. (Cestero, metodología de análisis y gestión de riesgos en sistemas de información, 2016)

Por otro lado, el autor Pardo, presentó en la universidad de Castilla-La Mancha (España) un marco llamado HFramework, el cual fue diseñado para apoyar la armonización entre múltiples modelos y estándares de gestión de seguridad de la información en donde se observó, que, para tratar el tema de la calidad, se han desarrollado una variedad de modelos, estándares y metodologías para proporcionar soporte en diferentes dominios de la industria de TI. (Pardo, 2015)

Así mismo, la implementación e institucionalización de estos enfoques permitieron a las organizaciones para las que se implantó el marco, mejorar, madurar, adquirir e institucionalizar las mejores prácticas y sistemas de gestión, y los múltiples problemas y necesidades de muchas dimensiones y jerarquías organizacionales resueltas mediante el uso de diversos enfoques tales como COBIT, CMMI, ISO 9001, Risk IT, Val IT, ITIL, ISO 20000, ISO 90003, ISO 12207, ISO 27001, etc.

Además de lo anterior, los hallazgos obtenidos muestran que el marco de armonización permitió resolver los conflictos y las diferencias estructurales de los modelos involucrados, y ponerlos en consonancia entre sí de manera sistemática y con respecto a las necesidades de cada caso, brindando a las organizaciones que planean aplicar un enfoque multi modelo un marco útil que tenga en cuenta sus necesidades comerciales.

**A nivel nacional** se han implementado los siguientes casos:

En la ciudad de Tuluá (valle), el autor Bocanegra, presentó un análisis y gestión de riesgos de los sistemas de información de la alcaldía municipal de Tuluá aplicando la metodología Magerit, la cual define la gestión de riesgo en dos fases: La etapa de análisis y la etapa de tratamiento del riesgo, desarrollando de forma metódica tres actividades principales: la identificación de los activos, la identificación de las amenazas y la determinación de salvaguardas que disminuyan el riesgo. (bocanegra, 2016)

Igualmente, con la retrospectiva realizada por el autor, se determinó que la Alcaldía Municipal de Tuluá no contaba con un análisis metodológico para el análisis y tratamiento de riesgos informáticos, por lo cual el estudio fue de gran utilidad para la correcta identificación y gestión de riesgos. Así mismo, por medio de la aplicación de la metodología MAGERIT se logró llegar a una identificación acertada de las principales problemáticas existentes en materia de seguridad.

Paralelamente, como resultado del estudio se generó un documento que permitió dar inicio a la ejecución de un plan de seguridad que involucro a toda la entidad, estableciendo políticas de seguridad y una adecuada gestión de los riesgos impactando de forma positiva en la confiabilidad de los usuarios y la mejora de la imagen corporativa.

De la misma manera, el análisis y gestión de riesgos es un proceso esencial en la gobernabilidad de TI y su ejecución permitió a la Alcaldía de Tuluá dar cumplimiento al componente número 4 de la premisa Gobierno En Línea: Seguridad y privacidad de la Información - Implementación del plan de seguridad y privacidad de la información y de los sistemas de información - Gestión de riesgos de seguridad y privacidad de la información.

Por otro lado, el autor Pineda, presentó una auditoría a la seguridad del sistema de información “gestión integrada de bienestar social” en la dirección territorial de salud del Departamento de Caldas, permitiendo desarrollar actividades reales aplicadas a una problemática real que se presentó en una empresa pública que tiene entre sus principales objetivos la confidencialidad de la información, y por tal motivo permitió que se ejecuten las auditorías internas para brindar aprendizajes continuos. (Pineda, 2015)

En este orden de ideas, cabe señalar que en conjunto al sistema de gestión de seguridad de la información realizado en el departamento de caldas se realizó una auditoría de verificación y socialización en donde se plantearon pequeños problemas con soluciones favorables, en donde fueron expuestos los diversos inconvenientes como el caso de algunos funcionarios que, por falta

de tiempo, por falta de cultura o simplemente por miedo al cambio se opusieron a brindar información de gran importancia y relevancia.

En condición a lo anterior, la auditoría arrojó los resultados esperados por el grupo de trabajo que consistían en determinar las vulnerabilidades, amenazas y riesgos a que se encuentra expuesto el sistema desde el punto de vista de la seguridad informática, creando una carta en navegación en cuanto a actividades a desarrollar, tiempos y responsables con roles específicos de acuerdo a su relación con el aplicativo objeto de la auditoría.

En el municipio de Aguachica, los autores Didier Fernando Guerrero Sumalave, Andrea Johana Navarro Claro, Roger Oswaldo Lizcano Ruiz y Laura Marcela Felizzola Conde, realizaron un proyecto llamado Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar, Seccional Aguachica.

El objetivo primordial fue implementar medidas para salvaguardar la integridad, disponibilidad y confidencialidad de lainformación que se maneja permitiendo proteger el bien más importante para la institución educativa y así poder cumplir con los objetivos misionales. En se sentido los autores concluyeron que existen necesidade de índole documental, humano, de infraestructora y de formación para abordar un sistema de gestión de seguridad de la información en la Universidad Popular del Cesar, seccional Aguachica. Igualmente, determinaron elementos del estándar ISO 27001 que pudieron aplicar y la investigación concluyó que se debe iniciar a docmentar aquellos que correspondan a la fase de Planificación donde se incluye el Alcance de un Modelo de Seguridad y Privacidad de la información. (Guerrero D. F., 2019)

**A nivel regional y local** se han implementado los siguientes casos:

El autor Manuel Esteban Ureche Ospino, a través de la Universidad Nacional Abierta y a Distancia UNAD, realizó un proyecto llamado Diseño de políticas de seguridad informática basadas en la norta NTC-ISO-IEC 27001:2013 para la universidad de Cartagena, centro tutorial Mompox Bolívar en el año 2017. Este proyecto tuvo como propósito diseñar las políticas de seguridad informática para esta institución, teniendo en cuenta el anállisis de riesgos y vulnerabilidades, tomando como referencia la norma NTC-ISO-IEC 27001:2013 y garantizar la seguridad de la información de los recursos informáticos del Centro Tutorial de la Universidad en mención. El proyecto se apoyó en estudios realizados a los estudiantes de acuerdo a la información levantada, se utilizó estadística no probalística donde se evidenció que no existen políticas de seguridad que se aplicaran para ese centrol. (Guerrero, 2019)

En la ciudad de Barranquilla, en la universidad del norte, se desarrolló una metodología propuesta presentando una oportunidad para entender mejor los conceptos definidos en los estándares mencionados para gestión de riesgos dándole un enfoque a los riesgos tecnológicos. Esta metodología brindo un mapa de ruta para la aplicación del proceso de gestión de riesgos evitando los vacíos y ambigüedades, dando indicaciones sobre cómo llevar a cabo las acciones que se presentaban. De lo anterior, los planes de seguridad se enfatizaron en crear conciencia en seguridad para prevenir riesgos y buscar estrategias para obtener el apoyo de la alta dirección con el fin de cumplir con los objetivos y asegurar la información crítica, adicionalmente, la gestión adecuada de los riesgos permitió evitar en gran medida la ocurrencia de incidentes y con ello evitar la activación de planes de continuidad. (Uninorte, 2016)

Finalmente, es necesario resaltar que sin importar el ámbito en el que se encontraba la organización se requirió la aplicación de gestión de riesgos, para formalizar y ser de carácter irrelevante en la continuidad del entendimiento del negocio, radicando la disminución de pérdidas y perjuicios.

Así mismo, este sistema de gestión de seguridad de la información fue creado con el compromiso de concebir un modelo de seguimiento y apoyo en conjunto con los ejes misionales de la organización logrando tener una visión futurista de la mano con las tecnologías de la información y comunicación; en donde se infiere que, en el desarrollo de un Sistema de Gestión de Seguridad de la Información, se puede solucionar problemas tanto técnicos como tecnológicos en el presente y futuro de la organización, logrando establecer iniciativas para el fortalecimiento en el ámbito de la seguridad.

### *Marco conceptual*

A continuación, se referencian una serie de palabras desconocidas por parte de los investigadores de manera que a medida que se avanza en el estudio del caso, se estudiaban ampliando los conocimientos por parte de los autores.

**Activo:** se refiere a cualquier información o elemento relacionado con el tratamiento de la seguridad de la información (sistemas, soportes, edificios,  personas…) que tenga valor para la organización. (ISO/IEC 27000). (MINTIC, 2016)

**Amenazas:** causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000). (MINTIC, 2016)

**Análisis de Riesgo:** proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo (ISO/IEC 27000). (MINTIC, 2016)

**Auditoría de sistemas:** es la revisión que se dirige a evaluar los métodos y procedimientos de uso en una entidad, con el propósito de determinar si su diseño y aplicación son correctos; y comprobar el sistema de procesamiento de Información como parte de la evaluación de control interno; así como para identificar aspectos susceptibles de mejorarse o eliminarse. (Ecured, 2016)

**Autenticación:** provisión de una garantía de que una característica afirmada por una entidad es correcta. (ISO/IEC 27000:2013).

**Contraseña:** cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales. El sistema compara el código con una lista de contraseñas y usuarios autorizados. Si el código es correcto, el sistema permite el acceso en el nivel de seguridad aprobado para el propietario de la contraseña. (MINTIC, Guía de Seguridad de la Información para Mypimes, 2016)

**Evaluación de riesgo**: es el proceso de comparar un riesgo estimado contra criterios de riesgo dados. La finalidad es determinar la importancia del riesgo. (Guía ISO/IEC73:2002)

**Firewall:** es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

**Programa de captura de teclado o keylogger:** malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón. Su finalidad es intentar robar información personal, pues su funcionamiento generalmente es encubierta.

**SGSI Sistema de Gestión de Seguridad de la Información:** parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información (ISO 27001:2013).

### *2.2.Marco contextual*

El presente proyecto se llevó a cabo en las instalaciones de la empresa Ultraline Electrónica S.A.S. ubicada en Cra. 45 #60 -37, en la ciudad de Barranquilla. Se realizó el diseño del sistema de gestión de la seguridad de la información (SGSI) basado en el estándar ISO 27001. La oficina de Sistemas de la empresa, fue nombrada como el área que se tomó como muestra piloto del presente proyecto. Debido a que se hizo necesario conocer su entorno, a continuación, se describe brevemente la historia de la empresa Ultraline Electrónica S.A.S. y como a través del tiempo tuvo un crecimiento importante que permitió su posicionamiento de marca a nivel nacional.

### *2.2.1.Historia de Ultraline Electrónica S.A.S.*

Ultraline de la Costa S.A. fue comprada con recursos propios en el año 1999 por los esposos Catherine Sagbini Echávez y Carlos Julio Cuello Mendoza en la ciudad de Barranquilla. En ese entonces, la empresa solo tenía un proceso de producción y comercialización de tres artículos electrónicos: reguladores, elevadores de voltajes y estabilizadores. La empresa funcionaba en la Cra 54 No.44-93 oficina 3 en la ciudad de Barranquilla con 5 empleados directos.

Con el tiempo, la empresa amplió su capacidad de producción y la variedad de artículos como: protectores de neveras, inversores, fuentes reguladoras de poder, equipos electrónicos, extensiones, convertidores, transformadores de ailamientes, ups , baterías para ups, Cargadores de baterías equipos, reguladores de voltajes de mayor capacidad. Tanto fue su crecimiento, que la Gerencia decidió ampliar sus operaciones comprando un espacio más amplio que le permitiera expandir su administración. Fue ubicada en la Cra. 45 #60-37, donde en una casa con 240 mts cuadrados de construcción permitió organizar los diferentes procesos con mejor estructura y mayor comodidad para realizar de forma cabal, la estrategia administrativa.

El nombre de Ultraline de la Costa S.A., fue cambiado a Ultraline Electrónica S.A.S. y la variedad de los productos permitió no solo distribuirlos en Barranquilla, sino abrir mercados en ciudades como Cartagena, Valledupar, Santa Marta, Montería, Riohacha y Sincelejo.

Ultraline Electrónica S.A.S. es una empresa dedicada a la fabricación y comercialización de equipos de protección de voltajes para electrodomésticos, equipos de oficina, médicos e industriales.

### *2.3.Marco teórico*

Diseñar un Sistema de Gestión de Seguridad de la Información SGSI requirió ubicar el problema dentro de un conjunto de conocimientos de manera que permitiera orientar la búsqueda conceptualizando los términos que se utilizaron. A continuación, se estudiaron estos conceptos como parte de referencia de la investigación:

#### *2.3.1.De la Norma ISO 27001*

La Organización Internacional de Estandarización (ISO, por sus siglas en inglés) estableció la norma ISO 27001, que se emplea para la certificación de los sistemas de gestión de seguridad de la información en las organizaciones empresariales. La norma ISO 27001:2013 también se basa en otras como ISO/IEC 17799:2005, la serie ISO 13335, ISO/IEC TR 18044:2004 y las Directrices de la OCDE para sistemas y redes de seguridad de la información, que brindan orientación para implementar sistemas de seguridad de la información. (Esan, 2016)

La norma ISO 27001 tiene como principal objetivo proteger la confidencialidad, la integridad y la disponibilidad de la información en una organización. Lo consigue gracias a la investigación de cuáles pueden ser los problemas que pueden afectar a la información y después se debe definir qué hacer para evitar que estos problemas se produzcan. Está basada en la gestión de riesgos, es decir, investigar donde se encuentra los riesgos y tratarlos de manera sistemática. (https://www.pmg-ssi.com, 2016)

La ISO 27001 está alineada con otros sistemas de gestión, y apoya la implementación y

funcionamiento estable e integrado con normas de gestión relacionadas. Sus características más importantes son:

- Armonización con normas de sistemas de gestión como ISO 9001 y ISO 14001.
- Énfasis y continuo proceso de mejora de su sistema de gestión de seguridad de la información.
- Aclaración de requisitos para la documentación y archivos.
- Valoración de riesgos y procesos de gestión utilizando un modelo de proceso Plan, Do, Check, Act –PDCA (Planificar, Realizar, Controlar, Actuar). (dnvgl.es, 2014)

### *2.3.2.De la norma ISO 27002*

Esta norma trata de un conjunto de buenas prácticas para la Seguridad de la Información. Su propósito es describir 114 controles y 35 objetivos de control aplicables como las mejores prácticas en la gestión de la seguridad de la información.

Dentro de los 14 capítulos que contiene esta norma, se estudiaron los siguientes temas: políticas de seguridad de la información, organización de la seguridad de la información , seguridad relativa a los recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad de las operaciones, seguridad de las comunicaciones, adquisiciones, desarrollo y mantenimiento, relación de proveedores, gestión de incidentes de seguridad de la información, aspectos de seguridad de la información para la gestión de la continuidad del negocio y cumplimiento.

La ISO 27002 está enfocada para todo los tipos de empresas, independientemente del tipo y del tamaño de ella y se publicó originalmente como un cambio de nombre de la antigua norma ISO 17799 que estaban enfocadas como un código de prácticas de seguridad de la información.

Tabla No.1. Diferencias entre la norma ISO 27001 y la norma ISO 27002

| ISO 27001 | ISO 27002 |
|---|---|
| Establece requisitos. Si una organización desea certificar su SGSI, debe cumplir con todos los requisitos de la norma 27001 | Son las mejores prácticas que no son obligatorias. Una empresa no necesita cumplir con la norma ISO 27002 pero puede usarla como inspiración para implementar los requisitos de la norma ISO 27001 |
| Exige la realización de una evaluación de riesgo para cada control y de esta manera poder identificar si es necesario disminuir los riesgos. | No distingue entre los controles que son aplicables a una organización determinada y los que no son. |

Fuente: Autores,2019

### *2.4.Marco legal*

A continuación, se mencionan los documentos que fueron indispensables para la aplicación en el desarrollo del presente proyecto:

ISO /IEC 27000 : proporciona una visión general de los sistemas de gestión de la seguridad de la información (SGSI) y contiene:

- Introducción a los SGSI
- Una breve descripción del proceso de mejora continua (PHVA): planificar, hacer, revisa y actuar.
- Comprensión de términos y definiciones en uso en toda la familia de normas relativas a los SGSI.

ISO /IEC 27001 : Tecnología de la información, técnicas de seguridad, SGSI. Define los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un sistema de gestión de la seguridad de la información documentado en el contexto de los riesgos de una organización en general. Se especifican los requisitos para la aplicación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de las mismas. Esta norma es certificable. (AENOR, 2012)

ISO/IEC 27002: Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información. Establece directrices y principios generales para crear, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Contempla las mejores prácticas de objetivos de control y controles de dicha gestión. (AENOR, 2012)

Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. (Ley1581, 2012)

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones,

entre otras disposiciones. (MINTIC, https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009)

Ley 44 de 1993. Por la cual se reglamenta el Registro Nacional del Derecho de Autor y se regula el Depósito Legal. Ley N° 44 de 1993 (5 de febrero) modifica y adiciona la Ley N° 23 de 1982 y se modifica la Ley N° 29 de 1944. Mediante la adición de disposiciones y medidas especiales para el Registro Nacional del Derecho de Autor, las sociedades de gestión colectiva de derechos de autor y derechos conexos, sanciones y otros derecho. (innovacionUNAL, 2017)

# 3.Diseño metodológico

El diseño metodológico de una investigación puede ser descrito como el plan general que dicta lo que se realizará para responder a la pregunta de investigación. La clave para el diseño metodológico es encontrar la mejor solución para cada situación. (LIFEDER, s.f.)

En el presente proyecto, se aplicó un marco de referencia basado en la norma ISO/IEC 27001:2013 el cual especifica detalladamente los requerimientos y cada una de las actividades que se deben desarrollar para realizar un diseño de un sistema de gestión de seguridad de la información en Ultraline Electrónica S.A.S., como una empresa productora y comercializadora de artículos electrónicos.

También se utilizó el CICLO PHVA en la investigación que consiste en una metodología diseñada por la Organización Internacional de Estandarización (ISO) para el desarrollo de un sistema de gestión de seguridad de la información, el cual consiste en ciclo PHVA (Planear, Hacer, Verificar y Actuar).

Con base al objeto de estudio que permita establecer el diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001 para la empresa Ultraline Electrónica S.A.S., en la ciudad de Barranquilla; se requirió realizar una caracterización e identificación de todos los elementos que intervinieron y cuantificaron el tamaño de la problemática para proceder a alcanzar los objetivos propuestos en el presente proyecto.

El primer paso fue diagnosticar el estado de la seguridad de la información en la empresa y para ello, se requirió realizar una auditoría interna basada en la norma ISO 27001. Esta auditoría fue socializada con los miembros directivos de la empresa. Posterior a esa auditoría, se realizó un análisis documental de la normatividad para poder establecer el sistema de gestión de la seguridad de la información SGSI. Con base a las políticas desarrolladas en el SGSI, se realizaron actividades en la oficina de Sistemas con la finalidad de encontrar pruebas de aceptación y aplicabilidad en el interior de la organización.

En ese marco, la primera fase del presente proyecto estuvo enfocada en caracterizar el centro de estudio identificando los objetos que participan, describiendo todos los elementos que intervinieron e hicieron protagonismo, cuantificando la problemática y buscando un alcance de los objetivos que se propusieron a alcanzar en la realización del diseño de un sistema de gestión de seguridad de la información para la empresa Ultraline Electrónica S.A.S en la ciudad de Barranquilla.

Se realizó una auditoría de sistemas basada en la norma ISO 27001 que permitió diagnosticar el estado de la seguridad de la información de la empresa Ultraline Electrónica S.A.S. y se socializó a los miembros directivos de dicha empresa. Posteriormente se propuso realizar un análisis documental normativo de los procesos internos de la organización para identificar los elementos del estándar ISO 27001 que puedan ser aplicables.

Con base a lo anterior, se pudo documentar el Sistema de Gestión de Seguridad de la Información de Ultraline Electrónica S.A.S., lo cual fue uno de los documentos necesarios para establecer políticas de administración de la información.

La última fase del proyecto presente, consistió en tomar las políticas del sistema de gestión de la seguridad de la información (SGSI) y realizar actividades en la oficina de Sistemas, buscando siempre pruebas de aceptación y poder ser aplicadas en el interior de la organización.

### *3.1.Tipo de investigación*

En el presente proyecto se usó un tipo de investigación exploratoria, debido a que permitió tener un primer acercamiento al problema que se pretendía estudiar y conocer. Este tipo de investigación al usarla, generó un conocimiento superficial a la problemática y un panorama general como primer paso.

También se usó el tipo de investigación descriptiva porque logró descubrir y describir tendencias, características de un fenómeno, un sujeto y de una población. Es decir, únicamente pretendió medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refirieron, esto es, su objetivo no fue indicar cómo se relacionan éstas. (HernadezSampieri, 2010)

### *3.2.Población y Muestra*

Debido a que la población de estudio es cuantitativamente reducida por ser una empresa

categorizada pyme pequeña (20 trabajadores), se estableció la muestra a conveniencia con cada una de las áreas que manipulan información a una gran escala por los procesos que realizan, en este caso, producción maneja muy bajo volumen, y no se incluye. Por lo anterior, se seleccionaron cuatro áreas cuyo volumen de información es alto (Contable/financiera, Almacén, Sistemas y Gerencia Comercial).

### *3.3. Técnicas de recolección de la información*

#### *3.3.1. Fuentes primarias y secundarias*

La recolección de datos se refiere al uso de una gran diversidad de técnicas y herramientas que pueden ser utilizadas por el analista para desarrollar los sistemas de información, los cuales pueden ser la entrevistas, la encuesta, el cuestionario, la observación, el diagrama de flujo y el diccionario de datos. (TécnicasdeRecoleccióndeDatos, 2013) Todos estos instrumentos se aplicaron en un momento en particular, con la finalidad de buscar información que fue útil a una investigación en común. En la presente investigación se trataron con detalle los pasos que se debían seguir en el proceso de recolección de datos, con las técnicas ya antes nombradas.

Se utilizó la entrevista que consistió en una conversación dirigida y que se buscaba un propósito específico de conocimiento de un proceso en el interior de la empresa Ultraline Electrónica S.A.S. utilizando preguntas prediseñadas con el fin de tener respuestas definidas basadas en un diálogo amigable.

También se utilizó la observación directa, para lo cual los autores se desplazaron hacia la ciudad de Barranquilla en varias oportunidades y pudieron apreciar y participar en el actuar como espectador en las actividades llevadas a cabo por cada persona que participaba en la manipulación y uso de la información.

# 5. Resultados

## *5.1 Diagnóstico del estado de la seguridad de la información en la empresa Ultraline Electrónica S.A.S., Barranquilla.*

El diagnóstico del estado de la seguridad de la información en la empresa Ultraline Electrónica S.A.S, Barranquilla se realizó por medio de una auditoría interna, donde se determinaron los requisitos de las partes interesadas pertenecientes al area de seguridad de la información (NTC-ISO-IEC 27001), donde a se describen los siguientes resultados:

### *5.1.1 Contexto de la organización*

Ultraline Electrónica S.A.S., empresa dedicada a la fabricación y comercialización de equipos de protección de voltajes para electrodomésticos, equipos de oficina, médicos e industriales, llamada anteriormente Ultraline de la Costa S.A., es una empresa industrial tipo pyme, inscrita en la cámara de comercio de Barranquilla con NIT N° 9004116093 y cuya matrícula mercantil es 514719-03, con forma jurídica de sociedad por acciones simplificada, cuyas operaciones comerciales iniciaron en el año 1999. En este sentido, Ultraline Electrónica S.A.S. se dedica a producir y comercializar equipos electrónicos tipo reguladores, elevadores de voltajes, multitomas, protectores de neveras, inversores, convertidores, transformadores de aislamientos, ups, baterías para ups, cargadores de baterías, entre otros.

En este orden de ideas, la empresa Ultraline Electrónica S.A.S. se encuentra ubicada con su centro de operaciones en la ciudad de Barranquilla, en el departamento de Atlántico, con domicilio social en la carrera 45 N° 60-37 en el Barrio Boston. En este sentido, desde su fundación, los

procesos de Ultraline Electrónica S.A.S., fueron crecido de forma consistente obligando ampliar sus operaciones productivas, comerciales y administrativas posicionándose en un mercado dinámico y competitivo. Con esto, cabe mencionar que de 5 personas que iniciaron laborando y 15 clientes comercializando sus productos; hoy, 20 años después, se pueden calcular 250 clientes y 20 empleados directos. Por tanto, sus productos son conocidos en toda la Costa Atlántica de Colombia generando ingresos y recursos para muchas familias de la región norte colombiana.

### *5.1.2 Objetivos organizacionales*

La empresa Ultraline Electrónica S.A.S está comprometida a la mejora continua con su Sistema de Gestión Integral, por lo cual, se detallan los siguientes objetivos organizacionales:

1. *Proveer soluciones electrónicas para todo tipo de organización garantizando la satisfacción de los clientes.*
2. *Garantizar el Mejoramiento continuo y desempeño en Sistemas Integrados de Gestión*
3. *Garantizar un proceso de formación continuo al personal.*
4. *Fomentar la cultura de autocuidado y la seguridad para la prevención de incidentes, accidentes y enfermedades laborales.*
5. *Controlar impacto al medio ambiente, haciendo uso eficiente de los recursos naturales y asegurando una disposición adecuada de los residuos que generamos*
6. *Reducir el consumo de energía, reducir los costos financieros asociados*

### *5.1.3 Lineamientos Estratégicos*

**Visión**

"En el año 2020 Ultraline Electrónica S.A.S, será reconocida como líder en la fabricación, servicio y distribución de reguladores de voltaje y otros equipos electrónicos de protección y se consolidará

como una empresa competitiva, logrando exportación a gran escala." (http://www.ultralineelectronica.com/, 2015)

**Misión**

"Somos una Empresa dedicada a la fabricación y comercialización de equipos de protección de voltaje, para electrodomésticos, equipos de oficina, médicos e industriales. Con este propósito, brindamos a nuestros clientes y consumidores, máxima protección a sus equipos por altos y bajos voltajes, picos y ruidos en la red eléctrica, los cuales ocasionan daños o mal funcionamiento de estos." (http://www.ultralineelectronica.com/, 2015)

**Responsabilidades del Gerente**

La Gerencia de Ultrailine Electrónica S.A.S está comprometida con:

- *Mantener, revisar y mejorar el Sistema de Gestión integral de la empresa personalmente y/o a través de delegados debidamente autorizados.*
- *Proporcionar recursos y asignar el personal entrenado para garantizar el cumplimiento de los requisitos por parte de la empresa, verificando la prestación del servicio.*
- *Establecer y aplicar la Política integral en el desarrollo de todos los procesos de la organización.*
- *Apoyar todas las iniciativas, actividades y sugerencias para mantener el servicio que cumpla con las expectativas y especificaciones de los clientes.*
- *Responsabilidades del Líder del Sistema de Gestión Integral*
- *Incorporar los cambios autorizados por el Comité Integral.*
- *Controlar la publicación y distribución a los empleados autorizados.*
- *Actualizar permanentemente las copias controladas del manual.*

- *Archivar y mantener actualizado el original del manual.*

### *5.1.4.Politica Integral*

Ultraline Electrónica S.A.S., empresa dedicada a la fabricación y comercialización de equipos de protección de voltajes para electrodomésticos, equipos de oficina, médicos e industriales, está comprometida a la mejora continua de nuestro Sistema de Gestión Integral, mediante:

1. Prevención de lesiones y enfermedades, fomentando una cultura de auto cuidado y la seguridad como responsabilidad de todos.

2. Prevención contaminación al medio ambiente, identificando los aspectos y minimizando los impactos ambientales.

3. Aseguramiento de la disponibilidad de la información y los recursos necesarios para alcanzar los objetivos y metas.

4. Mejora de la eficiencia energética en sus procesos.

5. Cumplimiento con la legislación vigente aplicable y con otros requisitos que la organización suscriba para nuestro sistema de gestión. (http://www.ultralineelectronica.com/, 2015)

### *5.1.5.Mapa de procesos*

En el mapa de procesos, se describen los procesos de estratégicos, misionales y de apoyo de Ultraline Electrónica S.A.S con las interacciones existentes desde que se detectan las necesidades del cliente hasta que se satisfacen. Su obejtivo es facilitar el entendimiento por parte del personal involucrado sobre el concepto de cliente interno, el objetivo de cada proceso y las actividades principales de cada proceso.

Figura No.1.Caracterizaciones de los procesos (Interacción).


Fuente: Manual de Sistema de Gestión Integral Ultraline Electrónica. Recuperado Nov 2019

Tabla No.2. Procedimientos de Ultraline Electrónica S.A.S.

**RELACIÓN DE PROCEDIMIENTOS**

| | CODIGO | TITULO DEL DOCUMENTO |
|---|---|---|
| | MAN-GER-001 | MANUAL SISTEMA DE GESTIÓN INTEGRAL |
| PROCESOS ESTRATEGIOS | **GESTION GERENCIAL** | |
| | PRO-GER-003 | Planificacion del SGI |
| | PRO-GER-004 | Comunicacion interna y externa |
| | PRO-GER-005 | Revision por la direccion |
| | PRO-GER-006 | Reglamento interno ed trabajo |
| | PRO-GER-008 | Percepcion del cliente |
| | PRO-GER-010 | Seguimiento y medicion del SGI |
| | A-GER-001 | Direccionamiento Estrategico |
| | A-GER-002 | Mapa de procesos |
| | A-GER-003 | Caracterizacion de procesos |
| | A-GER-004 | Especificacion matriz gerencial |
| | A-GER-005 | Tablero comando integrado de indicadores de gestion |
| | **SISTEMA DE GESTION INTEGRAL** | |
| | PRO-GSI-001 | Elaboracion y control de documentos |
| | PRO-GSI-002 | Elaboracion y control de registros |
| | PRO-GSI-006 | No conformidades Acciones Correctivas, Preventivas y de Mejora. |
| | PRO-GSI-007 | Auditorías internas |
| | PRO-GSI-015 | Matriz de Aspectos e Impactos Ambientales |
| | PRO-GSI-016 | Proc. De Orden y Aseo |
| | PRO-GSI-018 | Identificacion de peligro, valoracion del riesgo y determinacion de controles |
| | PRO-GSI-019 | Reporte de Accidentes e Incidentes |
| | PRO-GSI-020 | Control Operacional SST |
| | PRO-GSI-021 | Control Operacional medio ambiente |
| | PRO-GSI-022 | Seleccion, uso y reposicion de los EPP |
| | PR-GSI-001 | Programa de ahorro de energia |
| | PR-GSI-002 | Programa de Ahorro de Agua |
| | PR-GSI-003 | Programa de MIRS |
| | PR-GSI-004 | Progrma Orden y Aseo |
| | PR-GSI-005 | Programa del SGI |
| | PR-GSI-006 | PVE Osteomuscular |
| | A-GSI-002 | Reglamento de higiene y seguridad |
| | A-GSI-003 | Politica de control de comportamiento de la via |
| | A-GSI-004 | Politica de conducta etica |
| | A-GSI-005 | Politica de prevencion del consumo de alcohol y droga |
| | A-GSI-006 | Politica generales de comoprtamiento en la cafeteria |
| | A-GSI-007 | Politica integral |
| | A-GSI-008 | Politica General del comportamiento de la oficina |

| | | |
|---|---|---|
| PROCESOS MISIONALES | **GESTION DE VENTAS** | |
| | PRO-GCM-001 | Gestion Comercial |
| | PRO-GCM-002 | Propiedades del cliente |
| | A-GCM-001 | Clasificacion del producto |
| | **GESTION DE COMPRAS** | |
| | PRO-GCP-001 | Compras, seleccion, evaluacion y reevaluacion |
| | **GESTION DE ALMACEN** | |
| | PRO-ALM-001 | Proc. De almacen y entrega |
| | PRO-ALM-002 | Control de calidad |
| | PRO-AL-09 | Control de produucto no conforme |
| PROCESOS DE APOYO | **GESTION HUMANA** | |
| | PRO-GTH-011 | Seleccion, contratacion y retiro de persoal |
| | PRO-GTH-012 | Realizacion y manejo de historias clinicas laborales |
| | PRO-GTH-013 | Capacitacion, entrenamiento, sensibilizacion y conscientizacion |
| | PRO-GTH-002 | Manual de funciones y perfiles de cargos |
| | **GESTION ADMINISTRATIVA** | |
| | PRO-GMT-001 | Mantenimiento preventivo y correctivo |
| | **GESTION ENERGETICA** | |
| | MAN-GEE-0001 | MANUAL SGEE |
| | PRO-GSI-017 | Revision energetica |

Fuente: Manual del Sistema de Gestión de Integral de Ultraline Electrónica S.A.S., Recuperado en noviembre de 2019

**Procesos Estratégicos de Ultraline Electrónica S.A.S.**

**Proceso Gerencial**

***Enfoque al cliente:*** la Gerencia se asegura de identificar y cumplir los requisitos del cliente con el propósito de aumentar su satisfacción a través del procedimiento: Percepción del Cliente PRO-GER-020

***Enfoque Basado en Procesos:*** Ultraline Electrónica S.A.S tiene establecido su Sistema de Gestión Integral (SGI) con base en un enfoque por procesos, donde son identificados los procesos que inciden en la calidad del servicio, mostrando su secuencia e interacción, describiendo los métodos necesarios para su control y seguimiento, la identificación de la necesidad de recursos y la

implementación de acciones para alcanzar los resultados planificados y la mejora continua de dichos procesos.

La metodología utilizada en Ultraline Electrónica S.A.S, para establecer el modelo de la calidad basado en procesos, se determina en cuatro etapas:

- La planificación de la Política y Objetivos, necesarias para atender las necesidades y requisitos de los clientes.

- La implementación de las actividades establecidas para cada uno de los procesos críticos identificados como incidentes en la calidad del servicio para lograr los resultados.

- La ejecución de seguimiento y medición de los procesos y análisis de la información de los resultados del mismo.

- La toma de acciones y decisiones necesarias para mejorar continuamente los procesos y resultados.

**Comunicación interna y externa.**

Uno de los puntos más importantes en el ambiente laboral es la comunicación interna y externa. Es la clave de la motivación y permite que el personal tenga una mayor fidelización hacia la empresa y un mayor compromiso. La Gerencia de Ultraline Electrónica S.A.S ha definido en

FOR-GER-008 una Matriz de comunicaciones Internas y Externas con el fin de mejorar los lazos de comunicación del SGI con el personal de la organización y las partes externas interesadas.

**Gestión de los recursos**

El Gerente define con los integrantes del Comité del SIG, los recursos necesarios para mantener y mejorar el Sistema y también para realizar el trabajo requerido de manera que se logre la satisfacción del cliente.

**Proceso de gestión integral**

Asegurar la conformidad y eficacia del Sistema de Gestión Integral, así como la mejora continua del mismo a través de la implementación y verificación de acciones preventivas y de mejora propia y de otros procesos.

Proceso que documenta, implementa y mantiene los Sistemas Integrados de Gestión, que incluye:

**Procesos Misionales**

**Ventas**

Proceso que debe garantizar que los requisitos relacionados con el servicio, los especificados por el cliente y los ofrecidos por la empresa son revisados previamente antes de asumir compromisos con este. PRO-GCM-001 Gestión Comercial

Durante el proceso de la venta la organización tendrá acceso a la información del cliente como son sus datos (NIT, direccion, teléfono, representante legal, etc) por lo que se considera propiedad del cliente y debe ser protegida dicha información para prevenir su uso o alteración de la misma. También se entiende por propiedad del cliente cualquier dinero entregado por el cliente antes de la entrega del producto o el producto comprado y pagado que sea guardado en la empresa hasta que el cliente lo reciba. Todo lo anterior se lleva de acuerdo al Procedimiento de Propiedad del cliente PRO-GCM-002 Propiedad del Cliente.

**Compras**

Proceso que ejecuta la selección, compra, evaluación y reevaluación de proveedores que suministran productos y servicios, cumpliendo los requisitos especificados por el cliente interno en cuanto a tiempo de entrega y control de los costos PRO-GCP-001 Compras, Selección, Evaluación y Reevaluación de Proveedores

**Almacén y entrega**

Proceso operativo responsable por asegurar la calidad del producto para la comercialización como son: reguladores de voltaje, elevadores de voltaje, multitomas, transformadores de voltaje, fuentes reguladas de poder, protectores de nevera, inversores, ups, entre otros. Este proceso cuenta con el procedimiento de Almacén y el Instructivo de Control de Calidad. Dentro del proceso se realizan el control del producto no conforme PRO-GER-009 Control Producto no conforme.

**Procesos Apoyo : Proceso de Gestión Humana**

El Procedimiento PRO-GTH-011 Selección, contratación y retiro de personal define las

políticas para seleccionar y contratar personal competente para cubrir las vacantes que se generen en los diferentes procesos de la organización. PRO-GTH-012 Realización y manejo de historias clínicas se definen las directrices para la realización de la evaluación médica ocupacional de ingreso, periódica y de retiro. PRO-GTH-013 Capacitación, entrenamiento, sensibilización y concientización. Se describe la metodología con la cual se detecta la necesidad y se brinda capacitación y entrenamiento.

**Gestión Administrativa**

El Proceso Administrativo es el responsable por la realización de las actividades de Mantenimiento de la Infraestructura, el cual se realiza de acuerdo al Cronograma de Mantenimiento, los procesos contables y financieros de la organización, así como servicios generales o cafetería.

**Eficiencia Energética**

El proceso de Eficiencia Energética da respuesta a las necesidades de la NTC ISO 50001, de acuerdo al nivel de consumo e impacto de la organización. Se establece, documenta, implementa, mantiene y mejora de acuerdo al Manual de Eficiencia Energética MAN-GEE-001.

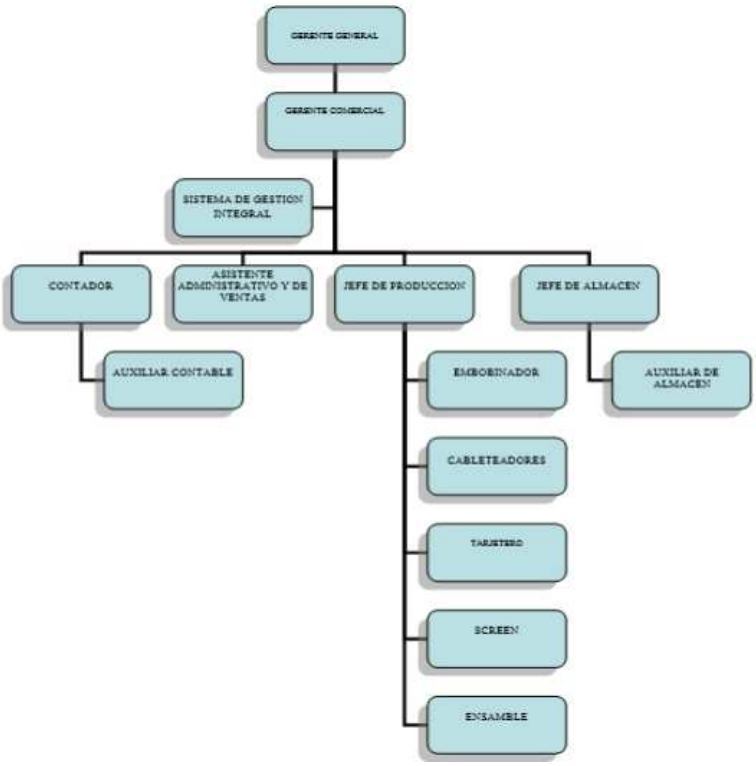
### *5.1.6.Estructura administrativa*

La estructura administrativa es el sistema de relaciones formales que se establecen en el interior de una organización/empresa para que este alcance sus objetivos de conservación, productivos y económicos. Esta estructura le permite a la empresa lograr una determinada

disposición de sus recursos, facilitando la realización de las actividades y la coordinación de su funcionamiento. Y es así como puede realizar el esfuerzo coordinado que la lleve a la realización de sus objetivos, definiendo relaciones y aspectos estables. (Minuto de Dios, 2015)

En el caso de Ultraline Electrónica, su estructura está determinada por un organigrama general con representación vertical donde representa su orden jerárquico y solo da a conocer el cargo, así:

Figura No.2 Organigrama Ultraline Electrónica.




Fuente: Manual de Gestión Integral de Ultraline Electrónica. Recuperado nov 2019

### *5.1.7. Infraestructura tecnológica de la empresa Ultraline Electrónica S.A.S.*

Una infraestructura tecnológica se podría definir como el conjunto de elementos para el almacenamiento de los datos de una empresa. En ella se incluye el hardware, el software y los diferentes servicios necesarios para optimizar la gestión interna y seguridad de información. (www.vegagestion.es, 2015)

La empresa Ultraline Electrónica S.A.S cuenta con una buena infraestructura tecnológica de acuerdo a sus requerimientos. Cuenta con tres nodos establecidos en puntos estratégicos de forma que se pueda tener conexión con todas las dependencias de la empresa, estos nodos estan orientados en la siguiente forma:

Tabla No.3. Infraestructura tecnológica Ultraline Electrónica S.A.S.

**Departamento de sistemas**

| Elemento | Características |
|---|---|
| Topología de red física | Estrella extendida |
| Router | Cisco Catalist 2960 |
| Ubicación | Departamento de sistemas |
| Tipo de rack | Armario Bastidor 30 ru |

**Gerencia**

| Elemento | Características |
|---|---|
| Topología de red física | Estrella extendida |
| Router | Cisco Catalist 2960 |
| Ubicación | Gerencia |

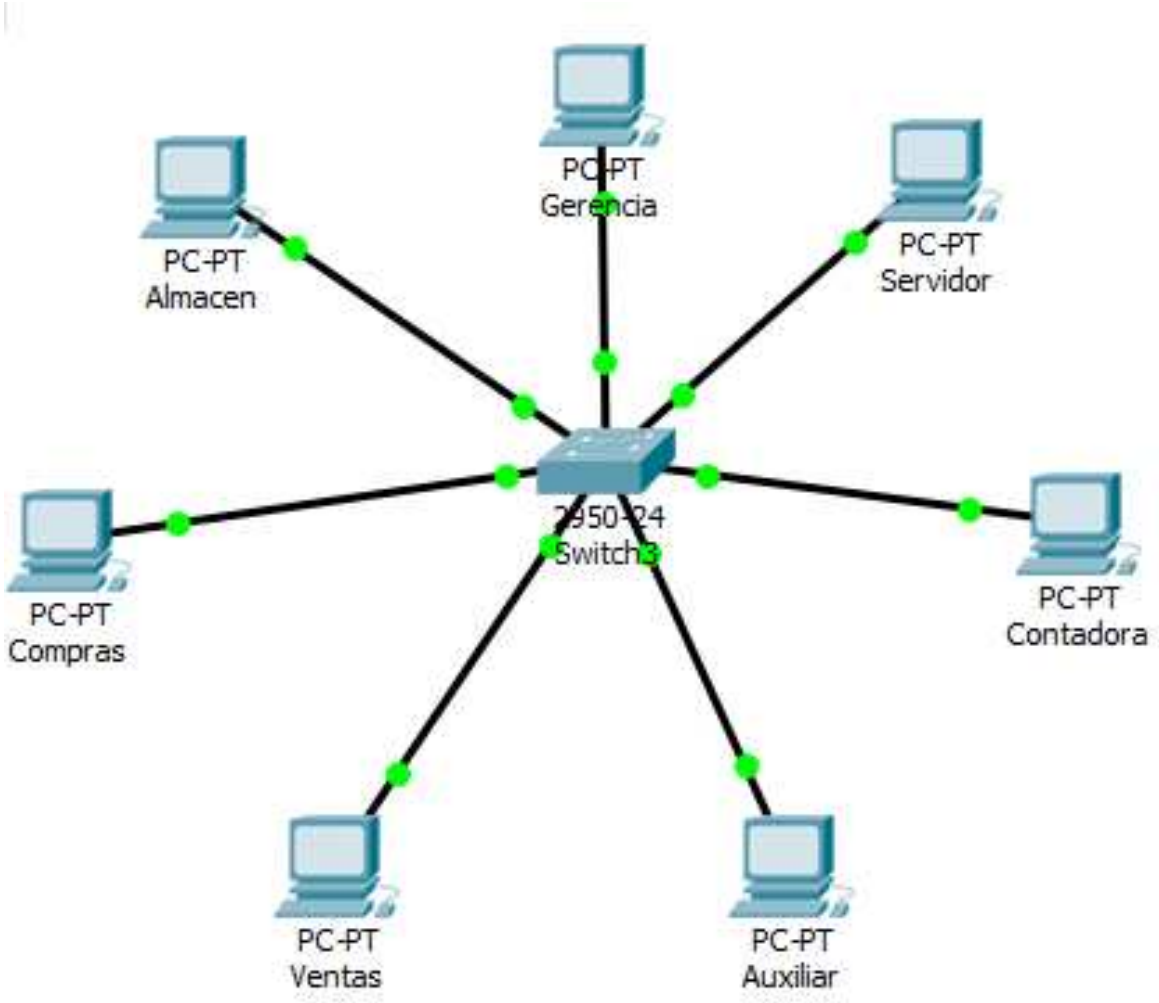
**Secretaria**

| Elemento | Características |
|---|---|
| Topología de red física | Estrella extendida |
| Router | Cisco Catalist 2960 |
| Ubicación | Secretaria |

Fuente: Autores, 2019

### *5.1.7.1 Esquema lógico de red*

Figura No.3 Esquema lógico de la red de Ultraline Electrónica




Fuente: Autores, 2019

#### *5.1.7.1.2. Sistemas de información utilizado por la empresa Ultraline electrónica S.A.S*

Tabla No.4. Sistema de Información utilizado en Ultraline Electrónica.

| Sistema de información | Descripción |
|---|---|
| Sistema Integrado Contable (SIC) | El sistema de información llamado Sistema Integrado Contable (SIC). creado especialmente para facilitarte la captura, proceso y mantenimiento de la información contable de la empresa. También te permite la generación de diversos reportes financieros, indispensables para la toma de decisiones: maneja Contabilidad, Inventarios y Nómina. |

Fuente: Autores,2019

*5.1.7.1.3.Servidores*

Tabla No.5. Servidor Utilizado en Ultraline Electrónica.

| Servidor | Función | Referencia | Sistema operativo |
|---|---|---|---|
| Hp server | Administra la red y ofrece el acceso compartido entre los equipos de cada una de las dependencias | ML110 G6 | Windows server 2008 Foundation |

Fuente: Autores, 2019

### *5.1.8.Informe de Auditoría*

Con el fin de diagnosticar el estado de la seguridad de la información en la empresa Ultraline Electrónica S.A.S y conocer el impacto tanto de sus amenazas como de sus vulnerabilidades, se procedió a realizar una auditoría interna de gestión con base en los estándares y requisitos establecidos por la normativa ISO 27001, obteniendo los siguientes resultados:

#### *Objetivo de la auditoría*

Determinar el estado en que se encuentra la protección de la información dentro de la organización Ultraline Electróncia S.A.S, involucrando la identificacion, análisis y evaluación de debilidades en los activos y los controles de seguridad aplicados.

#### *Objetivos Específicos*

- Identificar las insuficiencias presentadas en la organización en el contexto de la gestión de seguridad de la información.
- Establecer posibles causas, efectos, y soluciones potenciales para establecer un análisis completo y detallado de la información.

- Detallar las actividades de control.
- Emplear un enfoque sistémico para planificar, implementar, gestionar y monitorizar la seguridad de la información en la empresa Ultraline electrónica S.A.S.

***Alcance de la auditoría***

El alcance viene dado por la normativa ISO 27001 que indica de forma detallada, la manera de manejar eficientemente la seguridad de la información indicando la alineación de los objetivos de negocio de una organización y su evaluación paulatina para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Asi mismo, se evaluará la gestión de seguridad de la información de la organización, por lo que puede estar definido en términos de los activos de información, la ubicación física, la seguridad lógica, las unidades organizacionales, las actividades o procesos de mayor relevancia para la empresa. La principal intención es dejar en claro todo lo que es de interés para el sistema de gestión, relacionándose con las actividades esenciales que permitan cumplir con los ejes misionales y los objetivos generales de la organización.

Se examinará si la empresa tiene un sistema para la comprobación y reparación de errores. La idea es verificar si la enmienda de manera eficiente garantizando de esta forma la integridad de la información.

Para la elaboración de esta auditoría se evidenciaron limitantes como la distancia entre el equipo de trabajo de los auditores y la empresa. Igualmente, el poco tiempo para la realización de

la auditoría exhaustiva y la disponibilidad del personal para recibir a los auditores que labora en la empresa.

Por tanto, para los efectos del diagnóstico presentado en esta auditoría se evaluaron (11) procedimientos del sistema de gestión para la empresa Ultraline Electrónica S.A.S., de acuerdo a las actividades o funciones a evaluar relacionadas en la siguiente tabla:

Tabla No.6. Actividades que se evaluaron en la auditoría de Ultraline Electrónica S.A.S.

| Ultra Line | **ACTIVIDADES QUE SE EVALUARON EN LA AUDITORÍA** | | | |
|---|---|---|---|---|
| **Referencia** | **Actividad o función a evaluar** | **Técnica de evaluación** | **Calificación** | **Observación** |
| A.1 | Identificar el grado de uso de políticas de seguridad | | | |
| A.2 | Identificar el conocimiento sobre seguridad de la información en los empleados de la empresa Ultraline S.A.S | | | |
| A.3 | Seguridad Física y Ambienal | | | |
| A.4 | Control de accesos | | | |
| A.5 | Seguridad en redes y telecomunicaciones | | | |
| A.6 | Compra, desarrollo y mantenimiento en los sistemas de información | | | |
| A.7 | Administración y gestión de los activos presentes | | | |
| A.8 | Identificar la seguridad con respecto a recursos humanos | | | |
| A.9 | Aspectos de seguridad de la información con respecto a la continuidad del proceso | | | |
| A.10 | Gestión de problemas de seguridad de la información | | | |
| A.11 | Identificar el conocimiento sobre seguridad de la información en los empleados de la empresa Ultraline Electrónica S.A.S | | | |

Fuente: Autores, 2019

***Actores auditados***

La auditoría se realizó con la totalidad de los funcionarios que laboran en la empresa Ultraline Electrónica S.A.S., alcanzando un total de 20 empleados directos. A continuación, se dan a conocer los lineamientos que fueron utilizados para la realización de la uditoría.

Tabla No.7. Plan general de auditoría.

| UltraLine | | | PLAN GENERAL DE AUDITORÍA | | |
|---|---|---|---|---|---|
| **Etapa** | **Descripcion** | **Actividad a desarrollar** | **Participantes** | **Periódo estimado** | |
| | | | | inicio | Fin |
| 1 | Identificar la actividad que desarrolla la organización, mediante un estudio preliminar o toma de contacto, donde se investiguen su estructura, su actividad económica, sus lineamientos estratégicos y los servicios que presta, con la finalidad de realizar una auditoría apropiada. | Visitar las áreas que serán auditadas | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Verificar el manual de funciones, procesos y estructura de la organización. | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Determinar el alcance y objetivos de la auditoría | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Elegir las técnicas y métodos de recolección de información | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Realizar y hacer entrega a la organización el acta de inicio o apertura de la auditoría | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| 2 | Ejecutar cada una de las herramientas que se van a utilizar para el proceso de la auditoría | Efectuar las encuestas | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Llevar a cabo la aplicación de las listas de chequeo | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Realizar las pruebas que sean necesarias para el proceso | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| 3 | En esta etapa se aplica la verificación de la información captada en la organización y se da a conocer las situaciones encontradas, se entrega el dictamen y las recomendaciones necesarias | Identificar las situaciones relevantes | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Socializar los hallazgos encontrados en la empresa | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |
| | | Elaborar el dictamen final. Presentación del informe final a las partes interesadas | Jefferson Farelo Jenis Sagbini | 15-11-2019 | 20-11-2019 |

Fuente: Autores, 2019

Tabla No.8. Guía de auditoría fase de investigación preliminar.

| UltraLine | | | Fecha inicial | | | Fecha final | | |
|---|---|---|---|---|---|---|---|---|
| | | | día | mes | año | día | Mes | año |
| | | | 15 | 11 | 2019 | 20 | 11 | 2019 |
| **Referencia** | **Actividad o función a evaluar** | **Técnica de evaluación** | **Calificación** | | | **Observaciones** | | |
| 1 | Visita preliminar o toma de contacto en la empresa a auditar | Observación | Apropiado | | | Se hicieron fotos y video de las instalaciones | | |
| 2 | Identificar la estructura organizacional de la empresa Ultraline Electrónica S.A.S en conjunto con las funciones de cada empleado. | Verificar la documentación de la empresa, en este caso serían sus objetivos misionales, manual de funciones y procedimientos, estructura organizacional, inventarios e infraestructura lógica y física | Mejorable | | | Se evidenciaron carencia de algunos documentos | | |
| 3 | Plantear los objetivos y el alcance de la auditoría | Documentacion auditoría | Apropiado | | | | | |
| 4 | Establecer los lineamientos, personas y dependencias a auditar | Observación directa y documentacion | Apropiado | | | | | |
| 5 | Diseñar los documentos para la recolección de información | Documentacion | Mejorable | | | | | |
| 6 | Entrega del acta de inicio de la auditoría a la gerencia de la organización. | | Apropiado | | | | | |

Fuente. Autores del proyecto, 2019

Tabla No.9 Guía de auditoría fase dictamen de la auditoría.

| UltraLine | | | Fecha inicial | | | Fecha final | | |
|---|---|---|---|---|---|---|---|---|
| | | | día | mes | año | día | Mes | año |
| | | | 15 | 11 | 2019 | 20 | 11 | 2019 |
| **Referencia** | **Actividad o función a evaluar** | **Técnica de evaluación** | **Calificación** | | | **Observaciones** | | |
| 1 | Recopilar y agrupar la información recolectada para examinar las situaciones o problemáticas encontradas. | Documentación | Mejorable | | | | | |
| 2 | Reunir al equipo de auditoría y el personal auditado para comentar las situaciones encontradas y determinar las posibles causas y sus soluciones | Reunión, documentación | Apropiado | | | | | |
| 3 | Redactar el dictamen final | Documentación | Apropiado | | | | | |
| 4 | Realizar una reunión con el Gerente General de la organización y presentar el informe final | Reunión | Apropiado | | | | | |

Fuente: Autores del proyecto, 2019

***Instrumentos de Recolección de Información.***

Para la recolección de información se diseñaron dos tipos de encuesta tipo entrevista abierta, orientadas a diferentes actores, entre ellos participaron el equipo administrativo, y el encargado del area de sistemas. Todas las encuestas fueron de tipo oral y escrito, buscando obtener información de percepción. Ver Apice

**Dictamen**

Dentro de los principales hallazgos se identificaron los siguientes:

- No se encuentran políticas adecuadas para el tema de seguridad de la información y el tratamiento de información confidencial.
- Malos manejos de almacenamiento de información en medios magnéticos en diferentes áreas o dependencias de la organización.
- No se cuenta con un manual de gestión de seguridad de la información aprobado e implementado.
- Falta de buenas prácticas en el uso de contraseñas de acceso para los equipos y sistema de información SIC (Sistema integrado contable) en las distintas dependencias de la empresa.
- Ausencia de un programa adecuado de copias de seguridad y restauración de información.
- Uso de datos personales en contraseñas para acceso a equipos de cómputo y sistema de información SIC (Sistema integrado contable).
- Ausencia de controles de seguridad tanto físicos como lógicos para la entrada de personas no autorizadas en la información de la empresa.
- No existen criterios de acción o políticas de seguridad en las áreas de acción operativa en la empresa.
- No existen controles de autenticidad en los equipos de la empresa.
- No existen controles de organización y planificación en cuanto a la restricción de formatos importantes en la organización.
- La empresa Ultraline electrónica S.A.S no cuenta con una oficina de control interno que garantice que se estan cumpliendo las labores del manual de funciones de manera adecuada.
- Los empleados de la empresa Ultraline electrónica S.A.S no tiene claridad en cuanto a la instalación de software no licenciado y de uso prohibido.

- La empresa Ultraline electrónica S.A.S no maneja una documentacion de control para el registro de las actividades en la red de datos, fallas en servicios, entre otros puntos relacionados con el alto consumo de red.
- La empresa Ultraline electrónica S.A.S no ha realizado una auditoría de redes incluyendo el cableado estructurado ni certificación con normatividad de puntos.
- La empresa Ultraline electrónica S.A.S no ha realizado una auditoría en sus bases de datos.
- La empresa no cuenta con controles preventivos ni detectivos en cuanto al control de acceso de personal.
- No existen controles de acceso al Rack de comunicaciones. Este se encuentra en una zona abierta a todos los funcionarios de la compañía.
- La empresa no cuenta con políticas y controles de protección de activos.
- La empresa Ultraline electrónica S.A.S no cuenta con controles y políticas de eficiencia que aseguren la optimización de sus recursos.
- La empresa Ultraline electrónica S.A.S no cuenta con guías de proceso en la toma de decisiones para la omisión de registros en sus bases de datos.
- La empresa Ultraline electrónica S.A.S no cuenta con políticas de aseguramiento en coherencia de datos.
- No se cuenta con un plan de contingencias en caso de un evento o desastre natural.
- Los equipos de la empresa Ultraline electrónica S.A.S no cuentan con antivirus licenciado, se encuentran con la protección de Windows Defender el cual viene incorporado en el sistema operativo.
- La empresa no cuenta con herramienta de control para el uso, aplicación y restricción de código malicioso.

- La gerencia no recibe notificaciones de ingreso de terceros en áreas restringidas de la empresa.
- No existen controles ni políticas de detección de malware y Ransomware dentro de la empresa Ultraline electrónica S.A.S.
- Falta de entrenamiento y capacitación de los empleados sobre seguridad de la información y protección de datos.
- En el transcurso de la auditoría se observó en distintas ocasiones que no se solicita carnet de entrada o las credenciales adecuadas para el ingreso del personal a la organización.
- Dentro de la empresa Ultraline electrónica S.A.S no existe un método de cifrado para la información de tipo confidencial o de alto riesgo.
- No existen políticas de control de riesgo para mitigar accidentes en la zona operativa de la empresa.
- Falta de políticas de ingreso y subcontratación de terceros en la organización.
- En la entrada de la empresa Ultraline electrónica S.A.S. no se realiza una inspección de los posibles dispositivos electrónicos que ingresan el equipo de trabajo.

### *Oficio de entrega del dictamen*

Una vez realizada la auditoría y la preparación del informe, se procedió a la entrega de los dictámenes a la gerencia de la empresa Ultraline Electrónica S.A.S., con el fin de socializar los resultados encontrados, por lo tanto, se realizó un oficio de entrega de resultados el cual se encuentra en el Anexo C. Informe Final de la Auditoría.

### *5.2.Elementos del estándar ISO 27001 aplicables a la empresa Ultraline Electrónica S.A.S.*

En la investigación realizada en el punto de inicio de la auditoría y teniendo en cuenta los aspectos presentados en el contexto organizacional de la empresa Ultraline electrónica S.A.S, como son: sus procesos internos, su estructura funcional, sus objetivos misionales y las diferentes áreas que la componen, se puede identificar que el mayor contenido de información está situado en las áreas Administrativa, Almacén-inventarios y Contabilidad-Finanzas. Por tanto, se debe tener presente que, al hablar de una infraestructura tanto empresarial como tecnológica, toca relacionar cada aspecto concerniente a ella e involucrar cada actor de la organización, transformando cada necesidad encontrada en una posible fuente de información.

En este orden de ideas, de acuerdo al primer capítulo del estándar ISO 27001, objeto y campo de aplicación que reza "*Esta norma, especifica los requisitos para Establecer, Implementar, Mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización*" (ISO/IEC 27001, 2013) Pag. 1. Con esto, se puede evidenciar el marco fundamental que contiene el ciclo P.H.V.A. (Planificar, Hacer, Verificar, Actuar) el cual es el punto de inicio para determinar las fases de planificación, ejecución, verificación y mejoras del proceso.

Por tanto, como segunda medida se debe establecer cuales elementos pertenecientes al estándar ISO 27001, son aptos para ser aplicados en la empresa Ultraline Electrónica S.A.S.; con esto, se logró identificar que la organización no cuenta con alguna herramienta que permita garantizar el estado actual de la seguridad de la información, lo que indica que se debe iniciar con

un proceso de conceptualización y diseño del mismo, como fase preliminar en el proceso de implantación del sistema de gestión de seguridad de la información. (J, 2011)

### *5.2.1 Elementos de identificación de la línea base de seguridad de la información*

A continuacion, se encuentran relacionados el resumen de los resultados de la evaluación de controles y la evaluación del modelo según el ciclo P.H.V.A.

Tabla No.10. Elementos del componente de planificación

| N° | Dominio | Calificación actual | Calificación objetivo | Evaluación de efectividad del control |
|---|---|---|---|---|
| A.5 | Políticas de seguridad de la información | 0 | 100 | Inexistente |
| A.6 | Organización de la seguridad de la información | 12 | 100 | Inicial |
| A.7 | Seguridad en el area de recursos humanos | 0 | 100 | Inexistente |
| A.8 | Gestión de activos | 32 | 100 | Repetible |
| A.9 | Control de acceso y autenticidad | 5 | 100 | Inicial |
| A.10 | Criptografía | 0 | 100 | Inexistente |
| A.11 | Seguridad Física y del Entorno | 20 | 100 | Inicial |
| A.12 | Control de Seguridad de las operaciones | 11 | 100 | Inicial |
| A.13 | Seguridad de las comunicaciones | 14 | 100 | Inicial |
| A.14 | Adquisición desarrollo y mantenimientos de sistemas | 5 | 100 | Inicial |
| A.15 | Relaciones con los proveedores. | 0 | 100 | Inexistente |
| A.16 | Gestión de incidentes de seguridad de la información | 0 | 100 | Inexistentes |
| A.17 | Aspectos de seguridad de la información de la gestión de continuidad del proceso | 10 | 100 | Inicial |
| A.18 | Cumplimiento | 36,5 | 100 | Repetible |
| | Promedio evaluación de controles | 10 | 100 | Inicial |

Fuente: Autores, 2019

### *5.2.2 Elementos del componente de planificación aplicables a la empresa Ultraline electrónica S.A.S.*

Teniendo en cuenta lo anterior, el punto de partida del sistema de gestión de seguridad de la información se encuentra en su etapa de inicio, lo que indica la utilización de los siguientes componentes de planificación, los cuales son aplicables a la empresa Ultraline Electrónica S.A.S.

- Alcance del Modelo de Seguridad y Privacidad de la Información (MSPI): En este punto se deben establecer los límites y la aplicabilidad del sistema de gestión de seguridad de la información, lo que implica la determinación de su alcance.
- Políticas de Seguridad y Privacidad de la Información: Se debe establecer el conjunto de políticas que abarquen la seguridad de la información, las cuales deben ser aprobadas y publicadas por la gerencia de la empresa y comunicadas a los empleados y partes interesadas.
- Procedimientos de control documental del Modelo de Seguridad y Privacidad de la información: La información documentada en la etapa de planificación debe ser controlada.
- Roles y Responsabilidades para la gestión de la seguridad de la información: Para este enciso se debe concretar de manera específica todos los roles y responsabilidades de la seguridad de la información.
- Inventario de Activos: involucra la identificacion de cada uno de los activos que presenten acceso a la información, por tanto, se debe elaborar un inventario de los activos pertenecientes a la organización.
- Identificación y valoración de riesgos: Se debe aplicar la metodología de análisis y valoración de riesgos, determinando el informe de análisis de riesgos.
- Formación en seguridad de la información: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada incluyendo actualizaciones regulares sobre las políticas y procedimientos pertinente para su cargo. (MINTIC.GOV.CO, 2017)

### *5.3. Establecimiento del sistema de gestión de la seguridad de la información (SGSI) para la empresa Ultraline electrónica S.A.S.*

Para la empresa Ultraline electrónica S.A.S, es necesario implementar una estrategia organizacional que contribuya al fortalecimiento de la seguridad de la información, lo que establece un compromiso entre la organización y todas las partes interesadas, logrando el cumplimiento de sus objetivos misionales, por tanto, se establece una política de seguridad de la información que proporcione los elementos necesarios para una adecuada gestión de la misma.

Por consiguiente, se presenta a continuacion el contenido del sistema de gestión de seguridad de la información para Ultraline Electrónica S.A.S.:

Figura No.4. Contenido del SGSI de Ultraline Electrónica SAS


Fuente: Autores, 2019

### *5.3.1. Objetivos*

Construir una estrategia para la futura implementación, mantenimiento y mejora continua de la información, utilizando los elementos del componente de planificación del sistema de gestión de seguridad de la información en la empresa Ultraline Electrónica S.A.S.

### *5.3.2.Alcance*

Por ser una empresa industrial tipo pyme, en Ultraline electrónica S.A.S se aplican todas estas directrices en el marco de toda la organización implicando sus funcionarios, contratistas y todas sus dependencias.

### *5.3.3.Declaración de la política de seguridad de la información*

La siguiente política de seguridad de la información fue realizada para la empresa Ultraline Electrónica S.A.S., teniendo como base el modelo de política general de seguridad y privacidad de la información, el cual fue proporcionado por el Min Tic (MinTic, 2016):

Entendiendo la importancia de una adecuada gestión de seguridad de la información, Ultraline electrónica S.A.S., se ha comprometido con la implementación de un sistema de gestión de seguridad de la información, con el fin de establecer un marco de confianza en el ejercicio de sus deberes y sus lineamientos estratégicos y funcionales, cumpliendo con la normativa y en la protección de la información. Ultraline Electrónica S.A.S. busca una disminución del impacto generado sobre sus activos identificando los riesgos de forma sistemática con el objeto de mantener un nivel de exposición que permita responder por la disponibilidad, la integridad y la confidencialidad de la misma, de acuerdo a las necesidades que manejan los distintos grupos de

interés. Teniendo en cuenta lo anterior, el desarrollo de esta política se aplica en la entidad según como está definido el alcance, su capital humano, sus cliente y proveedores en general, por tanto, tomando en cuenta los principios sobre los que se encuentra basada la toma de decisiones en cuanto al sistema de gestión de seguridad de la información, se estarán utilizando las siguientes condiciones:

- Minimizar los riesgos en las funciones más importantes de la organización.
- Cumplir con los principios establecidos en la seguridad de la información.
- Cumplir con los principios establecidos en la función administrativa organizacional
- Mantener la confianza de sus clientes, proveedores y empleados.
- Proteger sus activos tecnológicos.
- Establecer manuales, políticas y procedimientos que abarquen la seguridad de la información.
- Establecer y fortificar una cultura de seguridad de la información en los funcionarios de la organización.
- Garantizar la continuidad de los procesos frente a eventualidades e incidentes.
- La empresa Ultraline electrónica S.A.S., como organización del sector industrial, ha decidido concretar, implementar, operar y mejorar de forma continua la seguridad de su información la cual se encuentra soportada bajo los lineamientos y requerimientos regulatorios los cuales se ajustan a las necesidades de cada uno de sus procesos. (LAURA FELIZZOLA, 2012)

En este contexto, se establecen los 12 principios de seguridad que soportan el sistema de gestión de seguridad de la información (SGSI) de la empresa Ultraline electrónica S.A.S.:

- Todas las responsabilidades que ocasiona el manejo de la seguridad de la información serán precisadas, socializadas, publicadas y aceptadas por todos los empleados, clientes, proveedores y terceros que tienen de manera directa o indirecta una relación con la organización.

- Ultraline electrónica S.A.S., protegerá la información generada, procesada y asegurada por cada uno de los procesos que se generen en su infraestructura tanto física como tecnológica y en sus activos de riesgo, los cuales pueden otorgar algún acceso a terceros o en su defecto un servicio interno en outsourcing.

- Ultraline electrónica S.A.S., protegerá la información generada, procesada y asegurada por cada uno de los procesos que se generen con el fin de minimizar algun impacto operativo, financiero o legal, que impliquen el uso indebido de la información. Para esto, es necesario la aplicación de controles tanto preventivos como correctivos de conformidad a la clasificación que se le otorgue a la información.

- Ultraline electrónica S.A.S, protegerá su información de las amenazas ocasionadas por parte del personal de la empresa.

- Ultraline electrónica S.A.S, protegerá su infraestructura tanto física como tecnológica que

soporte cada uno de sus procesos críticos.

- Ultraline electrónica S.A.S, controlará la operación de cada uno de sus procesos garantizando la seguridad de sus recursos tecnológicos.

- Ultraline electrónica S.A.S, implementara controles de acceso a la información, sistemas y recursos tecnológicos.

- Ultraline electrónica S.A.S, garantizara que la seguridad de la información sea parte integral del ciclo de vida de los sistemas de información.

- Ultraline electrónica S.A.S, certificara a través de una adecuada gestión una mejora efectiva de su modelo de seguridad en cuanto a eventos de seguridad y debilidades asociadas con los sistemas de información.

- Ultraline electrónica S.A.S, garantizara la disponibilidad y la continuidad tanto de sus procesos como de sus operaciones basado en el impacto que pueda ocasionar alguna eventualidad.

- Ultraline electrónica S.A.S, garantizara el cumplimiento de las obligaciones legales, contractuales y regulatorias establecidas dentro de la organización.

### *5.3.4. Roles y Responsabilidades*

Los **roles** en una organización también están relacionados con el **estatus**, ya que el empleado dentro de la empresa no sólo asume unos roles que tienen que ver con los asuntos que le competen, sino que también tienen un cierto estatus dentro de la empresa que es la que determina la jerarquía interna en la propia empresa. Los empleados asumen roles también en función de su estatus. Un empleado no puede tener en ningún momento el rol de jefe de manera que ordene a alguno de sus compañeros porque para eso está el jefe y porque esto desharía el equilibrio interno dentro de la empresa. (https://www.gestion.org/la-importancia-del-test-psicometrico-pda/, 2019)

En Ultraline, la Gerencia General es la encargada de establecer, implementar, mantener y mejorar el sistema de gestión de seguridad de la información, el cual se encuentra apoyado por las personas que operan de cada uno de sus procesos misionales.

Todo aquel que tenga acceso a la información de Ultraline Electrónica S.A.S. será responsable de velar por la seguridad de la información y deberá cumplir las políticas establecidas en este documento.

Todo aquel que tenga acceso a la información de Ultraline Electrónica S.A.S. deberá tener claramente definidas sus funciones. Esto con el fin de poder reducir el uso no autorizado, accidental o indebido de los activos de la información y la comunicación que tienen relación con Ultraline Electrónica S.A.S.

A continuación, se hace un breve resumen de los responsables de los diferentes procesos:

Tabla No.11. Roles y responsabilidades en Ultraline Electrónica S.A.S.

| Cargo/Area | Responsabilidades |
|---|---|
| Gerente General | Mantener, revisar y mejorar el Sistema de Gestión integral de la empresa personalmente y/o a través de delegados debidamente autorizados. Proporcionar recursos y asignar el personal entrenado para garantizar el cumplimiento de los requisitos por parte de la empresa, verificando la prestación del servicio. Establecer y aplicar la Política integral en el desarrollo de todos los procesos de la organización. Apoyar todas las iniciativas, actividades y sugerencias para mantener el servicio que cumpla con las expectativas y especificaciones de los clientes. |
| Gerente Comercial | Asegurarse de que se establecen, implementan y mantienen los procesos necesarios para el sistema de Gestión de Seguridad de la Información en Ultralne Electrónica S.A.S. Informar a la Gerencia General sobre el desempeño del Sistema de Gestión de Seguridad de la Información y de cualquier necesidad de mejora. Promover la toma de conciencia de la política y objetivos de Gestión Integral en todos los niveles de la organización. Asegurarse de que se promueva la toma de conciencia de los requisitos del cliente en todos los niveles de la organización. Garantizar que la planificación de las actividades de gestión de la energía está diseñada para apoyar la política de la organización de la energía. Definir y comunicar las responsabilidades y competencias con el fin de facilitar la gestión eficaz de la energía y demás Sistemas de Gestión. Determinar los criterios y métodos necesarios para asegurarse de que tanto la operación como el control del SGI son eficaces. |
| Contador | Liquidación y presupuesto. Gestión de activos. Seguridad de la información en el área finaniero y contable. |
| Auxiliar Contable | Liquidación y presupuesto |
| Asistentes Adtivo y de Vtas | Seguridad de la información en las relaciones con los proveedores. Gestión de la prestación de servicios de proveedores. Seguridad de la información en ventas. |
| Jefe de Producción | Existencia de la materia prima, materia utilizada y productos en proceso durante el desempeño de sus funciones. Velar por el correcto funcionamiento de maquinarias y equipos, de los procesos productivos para lograr la eficiencia y productos de buena calidad. |
| Embobinador | Solicitar los materiales necesarios para la reparación de cada embobinado. Cambiar sellos y baleros de los motores eléctricos. Notificar anomalía vista en los equipos eléctricos |
| Cableteadores | Cambiar y restaurar el cableado de cada bobina eléctrica. Hacer prueba del funcionamiento del voltaje |
| Tajetero | Garantizar el cuidado y la conservación de las tarjetas. Entregar normas para el manejo y uso del tarjetero. |
| Screen | Revisar y evaluar todo el equipo de producción. Supervisar las series desde producción/financiero. Monitorear la producción. |
| Ensamble | Coordina y supervisa la conducción general de producción y screen en la producción |
| Jefe de Almacén | Gestión de inventario, ingreso y salidad de almacén. Seguridad de la información en relación a proveedores. |
| Auxiliar de Almacén | Gestión de inventario |
| Responsable TI | Políticas de la seguridad de la información, organización de la seguridad de la información, seguridad de los recursos humanos, criptografía, seguridad física y del entorno, seguridad de las operaciones, procedimientos operacionales y responsabilidades, gestión de cambios, gestión de capacidad, separación de los ambientes, protección contra códigos maliciosos, copias de respaldo, registro de eventos, protección de la información de registro, control de software operacional, instalación de software, gestión de vulnerabilidad técnica, restricciones, consideraciones sobre auditoría de sistemas, controles de auditoría de sistemas de información, seguridad de las comunicaciones, gestión de la seguridad de las redes, transferencia de información, adquisición, desarrollo y mantenimeinto de sistemas, alcance MSPI (modelo de seguridad y privacidad de la información), identificación y valoración de riesgo, tratameinto de riesgos de seguridad de la información, toma de conciencia, educación y formación en seguridad de la información, indicadores de gestión MSPI, implementar plan de tratamiento de riesgo. |

Fuente: SGI y Autores, 2019

### *5.3.5.Inventario de Activos e identificación y valoración de riesgos*

Para la realización del inventario de activos y la identificacion y valoración del riesgo se tomó en cuenta la metodología de la guía de gestión de riesgos del MINTIC, donde se establece la matriz de calificación, evaluación y respuesta a los riesgos, así:

Tabla No.12. Matríz de calificación, evaluación y respuesta a los riesgos.

| PROBABILIDAD | IMPACTO | | | | |
|---|---|---|---|---|---|
| | Insignificante (1) | Menor (2) | Moderado (3) | Mayor (4) | Catastrófico (5) |
| Raro (1) | B | B | M | A | A |
| Improbable (2) | B | B | M | A | E |
| Posible (3) | B | M | A | E | E |
| Probable (4) | M | A | A | E | E |
| Casi Seguro (5) | A | A | E | E | E |

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada:* Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema:* Reducir el riesgo, Evitar, Compartir o Transferir

Fuente: Guía Gestión de Riesgos, MINTIC,2019

### *5.3.6. Inventario de activos*

Se identificaron (13) activos generales del sistema de gestión de la seguridad de la información para la empresa Ultraline Electrónica S.A.S. Ver Apéndice E – Inventario de activos de los procesos Gerencia, Contabilidad, Almacén y TI.

### *5.3.7. Identificación de riesgos*

Se define el riesgo como la *"Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias"*. (NTC-ISO/IEC27000:2014, 2018)

El propósito de la identificación del riesgo es determinar que podría suceder que cause una pérdida potencial y llegar a comprender el cómo, donde y por qé podría ocurrir esta pérdida. Para ello, según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar a cabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. (Riesgo, 2019)

Para identificar el riesgo en Ultraline Electrónica S.A.S., se hizo necesario conocer todos los procesos y entender las causas que pueden ser internas o externas e identificarlas. Por ello, se hizo una clasificación de los activos críticos para asociarlos a los procesos correspondientes y se generó un listado de procesos críticos. Así, se identificaron los activos de información sensible, se revisaron los procesos según la clasificación del MECI y del modelo de gestión y por último, se revisó la pertinencia del alcance planteado para el MSPI.

Para evaluar el riesgo, se realizó de manera cualitativa generando una comparación entre el análisis de probabilidad de ocurrencia del riesgo, versus el impacto del mismo. Se tuvo como base, la "Matriz de Calificación, Evaluación y Respuesta a los Riesgos", establecida en la Guía de

Gestión de Riesgo del Ministerio de las TiC. Se identificaron 29 riesgos en Ultraline Electrónica S.A.S. Ver Apendíce F – Riesgos encontrados en Ultraline Electrónica S.A.S.

### *5.3.8. Identificación de controles*

En Ultraline Electrónica se lograron identificar 29 riesgos del sistema de gestión de la seguridad de la información a los cuales se les diseñaron sus controles adecuados. Estos controles pueden vistos en el Apéndice I – Controles identificados en las áreas administrativas de Ultraline Electrónica S.A.S.

### *5.3.9.Plan de capacitación*

La seguridad normalmente requiere adquirir nuevas habilidades, por ello es necesario realizar una capacitación al personal involucrado en el Sistema de Gestión de Seguridad de la Información SGSI de Ultraline Electrónica. Para ello, se diseñó un Plan de Capacitación que involucra los procesos: Gerencia General, Gerencia Comercial, Gestión Administrativa, Gestión TI, Almacén, Contabilidad/Finanzas. A continuación, se muestra el esquema del plan:

Tabla No.13. Plan de capacitación del sistema de seguridad de información 2019

**ULTRALINE ELECRONICA S.A.S.**
**Plan de Capacitación Sistema de Seguridad de la Información 2019**

| Areas | Temas a Capacitar | Cant empleados con necesidades de Capacitación | Modalidad de Capacitación | Intensidad | Fecha de Ejecución |
|---|---|---|---|---|---|
| Gerencia General, Gerencia Comercial, Contabilidad/Finanzas, Almacenista y Auxiliares | Políticas de seguridad y rivacidad de la información | 17 | Seminario Taller, Presencial | 2 horas | 16-dic-19 |
| | Seguridad de las contraseñas, los controles de software | 17 | Charla | 1 hora | 16-dic-19 |
| | Reporte de incidentes de seguridad de la información | 17 | Seminario Taller, Presencial | 1 hora | 16-dic-19 |
| | Sensibilizar para la conformación de Comité de apoyo al Resposable de Ti en el tema de Seguridad de la Información | 17 | Charla | 1 hora | 16-dic-19 |
| **Preparó: Jenis Sagbini y Jefferson Farello** | | | | | |

Fuente: Autores, 2019

## *5.4. Realización de la prueba piloto utilizando las políticas del sistema de gestión de la seguridad de la información (SGSI) en el departamento de T.I.*

### *5.4.1. Generalidades de la oficina TI en Ultraline Electrónica S.A.S. Barranquilla*

En Ultraline Electrónica S.A.S. no se cuenta con una oficina oficial para el responsable de TI, solamente se cuenta con un escritorio que es compartido con la contadora. Ambos cargos: contador y responsable de TI, trabajan bajo la modalidad de contrato de prestación de servicios, lo que quiere decir que no existen actividades de seguimiento, control, monitoreo y prevención tanto para los equipos de la empresa como para la seguridad de la información.

Por lo anterior, se sugiere que no exista esa unión de una oficina compartida y que el responsable de TI tenga un espacio para ejercer sus funciones como responsable de la seguridad de la información de Ultraline donde pueda conformar un Comité o Equipo de Protección que le apoye en todas sus labores y que le permita realizar los controles y seguimientos adecuados para garantizar el integridad, disponibilidad y confidencialidad de la información.

El responsable de TI tendrá que ejercer las siguientes funciones:

- Atender, realizar mantenimiento y solucionar las dificultadas presentadas en los servicios de la Red LAN así como realizar labores preventivas permitiendo mejorar el rendimiento y sostenibilidad en el tiempo.
- Hacer recomendaciones para el mejoramiento de los servicios de la Red LAN
- Reinstalación de aplicaciones y reconfiguración de servidores.
- Instalación y configuración de nuevos equipos de la plataforma de Red de área local.

- Solución a los problemas de red en su nivel físico (cableado o terminaciones dañadas o sucias, atenuación excesiva de la señal, insuficiente ancho de banda para el cableado, interferencia inalámbrica entre otros.
- Solución a los problemas en el nivel de red Ethernet e IP: identificación de dispositivos de red defectuosos, configuraciones de dispositivo incorrectas o no óptimas, problemas de autenticación y asociación, ancho de banda de red insuficiente.
- Solución a fallas a nivel de Switches y VLAN causados por inscripción de VLAN asignada incorrectamente y problemas de prioridad del tráfico (CoS/QoS).
- Capacitación y entrenamiento al recurso humano que la seccional disponga para la solución de problemas.
- Informar detalladamente sobre las fallas o las configuraciones aplicadas y con recomendaciones para la mejora de los servicios.

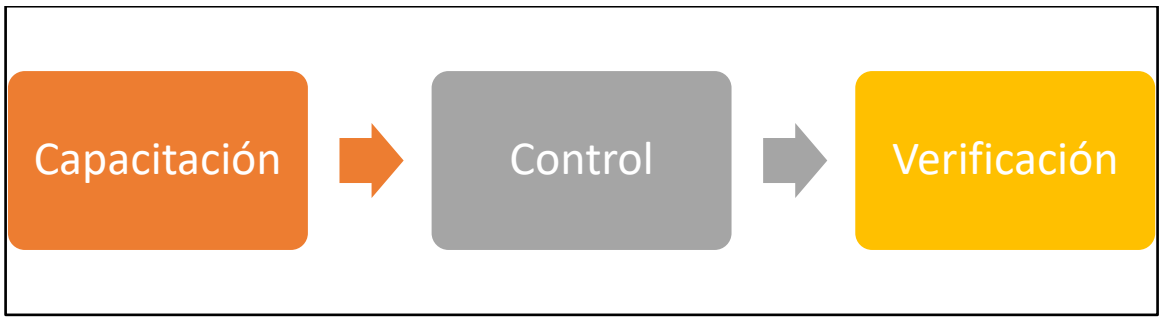
### *5.4.2. Metodología de la prueba piloto*

Realizar una prueba piloto del sistema de gestión de la seguridad de la información propuesto para Ultraline Electrónica S.A.S. fue de gran valor para lograr el inicio de una efectiva implementación.

Se inició con la realización de una capacitación en la política de seguridad de la información donde participaron todas las personas implicadas en el manejo de información en el interior de la organización, con la idea de promover una cultura de prevención. Posteriormente, se aplicó la lista de chequeo de mantenimiento de computadores teniendo en cuenta el formato institucional debidamente elaborado por los auditores y aprobado por el Gerente General.

El esquema de la prueba piloto establecido es:

Figura No.5 Esquema de prueba piloto




Fuente: Autores, 2019

### *5.4.3. Primera prueba: capacitación en la política de la seguridad de la información*

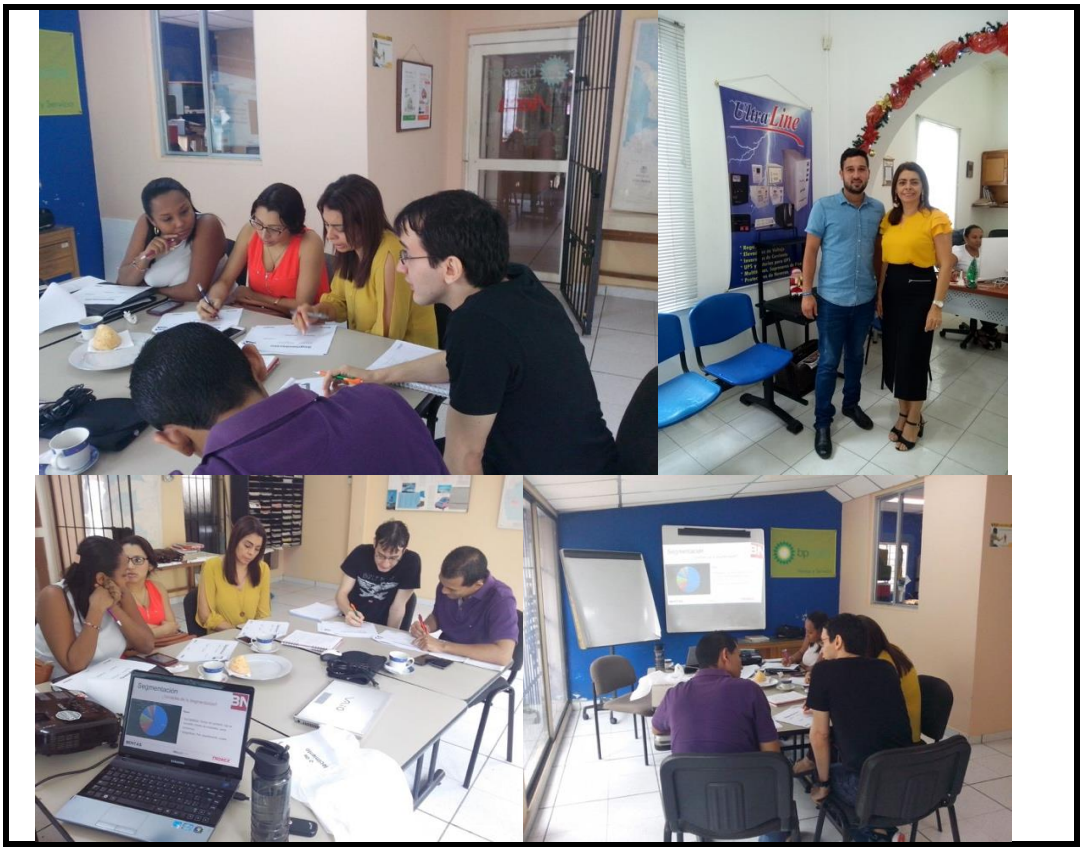
Para la primera prueba del plan piloto, los ingenieros líderes del proyecto se trasladaron a Ultraline Electrónica S.A.S. y programaron la primera capacitación dirigida hacia los funcionarios de Ultraline para dar a conocer la política de seguridad de la información diseñada para la organización. El objetivo final fue propiciar una cultura y una motivación a la protección de la información que se produce en cada una de las áreas.

Dentro de la capacitación se dieron a conocer temas como:

- Conocimiento general de la estructura de la política de seguridad de la información de Ultraline Electrónica S.A.S.
- Conocer las funciones más importantes de los cargos de los funcionarios de la entidad con el fin de minimizar el riesgo en seguridad de la información.
- Cumplir con los principios generales de la seguridad de la información teniendo en cuenta las funciones administrativas de cada cargo.

- Lograr mantener la confianza de los usuarios, socios y empleados de Ultraline Electrónica S.A.S.
- Entender la protección de los activos tecnológicos basados en procedimientos e instructivos en materia de seguridad de la información.
- Garantizar la continuidad del proceso frente a incidentes.
- Se socializó la decisión de Ultraline Electrónica S.A.S. de definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información SGSI soportando lineamientos claros a las necesidades del proceso y de los requerimientos regulatorios.

Figura No.6. Capacitaciones realizadas en Ultraline Electrónica S.A.S.




Fuente: Autores, 2019

### *5.4.4. Segunda prueba: establecimiento de controles en la oficina de TI*

Se estableció una reunión entre el equipo líder del presente proyecto y el Responsable de TI y se analizaron los controles pertinentes y contempladas en la política de seguridad de la información permitiendo definir un ciclo redactado a través de un acta de responsabilidades. Ver Apéndice J – Acta de reunión capacitación y establecimiento de controles.

### *5.4.5. Tercera prueba: aplicación de la lista de chequeo de mantenimiento de computadores de acuerdo al formato institucional*

El equipo líder del proyecto del SGSI junto con el Responsable de TI, se reunieron para dar inicio a la aplicabilidad de los instrumentos de control. En este caso, aplicar el Formato diseñado como lista de chequeo y garantizar el cumplimiento de cada paso del mantenimiento físico de los computadores de Ultraline Electrónica S.A.S. Ver Apéndice K – Aplicación del Check List para seguimiento al mantenimiento físico de los computadores personales.

# 6.Conclusiones

Ultraline Electrónica S.A.S. es una empresa tipo pyme perteneciente al sector industrial radicada en la ciudad de Barranquilla que con dedicación, buenas estrategias e innovación, ha podido crecer posicionando su marca en un mercado regional y nacional.

Diagnosticar el estado de la seguridad de la información en Ultraline Electrónica S.A.S. se pudo llevar a cabo utilizando herramientas debidamente estructuradas a través del análisis de elementos y aplicación de metodologías que permitieran conocer todo el universo para salvaguardar la integridad, disponibilidad y confidencialidad de la información. Igualmente, se concluyó que existen necesidades de índole documental, infraestructura, espacio físico y de formación integral para abordar un sistema de gestión de la seguridad de la información en Ultraline Electrónica S.A.S.

En la determinación de los elementos del estándar ISO 27001, que son necesarios en la aplicación de la empresa Ultraline Electrónica S.A.S. de la ciudad de Barranquilla, se pudo concluir que se hace necesario hacer una documentación de todos aquellos que de alguna manera, pertenecen a una de las fases más importantes, como es la Planificación. Es aquí donde se pudo llegar a incluir el Alcance de un modelo de seguridad y privacidad de la información para empresas tipo pymes que incluye unas políticas de seguridad y privacidad de la información, unos modelos de controles documentales que incluyan roles, responsabilidad. De igual manera, se realizó un inventario de activos, identificaron riesgos, controles y se realizó formación a los funcionarios de

Ultraline Electrónica. Esto demuestra que se cumplió satisfactoriamente la determinación de los elementos de ISO27001 aplicados a Ultraline Electrónica S.A.S.

Se pudo establecer el sistema de gestión de la seguridad de la información en Ultraline Electrónica S.A.S. en Barranquilla por lo que se pudieron definir brevemente unas políticas de seguridad, unos roles y responsabilidades de los funcionarios de la empresa, unos inventarios de activos que si bien, no estaban bien estructurados y se encontraron 29 riesgos a los cuales se les pudo analizar sus controles asociados. Posterior a todo ello, se realizó un plan de capacitación involucrando a todos los funcionarios pertinentes con la temática que permitió promover la cultura de la seguridad de la información en el interior de la organización.

Para finalizar, en este proyecto se pudo validar unas premisas aplicando unas pruebas piloto involucrando a los funcionarios directamente responsables de procesos centrales y que manejan un flujo interesante de información. Articular esfuerzos en el equipo de trabajo de Ultraline Electrónica permitió gestionar de mejor manera los procesos asociados a los sistemas de información y verificar la aplicación de herramientas de chequeo, consiguiendo así buenos objetivos para garantizar la integridad, disponibilidad y confidencialidad de la información en Ultraline Electrónica S.A.S. en la ciudad de Barranquilla.

# 7.Recomendaciones

A continuación, el equipo líder de investigación recomienda tener en cuenta los siguientes ítems para el buen manejo de la seguridad de la información en Ultraline Electrónica S.A.S.:

1. Reconocer la importancia de establecimiento de un modelo de seguridad de la información, teniendo en claro la responsabilidad social de la entidad constituyéndose como parte misional en la ejecución de sus actividades.

2. La Gerencia General debe hacer un esfuerzo de tipo financiero para que el sistema de gestión de seguridad de la información se cumpla cabalmente en el interior de la organización.

3. La Gerencia General de Ultraline Electrónica S.A.S. debe promover la formación continúa involucrando a todos los actores de la entidad independientemente del tipo de contratación que tenga, así como a proveedores.

4. Garantizar la aplicabilidad de los controles adecuados para mantener a través del tiempo la confiabilidad y veracidad de toda la información que produce la entidad desde el interior de sus procesos

## Referencias

Informática, T. e. (2018). *tecnologia-informatica.com*. Obtenido de https://tecnologia-informatica.com/sistemas-informacion-empresa/

blogs.eusto.es. (8 de 12 de 2015). Obtenido de https://blogs.deusto.es/master-informatica/la-informacion-en-las-empresas/

cic.es. (15 de 05 de 2019). *cic.es*. Obtenido de CIC Consulting Informático: https://www.cic.es/que-es-un-sgsi/

www.arroyosdebarranquilla.co. (23 de 4 de 2013). *Arroyos de Barranquilla*. Obtenido de www.arroyosdebarranquilla.co:

http://www.arroyosdebarranquilla.co/servicios/barranquilla/posicion

Atlántico, G. d. (22 de 10 de 2010). *www.atlantico.gov.co*. Obtenido de www.atlantico.gov.co: https://www.atlantico.gov.co/index.php/departamento

http://video.anetcom.es/editorial/. (2015). *http://video.anetcom.es/editorial/Seguridad_empresa.pdf, disponible en internet en:Gestión estratégica de seguridad en la empresa*. Obtenido de http://video.anetcom.es: http://video.anetcom.es/editorial/Seguridad_empresa.pdf, disponible en internet en:Gestión estratégica de seguridad en la empresa

http://video.anetcom.es/. (2015). *http://video.anetcom.es/editorial/Seguridad_empresa.pdf, disponible en internet en:Gestión estratégica de seguridad en la empresa*. Obtenido de http://video.anetcom.es/editorial/Seguridad_empresa.pdf, disponible en internet en:Gestión estratégica de seguridad en la empresa

AS/NZS 4360. (2004). *ADMINISTRACION DE RIESGOS.*

Sant-Germain, R. (2005). *Information Security Management Best Practice Based on ISO/IEC 17799.* The Information Management Journoi .

Josef Pieprzyk, T. H. (2003). *Fundamentals Of Computer Security.* Springer.

http://168.243.33.153/infolib/tesis/50107386.pdf, d. e. (s.f.). *La auditoría interna como una herramienta para establecer controles internos eficientes en las pequeñas y medianas empresas ferreteras de la Ciudad de San Miguel.*

www.iso27000.es. (2008). *INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO27000.*

ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD-AEC - . (2012). La gestión de la seguridad en la empresa . *revista calidad* .

Laudon, L. &. (s.f.). *Sistemas de Informacion Gerencial* . Pearson.

CORLETTI, A. (2006). *Análisis de ISO-27001*.

SGSI, I. E. (2015). *ISO 27001*.

PACHECO, F. (2010). *La importancia de un SGSI.* Welivesecurity en Español.

Ever ariza, J. B. (2018). Entrevista a la alcaldia del Paso (Cesar). El Paso (Cesar).

Pardo. (2015). *HFramework.* España: Universidad de castilla- la mancha.

cestero. (2016). *metodología de análisis y gestión de riesgos en sistemas de información.* madrid (España): universidad politecnica de madrid.

bocanegra. (2016). *análisis y gestión de riesgos de los sistemas de información aplicando la metodologia Magerit.* Tulua (Valle).

Pineda. (2015). *auditoría a la seguridad del sistema de información "gestión integrada de bienestar social".* manizales (caldas).

Uninorte. (2016). *metodologia para conocer estandares en gestion de riesgos tecnologicos.* Barranquilla: Uninorte.

Normas ISO/iec 27001, 2. y.-2. (2013). *Normas ISO/iec 27001,27002 y su estructura.* Networking online.

Cestero. (2016). *metodología de análisis y gestión de riesgos en sistemas de información.* Madrid: Universidad Politécnica de Madrid (España).

Cestero. (2016). *metodología de análisis y gestión de riesgos en sistemas de información.* Madrid: universidad politécnica de Madrid (España).

Guerrero, N. L. (2019). Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 27001, en la UPC, seccional Aguachica. En *Diseño del Sistema de Gestión de Seguridad de la Información SGSI basado en el estándar ISO 27001, en la UPC, seccional Aguachica.* Ocaña.

Guerrero, D. F. (2019). Diseño del SGSI basado en la estándar ISO 270001 en la UPC, seccional Aguachica. En *Diseño del SGSI basado en la estándar ISO 270001 en la UPC, seccional Aguachica* (pág. 95). Ocaña.

MINTIC. (2016). *Guía para la implementación de Seguridad de la Información en una MiPYME.* Bogotá.

Ecured. (2016). *Auditoría de Sistemas*. Obtenido de Ecured.cu/Auditoría de Sistemas: https://www.ecured.cu/Auditor%C3%ADa_de_sistemas

MINTIC. (2016). *Guía de Seguridad de la Información para Mypimes*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles5482_Guia_Seguridad_informacion_Mypimes.pdf

Esan. (05 de 2016). *https://www.esan.edu.pe/*. Obtenido de https://www.esan.edu.pe/: https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/

https://www.pmg-ssi.com. (2016). *https://www.pmg-ssi.com*. Obtenido de Blog Sistema de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2016/07/normativa-que-utiliza-norma-iso-27001/

dnvgl.es. (2014). *DNV GL*. Obtenido de https://www.dnvgl.es/services/iso-27001-sistema-de-gestion-de-seguridad-de-la-informacion-3327

AENOR. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO, AENOR -*. Madrid.

Ley1581. (2012).

MINTIC. (s.f.). *https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009.*

innovacionUNAL. (2017).

LIFEDER. (s.f.). Obtenido de https://www.lifeder.com/diseno-metodologico-investigacion/
HernadezSampieri. (2010). *Metodología de la Investigación.*

TécnicasdeRecolecciónde Datos. (2013). *https://gabriellebet.files.wordpress.com.* Obtenido de https://gabriellebet.files.wordpress.com: https://gabriellebet.files.wordpress.com/2013/01/tecnicas-de-recoleccic3b3n4.pdf

Gómez, F. L. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad, .* Madrid: AENOR - Asociación Española de Normalización y Certificación.

LAURA FELIZZOLA, A. N. (2012). *DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION SGSI BASADO EN EL ESTANDAR ISO 27001 EN LA UNIVERSIDAD POPULAR DEL CESAR.* AGUACHICA (CESAR).

J, A. G. (2011). *Guia de buenas practicas de seguridad de la informacion en contextos de micro, pequeñas y medianas empresas de la region.* Pereira.

http://www.ultralineelectronica.com/. (2015). *http://www.ultralineelectronica.com/*. Obtenido de http://www.ultralineelectronica.com/: http://www.ultralineelectronica.com/

http://www.ultralineelectronica.com/. (2015). *http://www.ultralineelectronica.com/#empresa*. Obtenido de http://www.ultralineelectronica.com: http://www.ultralineelectronica.com/#empresa

Minuto de Dios. (2015). *http://mdc.org.co/como-definir-una-estructura-administrativa/*. Obtenido de http://mdc.org.co/como-definir-una-estructura-administrativa/: http://mdc.org.co/como-definir-una-estructura-administrativa/

www.vegagestion.es. (2015). *https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/*. Obtenido de https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/: https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/

MINTIC.GOV.CO. (2017). *https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf: https://www.mintic.gov.co/gestionti/615/articles-5482_Instructivo_instrumento_Evaluacion_MSPI.pdf

NTC-ISO/IEC27000:2014. (2018). *NTC-ISO/IEC27000:2014*. Obtenido de NTC-ISO/IEC27000:2014.

Riesgo, G. d. (2019). *www.mintic.gov.co.* Obtenido de www.mintic.gov.co: www.mintic.gov.co

https://www.gestion.org/la-importancia-del-test-psicometrico-pda/. (2019). *https://www.gestion.org/la-importancia-del-test-psicometrico-pda/*. Obtenido de https://www.gestion.org/la-importancia-del-test-psicometrico-pda/

Apéndice A : Carta de Inicio de Auditoría de Sistemas a Ultraline Electrónica S.A.S.

Valledupar, 12 de noviembre de 2019

Señora
CATHERINE SAGBINI ECHÁVEZ
Gerente
Ultraline Electrónica S.A.S.
Barranquila

Ref: Inicio de Auditoría de Sistemas a Ultraline Electrónica S.A.S.

Estimada Señora:

De acuerdo a lo señalado en la referencia, nos permitimos informarle que conforme al programa de estudio de la Universidad Francisco de Paula Santander Ocaña y al trabajo de grado titulado DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN EL ESTÁNDAR ISO 27001, EN ULTRALINE ELECTRONICA S.A.S., EN LA CIUDAD DE BARRANQUILLA, para obtener el título de Especialistas en Auditoría de Sistemas, corresponde efectuar una auditoría en las dependencias Directivas, Administrativas, Financieras y de Sistemas en cuanto a seguridad informática, pues son las dependencias más vulnerables y expuestas a cualquier alteración en los sistemas de información.

El grupo de estudiantes está integrado por los siguientes Ingenieros de Sistemas:

| Nombres Completos | Código |
|---|---|
| Jenis del Carmen Sagbini Echávez | 850256 |
| Jefferson Farelo Paez | 850258 |

Esta auditoría está planificada para realizar su ejecución desde el 15 al 22 de noviembre de 2019 y tiene como objetivo diagnosticar los requisitos de las partes interesadas pertinentes a la seguridad de la información, con el fin de comprender las necesidades y expectativas determinando una línea base para el Diseño del Sistema de Gestión de la Seguridad de la Información SGSI de Ultraline Electrónica S.A.S. en la ciudad de Barranquilla. con base a esta labor, se podrá constatar si las actividades del sistema son correctas y si están de acuerdo con la normatividad institucional y general (basado en el estándar ISO 27001) que están establecidas a dar sugerencias y soluciones estratégicas de los hallazgos.

Cordialmente,

Jenis Sagbini Echavez
JENIS DEL CARMEN SAGBINI ECHAVEZ

Jefferson Farelo P.
JEFFERSON FARELO PAEZ

UltraLine
Electrónica S.A.S.

Nov 12 de 2019.

Apéndice B. Encuestas a aplicar a funcionarios Adtivos de Ultraline Electrónica

**AUDITORIA SGSI PARA ADMINISTRATIVOS DE ULTRALINE ELECTRÓNICA S.A.S**
**ENCUESTA.**

Objetivo. Determinar el grado de conocimiento y el manejo de políticas de seguridad de la información para los administrativos de Ultraline Electrónica S.A.S, en la ciudad de Barranquilla.

Población_____ funcionarios.
Cantidad de preguntas ____.

Marque con una (X) o un ✓ la respuesta que considere de su elección.

1. ¿Conoce si la Ultraline Electrónica S.A.S. - Barranquilla tiene implementado un Sistema de Gestión de seguridad de la información para los procesos que involucren el tratamiento de los datos generados?
   Sí _____ No _____ Nunca ____

2. ¿Dentro de los procesos que competen a su cargo o dependencia existen metodologías de respaldo de información que puedan evitar la pérdida o daño de la misma en casos especiales o fallas de su equipo de cómputo?
   Sí NO NS/NR

3. ¿Con que regularidad realiza el cambio de contraseña para su equipo de cómputo, correo institucional o cuentas que utilice en el desarrollo de sus labores diarias?

   1 Vez a la semana
   1 Vez al mes
   3 a 6 meses
   Nunca

4. ¿Las contraseñas que normalmente utiliza en sus cuentas se forman con el conjunto de caracteres en minúscula, mayúscula, números y caracteres especiales?
   Con mucha frecuencia___ Con Frecuencia ____ Poco _____ Nunca_____

5. ¿Conoce si existen políticas de seguridad para el correcto mantenimiento preventivo y correctivo de su equipo de cómputo, Software de aplicativo y Sistema operativo funcional?
   Si
   No
   Nunca/No sabe

6. ¿Dentro de la institución se realizan procesos de gestión de riesgos para mitigar posibles incidentes y fortalecer las vulnerabilidades relacionadas a la gestión de la seguridad de la información?

   Con frecuencia____ Mucha Frecuencia ____ Poca Frecuencia ___ Nunca ____

7. ¿Tiene conocimiento de si en su equipo de cómputo se encuentra instalado un software de antivirus y este se encuentra en estado activo y actualizado?
   Si _____ No _____

8. ¿La institución cuenta con un departamento de sistemas encargado de priorizar y mantener procesos de gestión de la seguridad de la información, mitigación de riesgos y control de datos?
   Sí _____ No _____

9. ¿La institución brinda mediante capacitaciones periódicas conocimiento sobre políticas de seguridad de la información, Gestión del riesgo y posibles delitos o fraudes de los que podría ser víctima? Sí_____ No ____

10. ¿Cómo funcionario de la institución se le realiza la solicitud del carnet en la entrada por parte del equipo de vigilancia contratado?
    Con mucha frecuencia _____ Con poca Frecuencia _____ Nunca _____

11. ¿Durante los últimos meses ha recibido correos sospechosos o alertas de posibles virus y

    phishing (robo de claves y datos personales)?
    Si No

Apéndice C. Entrevista a aplicar al Funcionario de TI

**ENTREVISTA AL RESPONSABLE TI**
**AUDITORIA SGSI DE LA ULTRALINE ELECTRÓNICA SAS**

Objetivo. Dar una evaluación sobre los aspectos relacionados con la usencia del departamento de sistemas de la Ultraline Electrónica S.A.S. - Barranquilla.

Población. (Analista de sistemas Y/O Jefe de Sistemas de la Ultraline Electrónica S.A.S. - Barranquilla).

1. ¿Dentro de la ULTRALINE ELECTRÓNICA S.A.S. se ha planteado la posibilidad y viabilidad de contar con un departamento de sistemas y un Data center centralizado para mejorar y garantizar metodologías que controlen incidentes y riesgos latentes en contra de la seguridad de la información?
2. ¿De qué manera se controla el acceso a los rack de comunicación, quien maneja las llaves y de qué manera se lleva el registro de cada acceso y modificación?
3. ¿Qué tipo de controles se utilizan para evitar que personas que no cuentan con autorización ingresen a áreas restringidas dentro de la Ultraline Electrónica S.A.S. - Barranquilla?
4. ¿Realiza revisiones de seguridad física a las instalaciones, con qué frecuencia las realiza?
5. ¿Realiza backups de la configuración de equipos de comunicación como Router y Switches para posteriores restauraciones?
6. ¿Lleva control de cambios de Hardware y Software en los mantenimientos preventivos y correctivos que realiza?
7. ¿De qué manera realiza el borrado de información de manera segura, cuenta con procedimientos ya establecidos?
8. ¿Existen controles para determinar si se habilita o deshabilita un punto de datos dentro del cableado estructurado, todos se encuentra por defecto habilitados?
9. ¿Existe un sistema de monitoreo de video vigilancia en las áreas restringidas ?
10. ¿Con que frecuencia realiza mantenimientos a equipos de cómputo, impresoras y cableado estructurado dentro de la Ultraline Electrónica S.A.S. - Barranquilla?
11. ¿Cómo se control el ingreso de otros equipos de cómputo por parte de usuarios externos o visitantes?
12. ¿Dentro de los laboratorios de informática existen políticas de seguridad para evitar que los usuarios usen los equipos de cómputo para tratar de vulnerar áreas administrativas?
13. ¿Se cuenta con un cronograma de actividades para realizar tareas de mantenimiento preventivo y correctivo a los equipos de cómputo de los laboratorios destinados al uso general de los estudiantes y docentes de la seccional?
14. ¿El acceso al nodo de conexión de fibra y Router de la sala de informática es registrado en un formato al igual que los cambios generados dentro del mismo?
15. ¿El acceso a los laboratorios es monitoreado por un sistema de cámaras de vigilancia, donde se registre los acontecimientos y accesos a los equipos de conexión dentro del rack?
16. ¿Quién brinda acceso y manejo de las llaves de los laboratorios?
17. ¿Se registra en formatos el ingreso de cada usuario, y se monitorean las actividades que realiza durante su estadía dentro de los laboratorios de informática?

# Apéndice D Situaciones encontradas en la Auditoría

| AUDITORÍA DE SISTEMAS | | | | | |
|---|---|---|---|---|---|
| **EMPRESA A AUDITAR: ULTRALINE ELECTRÓNICA** | | | | **Fecha: 15/11/2019** | |
| **AREAS A AUDITAR: GERENCIA COMERCIAL, CONTABILIDAD/FINANZAS, ALMACEN, OFICINA TI** | | | | | |
| **Ref** | **Situación Encontrada** | **Causas** | **Solución** | **Fecha Solución** | **Responsable** |
| OO1 | No existen una políticas de seguridad de la infomación adecuadas para el tto. De la seguridad de la información | No hay conocimiento sobre la importancia de establecer unas políticas de seguridad de la información | Implementar las políticas de seguridad de la información | 2020 | Gerente General y Responsable TI |
| OO2 | Los usuarios del sistema carecen de buenas prácticas en el uso de contraseñas de acceso para los equipos y los Sist de Información | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Capacitación a todo el personal que hace uso de los sistemas de información | 16-dic-19 | Responsable TI y su apoyo |
| OO3 | No se realizan las copias de seguridad o Backups de forma adecuada garantizando la seguridad, confiabilidad y disponibilidad de la información en las oficinas de contabilidad y Gerencia Comercial | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Capacitación a todo el personal que hace uso de los sistemas de información | 16/12/19 | Gerente Comercial, Responsable TI y su apoyo |
| OO4 | Existen malas condiciones físicas en la infraestructura tecnológica (cables, equipos mal conectados) en la oficina del contador y auxiliar administrativo | Muy poco espacio y desorden de cables y equipos en el área | Transladar la infraestructura tecnológica de lugar asegurando su permisibidad solo para los que laboran en TI | 2020 | Gerente Comercial, Responsable TI y su apoyo |
| OO5 | No se cuenta con un manual de seguridad de la información aprobado e implementado por la gerencia | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Diseñar, aprobar e implementar un Manual de Buenas Prácticas de Seguridad de la Información | 2020 | Responsable TI y Gerencia General |
| OO6 | Uso de datos personales como contraseña para acceso a sistemas de información | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Capacitación sobre buenas prácticas de seguridad de información | 2020 | Responsable TI |
| OO7 | Falta de políticas de seguridad en la entrada de personas no autorizadas para manipular en Rack central | No existe un control en el Rack y su ubicación no es la adecuada. | Colocarle seguridad al panel y rack. Se recomienda ubicarlo en un espacio menos accesible a personas ajenas de su manipulación | 2020 | Responsable TI |
| OO8 | No existe un control pertinente para el manejo de dispositivos de almacenamiento externos | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Capacitación sobre buenas prácticas de seguridad de información | 2020 | Responsable TI |
| OO9 | No se cuenta con un sistema de contingencia para la continuidad de energía eléctrica en caso de fallas | Falta de políticas que mejoren el objetivo de continuidad del proceso | Socializar con el área administrativa para hacer una propuesta de diseño e implementación | 2020 | Gerente Comercial, Responsable TI y su apoyo |
| O10 | Ultraline Electrónica no cuenta con un equipo hardware para realizar filtrado de contenido WEB | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Adquirir un equipo de cómputo encargado de realizar filtrado de contenido WEB y capacitar al personal involurado | 2020 | Gerente General y Responsable TI |
| O11 | Ultraline no cuenta con un DATA CENTER centralizado | Se carece de políticas de centralización de información y datos | Adecuar un espacio físico para el departamento TI | 2020 | Gerente General y Responsable TI |
| O12 | Ultraline no cuenta con un sistema de alarma y detección de humo que esté conectada a la central de bomberos | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Propuesta de implementación de equipos de detección de humo y conexión con bomberos locales | 2020 | Gerente General y Responsable TI |
| O13 | No existe un procedimiento adecuado para la eliminación de informacón de manera segura de los equipos de cómputos y demás | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Crear un comité de mejora de las políticas de seguridad de la información que realice un documento sobre le procedimiento | 2020 | Gerente General y Responsable TI |
| O14 | No existe una bitácora que documente los registros de actividades dentro de la red de datos, fallas del servicios, direcciones IP, consumo de banda de ancha, entre otros | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Crear políticas para el registro de cada acontecimiento que ocurra en la red y que requiera atención y monitoreo | 2020 | Responsable TI |
| O15 | No se cuenta con políticas de control formal para la transferencia de información por cualquier medio | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Crear una política para limitar o establecer los correctos procedimientos sobre esta situación | 2020 | Responsable TI |

**AUDITORÍA DE SISTEMAS**

**EMPRESA A AUDITAR: ULTRALINE ELECTRÓNICA** **Fecha: 15/11/2019**

**AREAS A AUDITAR: GERENCIA COMERCIAL, CONTABILIDAD/FINANZAS, ALMACEN, OFICINA TI**

| Ref | Situación Encontrada | Causas | Solución | Fecha Solución | Responsable |
|---|---|---|---|---|---|
| O16 | No se evidencian auditorías de sistemas realizadas a la red y al cableado estructurado | Desconocimiento del control y mejora continua que permiten las auditorías en la red | Desarrollar un plan de auditorías y sensibilizar a usuarios sobre la importancia de registro y supervisión de actividades | 2020 | Responsable TI |
| O17 | No existen controles o bitácoras de acceso a los diferentes Rack de equipos ubicados en distintos puntos de la empresa | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Adquirir para el 2020 un control ya sea biométrico o similar para el acceso a los equipos | 2020 | Gerente General y Responsable TI |
| O18 | No existe señalización adecuada para rutas de evacuación en las instalaciones | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Implementar un plan de señalizaión de evacuación y demás | 2020 | Gerente General y Responsable TI |
| O19 | Los equipos de cómputo de Ultraline Electrónica no cuentan con un antivirus licenciado que controle acceso a redes. Usan el antivirus de Microsoft | Deconocimiento de protección de datos e información | Adquirir un antivirus licenciado para todos los equipos de Ultraline Electrónica | 2020 | Responsable TI y Gerencia General |
| O20 | El responsable de TI no realiza registro en una bitácora/formatos de control en las diferentes dependencias cuando realiza cambios de hardware y software | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Crear política de gestión de la seguridad de la información e implementar un procedimiento para registrar cambios | 2020 | Responsable TI |
| O21 | No existe un plan de contingencia en caso de emergencias o desastres naturales | Desconocimiento del diseño de un plan de contingencia | Crear una política y un plan de contingencias para evacuación y emergencias naturales y sensibilizar al personal | 2020 | Responsable TI y Gerencia General |
| O22 | No existen herramientas para la protección contra el código malicioso | Deconocimiento de protección de datos e información | Crear una política de seguridad para mejorar situaciones de riesgo en cuanto un código malicioso | 2020 | Responsable TI y su apoyo |
| O23 | No exite gestión y registro de incidentes de la seguridad de la información | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Crear un comité liderado por el Responsable de TI para registrar y gestionar distintos tipos de incidentes de seguridad | 2020 | Responsable TI y su apoyo |
| O24 | No existe un control para deshabilitar los puertos de red que puedan ser riesgo en la conexión de visitantes | Falta de controles que determinen los puertos que deben estar desactivados | Establecer como política permitir desactivar puertos que no estén en uso | 2020 | Responsable TI |
| O25 | No existe un monitoreo y registro permanente de la cantidad de usuarios de la red inalámbrica durante los momentos de más afluencia | Falta de conocimiento de unas buenas prácticas de seguridad de la información | Monitorear en las horas de mas afluencia dentro del Ruckus la cantidad de IP asignadas para equipos o dispositivos | 2020 | Responsable TI |
| O26 | No existe una oficina o espacio para el Responsable de TI que soporte todo el sistema de información dentro de la organización | Falta de asignación para el control de políticas de seguridad de la información | Crear como apoyo un equipo de soporte que controle el sistema de gestión de seguridad de la información | 2020 | Gerente General y Responsable TI |
| O27 | No existe dentro de Ultraline Electrónica, un método de cifrado de información para las dependencias de manejo de datos de alto riesgo | Desconocimiento de los posibles robos de datos o accesos no autorizados | Adquirir herramientas que permitan en los momentos que se necesite, el cifrado de datos importantes para las dependencias que lo requieran | 2020 | Gerente General y Responsable TI |
| O28 | Falta de entrenamiento y capacitación colectivo de administrativos sobre la seguridad de la información | Desconocimiento sobre políticas de seguridad d ela información | Crear una capacitación para informar sobre la gestión de seguridad de la información | 2020 | Gerente Comercial, Responsable TI y su apoyo |
| O29 | Se carece de políticas de control y detección de Ransomarre y Malware dentro de las dependencias de Ultraline Electrónica SAS | Existe exceso de confianza con el desconocimiento sobre correos con virus y codificación sobre Ransomware y Malware | Socializar y sensibilizar al personal sobre los distintos tipos de virus y amenazas dentro de la red y equipos de cómputo | 2020 | Responsable TI |

Elaborado por: Jenis Sagbini y Jefferson Farelo

Apéndice E – Inventario de activos de los procesos Gerencia, Contabilidad, Almacén y TI

| Inventario de Activos de los procesos de : Gerencia, Contabilidad/Finanzas y Adtivo/Almacén | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Clasificación | | | | | | | | | Criticidad | Propiedad | |
| Cód | Proceso | Activo | Observaciones | Tipo | Ubicación | Confiabilidad | Integridad | Disponibilidad | | Propietario | Responsable |
| A1 | Gerencia General | Canal Comunicación | Físicos,Virtuales | Software | Red | Privada | A | 1 | Alta | Ultraline | Oficinas |
| A2 | Gerencia Ccial | Documentos | Físicos,Virtuales, verbales | Información | Oficina Gerente Comercial | Pública | A | 1 | Alta | Ultraline | Oficinas |
| A3 | Contador | Equipos de Cómputos | Incluye todos los equipos | Hardware | Oficinas productoras y receptoras de información | Reservada | A | 1 | Alta | Ultraline | Oficina |
| A4 | Auxiliar Contabilidad | Equipos de Cómputos | Incluye todos los equipos | Hardware | Oficinas productoras y receptoras de información | Reservada | A | 1 | Alta | Ultraline | Oficina |
| A5 | Ventas | Equipos Tecnológicos | Incluye todos los equipos | Hardware | Oficinas productoras y receptoras de información | Privada | A | 1 | Alta | Ultraline | Oficina Adtiva/Financiera |
| A6 | Gestión Adtiva | Información Proveedores/Clientes | Físicos,Virtuales, verbales | Información | Oficinas productoras y receptoras de información | Reservada | A | 2 | Alta | Ultraline | Oficina Adtiva/Compras |
| A7 | Almacén | Infraestructura física y Tecnológica | Incluye todos los equipos | Hardware | Instalaciones de Ultraline Electrónica | Privada | A | 1 | Alta | Ultraline | Oficina Adtiva/Compras |
| A8 | Gestión Tecnológica | Medios de Almacenamiento extraíbles | Incluye todos los equipos | Hardware | Instalaciones de Ultraline Electrónica | Clasificada | A | 1 | Alta | Ultraline | Oficinas |
| A9 | Gestión Tecnológica | Nodos de comunicación | Físicos,Virtuales, verbales | software | Instalaciones de Ultraline Electrónica | Clasificada | A | 1 | Alta | Ultraline | Oficina Tecnología |
| A10 | Gestión Adtiva y Financiera | Recurso humano | Empleados | Recurso humano | Instalaciones de Ultraline Electrónica | Pública | A | 1 | Alta | Ultraline | Dirección Adtiva/Financiera |
| A11 | Gestión Tecnológica | Red de datos | Herramienta | Software | Instalaciones de Ultraline Electrónica | Pública | A | 1 | Alta | Ultraline | Oficina Tecnología |
| A13 | Gestión Tecnológica | Sofware | Herramienta | Software | Instalaciones de Ultraline Electrónica | Clasificada | A | 1 | Alta | Ultraline | Oficina Tecnología |

Apéndice F – Carta dictamen de la auditoría

Barranquilla, 23 de noviembre de 2019

Recibido: Katherine Sagbini nov. 23 de 2019

Doctora
KATHERINE SAGBINI ECHAVEZ
Gerente Comercial
Ultraline Electrónica S.A.S.
Ciudad

Reciba un cordial saludo.

Nos permitimos comunicarle que durante los días del 15 al 22 de noviembre 2019, se realizó la auditoría de sistemas con el objetivo de detectar gran parte de inconsistencias en relación con el tratamiento de la seguridad de la información dentro de las dependencias de su organización. En estas oficinas se maneja información importante y crítica para cada uno de los procesos que lleva la empresa, lo que compromete los objetivos misionales de la organización, por lo tanto, presentamos de manera oficial los resultados obtenidos en el hallazgo de información.

Durante este tiempo se efectuaron actividades concernientes al tema de auditoría, teniendo como prioridad el análisis de cada uno de los procesos relacionados con el uso objetivo de la seguridad de la información en la empresa Ultraline ElectrónicaS.A.S.. Estos procesos se encuentran soportados bajo los ejes misionales de la organización en cuanto a temas importantes como son: su estructura organizacional, infraestructura tecnológica que incluye manejo de bases de datos, sistemas de información, cableado estructurado, hardware y software, esquema físico y lógico entre otros puntos, los cuales se encuentran focalizados bajo el estándar ISO 27001:2013. En este sentido, para el desarrollo de este análisis, se utilizaron diferentes instrumentos de recolección de información como son las entrevistas, cuestionarios y listas de chequeo.

Teniendo en cuenta lo anterior, en el informe anexo a ésta, se dan a conocer los hallazgos encontrado donde se mencionan las fallas encontradas las cuales provocan tanto deficiencias como ineficiencias en cada uno de los procesos incluyendo el capital humano que maneja la organización, siendo éste, uno de los principales puntos claves encontrados en la auditoria. Cabe mencionar que, la organización no cuenta con el personal establecido para realizar el tratamiento de la seguridad de la información, la aplicación de los controles tanto preventivos como correctivos para el seguimiento de las funciones y las actividades que abarcan los objetivos organizacionales de la empresa incluyendo todas sus dependencias. La empresa tiene una oficina de sistemas pero no adecuada para ejercer desde allí un control de la infraestructura tecnológica que permita establecer una mejora continua en el desarrollo de las actividades.

Por consiguiente, y resumiendo, la falta de un manual de buenas prácticas para garantizar la seguridad de la información, focalizado al manejo de políticas de información, es de gran relevancia e importancia para la empresa, dado que, en ésta no se lleva un control adecuado en cuanto al registro de incidentes que involucren el tema de seguridad de la información, más aun, no se realizan de forma adecuada los respaldos de la información y por tanto, no existen controles preventivos ni correctivos ante cualquier eventualidad o desastre natural.

Se hace necesario para el buen funcionamiento de la empresa, la gestión, aplicación, verificación e implementación de dichas políticas para lograr minimizar los riesgos que se presenten en las distintas dependencias en cualquier eventualidad dentro de la organización.

Elaborado por:

**Jenis del Carmen Sagbini Echavez**
Ing. de Sistemas, Auditor de Sistemas

Jefferson Farelo P.

**Jefferson Farelo Páez**
Ing. de Sistemas, Auditor de Sistemas

# Apéndice G : Componentes de Planificación que pueden ser aplicables a Ultraline Electrónica

| COMPONENTES DE PLANIFICACION QUE PUEDEN SER APLICABLES A ULTRALINE ELECTRÓNICA S.A.S. | | | | | |
|---|---|---|---|---|---|
| EMPRESA A AUDITAR: ULTRALINE ELECTRÓNICA S.A.S. | | | FECHA DE AUDITORÍA: | | Del 15 al 20 nov 2019 |
| **Id** | **Cargo** | **Item** | **Descripción** | **Prueba** | **MSPI** |
| P.1. | Responsable TI | Alcance del MSPI (Modelo de Seguridad y Privacidad de la Información) | Se hace necesario determinarlos límites y aplicabilidad del SGSI para determinar su alcance | El Documento del Alcance aprobado por Gerencia General y debe estar socializado. Ultraline debe determinar los aspectos que son necesarios para el cumplimiento de su objetivo y que afectan su capacidad en el logro de los resultados en le SGSI. (Apartado 5.3. del ISO 31000:2009). Los requisitos referidos en 4.2.: aSe deben determinar las partes interesadas que son pertinentes al SGSI. b) Los requisitos de las partes interesadas (se incluyen los requisitos legales y de reglamentación, así como las oblicaciones contractuales) c) Se deben incluir las dependencias internas y externas. | Componente de Planificación |
| P.2. | Responsable TI | Políticas de seguridad y privacidad de la información | Se hace necesario definir un conjunto de políticas para la seguridad de la información aprobada por la Gerencia General, publicada y comunicada a los empleados y a las partes externas que tienen relación con las operaciones de la empresa | a) Si son definidos los objetiovs y el alcance de la política. b) Si ésta se encuentra alineada con la estrategia y objetivos de la empresa o entidad c) Si fue debidamente aprobada y socializada en el interior de la entidad por la Gerencia General. Igualmente revisar si la política incluye: a) Definición de seguridad de la información b) Asignación de responsabilidad generales y específicas para la gestión de la Seguridad de la Información y roles definidos. c)Los procesos para manejar las desviaciones y las excepciones. Se hace necesario indagar sobre las personas responsables que se designen por parte de la Gerencia General. Verificar frencuencia y circunstancias en que se revisan y se actualizan. Tener en cuenta la fecha actual y una revisión anual como mínimo. | Componente de Planificación |
| P.3. | Calidad | Procedimientos de control documental del MSPI | Toda información documentada se debe controlar para asegurar que: a) esté disponible y su uso sea adecuado. B) La información esté protegida debidamente | Diseño de formatos de procesos y de procedimientos debidamente definidos y aprobado por un comité que integre el Sistema de Gestión de Calidad. Tener en cuenta: distribución, acceso uso, recuperación y como se almacenan | Componente de Planificación |
| P.4. | Responsable del Sistema de Información | Responsabilidades y roles para la seguridad de la información | Se hace necesario definir y asignar todas las responsabilidad de la seguridad de la información | El SGSI debe tener suficiente apoyo de la Gerencia General, tener claramente definidos los roles y las responsabilidades del personal responsable, tener identificadas los responsablies para la protección de los activos (se debe nombrar un propietario de activos quien se convierte en el responsable). Tener definidas las responsabilidad para la gestión del riesgo de Sistemas de Información y la aceptación de riesgos residuales. Definidos y documentados los niveles de autorización. Igualmente, contar conun presupuesto formal para las actividades del SGSI | Componente de Planificación |
| P.5. | Responsable TI | Identificación y valoración de riesgos | Metodología de analisis y valoración de riesgos e informs de análisis de riesgos | Establecer una metodología y criterios de riesgo de seguridad aprobado por la Gerencia General que incluya: 1) Criterios de aceptación y tolerancia al riesgo 2)Establecer criterios para realizar evaluaciones de riesgo 3) Cuantificar las evaluaciones repetidas de riesgo encontradas y sus resultados deben ser comparable 4) Que se hayan identificado los riesgos asociados con los tres elementos de la seguridad de la información: integridad, disponiblidad y confidencialidad 5) que se hayan identificado y analizado los dueños del riesgo evaluando su impacto y probailidades que ocurran | Componente de Planificación |
| P.6. | Responsable TI | Formación e interiorización en seguridad de la información tomando conciencia general | Se deberá dar formación en la toma de conciencia apropiada a todo el personal directo e indirecto sobre las políticas y procedimiento pertinentes sobre seguridad de la información | La Gerencia General deberá liderar un plan de comunicación y formación donde deberá tener soportes con revisión y aprobación para todo el personal de la organización directa e indirecta. Este plan deberá incluir campañas, folletos, boletines, planes que permita validar y comprobar el conocimiento y la toma de conciencia de cada funcionario sobre la importancia de cumplir las políticas de seguridad y privacidad de Ultraline Electrónica S.A.S. Se hace necesario que se verifique que los funcionarios con roles privilegiados entiendas sus responsabilidad (de acuerdo con NIST) | Componente de Planificación |

Prepararon: Jenis Sagbini Echávez y Jefferson Farello Paez

Apendíce H – Riesgos encontrados en Ultraline Electrónica S.A.S.

| Código | Activo | Riesgo | Calificación | | Tipo | Evaluación Zona de Riesgo |
|---|---|---|---|---|---|---|
| | | | Probabilidad | Impacto | | |
| R-1 | Canales de Comunicación | No existen políticas de control para la trasnferencia de información por cualquier medio | 3 | 4 | Integridad | E |
| R-2 | Canales de Comunicación | Los usuarios no realizan cambio periódico a las claves de acceso | 3 | 4 | Disponibilidad | E |
| R-3 | Documentos | No se cuenta con un manual de seguridad de la información implementado | 4 | 4 | Confidencialidad | E |
| R-4 | Documentos | No se realiza gestión y registro de incidentes pertenecientes a la seguridad de la información | 3 | 4 | Integridad | E |
| R-5 | Documentos | Fala de políticas de seguridad en el control de acceso y proceso de contratación de servicios y terceros | 4 | 4 | Confidencialidad | E |
| R-6 | Equipos de Cómputo | Falta de buenas prácticas en el uso de contraseñas en el SIC y al Sistema Operativo | 4 | 4 | Confidencialidad | E |
| R-7 | Equipos de Cómputo | Ausencia de un protocolo seguro para las copias de seguridad y restauración | 4 | 4 | Disponibilidad | E |
| R-8 | Equipos de Cómputo | No se cuenta con un procedimiento adecuado para la eliminación de información de manera segura de los equipos de cómputo y demás dispositivos | 3 | 4 | Integridad | E |
| R-9 | Equipos tecnológicos | No existe un control adecuado para el acceso al Rack de equipos ubicado en la oficina del Contador. | 3 | 4 | Integridad | E |
| R-10 | Equipos de Cómputo | Ausencia de un informe mensual de los cambios o soportes en hardware/sofwtare por parte del Ingeniero de Soporte contratista | 4 | 4 | Confidencialidad | E |

| Código | Activo | Riesgo | Calificación | | Tipo | Evaluación Zona de Riesgo |
|---|---|---|---|---|---|---|
| | | | Probabilidad | Impacto | | |
| R-11 | Equipos de Cómputo | Los equipos de Ultraline Electrónica no cuentan con un antivirus licenciado o algún dispositivo firewall que controle accesos a la red. Usan el antivirus de Microsoft | 4 | 4 | Integridad | E |
| R-12 | Equipos de Cómputo | Falta de políticas de control y detección de Ransomware y Malware | 4 | 4 | Integridad | E |
| R-13 | Equipos de seguridad Incendios | No se cuenta con un sistema de seguridad contra incendios (detección de humo) | 4 | 4 | Integridad | E |
| R-14 | Equipos de seguridad Incendios | Existen extintores pero no son suficientes para la zona y el control de cambios/mtto no existe | 4 | 4 | Integridad | E |
| R-15 | Equipos de seguridad Incendios | No existe un plan de contingencia en caso de emergencias o desastres naturales | 4 | 4 | Integridad | E |
| R-16 | Equipos de seguridad | No existe un método de cifrado de información para el manejo de datos de alto riesgo | 4 | 4 | Confidencialidad | E |
| R-17 | Equipos tecnológicos | No se cuenta con un control permanente para el manejo de dispositivos pendrive. | 3 | 4 | Disponibilidad | E |
| R-18 | Información | No existen políticas de seguridad de lainformación | 4 | 4 | Confidencialidad | E |
| R-19 | Infrestructura física y tecnológica | Malas condiciones de espacio en la oficina TI ubicada en la oficina de la Contadora sin ninguna restricción | 3 | 4 | Integridad | E |
| R-20 | Infrestructura física y tecnológica | Se carecen de restricción y políticas para la seguridad de acceso a la oficina del contador y TI | 4 | 4 | Integridad | E |

| Código | Activo | Riesgo | Calificación | | Tipo | Evaluación Zona de Riesgo |
|---|---|---|---|---|---|---|
| | | | Probabilidad | Impacto | | |
| R-21 | Infrestructura física y tecnológica | No se han realizado auditorías de sistemas a la red ni al cableado estructurado | 4 | 4 | Integridad | E |
| R-22 | Infrestructura física y tecnológica | Las instalaciones no cuentan con la señalización adecuada para establecer las rutas de evacuación y demás | 3 | 4 | Integridad | E |
| R-23 | Medios de almacenamiento extraíbles | Malos manejos en los almacenamientos de información utilizando medios magnéticos en diferentes dependencias | 4 | 4 | Integridad | E |
| R-24 | Nodos de comunicación | No existe un control o bitácora para cambios y acceso a los rack de comunicación | 4 | 4 | Disponibilidad | E |
| R-25 | Nodos de comunicación | No existen herramientas para la protección contra código malicioso | 4 | 4 | Integridad | E |
| R-26 | Recurso humano | No existe una oficina de sistemas o soporte específica para el trabajo del Ingeniero contratista que soporte el Sistema de Seguridad de la Inform | 3 | 4 | Disponibilidad | E |
| R-27 | Recurso humano | Falta de entrenamiento y capacitación al personal administrativo y operativo sobre la seguridad de la información | 4 | 4 | Disponibilidad | E |
| R-28 | Red de Datos | No se tiene documentado los acontecimientos dentro de la red de datos por falas | 4 | 4 | Integridad | E |
| R-29 | Servicios Püblicos | No se cuenta con un sistema de contingencia en caso de falla la energía eléctrica. | 4 | 4 | Integridad | E |

# Apéndice I – Controles identificados en las áreas administrativas de Ultraline Electrónica

| Cód | Activo | Riesgo | Calificación | | Tipo | Evaluación Zona de Riesgo | Medida de Respuesta | Controles | Tipo de Control | Nueva Calificación | | Evaluación zona de riesgo | Medida de Respuesta |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Probabilidad | Impacto | | | | | | Probabilid | Impacto | | |
| C1 | Canales de Comunicación | No existen políticas de control para la trasnferencia de información por cualquier medio | 3 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Realizar una Política para establecer los procedimientos adecuado en dicha situación | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C2 | Canales de Comunicación | Los usuarios no realizan cambio periódico a las claves de acceso | 3 | 4 | Disponibilidad | E | Reducir el riesgo, evitar, compartir o transferir | El Responsable de TI deberá implementar el cambio de claves previa socialización con Gerencia General | Correctivo | 2 | 3 | M | Asumir el riesgo |
| C3 | Documentos | No se cuenta con un manual de seguridad de la información implementado | 4 | 4 | Confidencialidad | E | Reducir el riesgo, evitar, compartir o transferir | Creación de un manual de seguridad de la información y socializarlo con el personal | Correctivo | 2 | 4 | A | Reducir el riesgo, evitar, compartir o transferir |
| C4 | Documentos | No se realiza gestión y registro de incidentes pertenecientes a la seguridad de la información | 3 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Creación de un comité de ayuda del Responsable TI para registrar y gestionarlos tipos de incidente de seguridad de la información | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C5 | Documentos | Falta de políticas de seguridad en el control de acceso y proceso de contratación de servicios y terceros | 4 | 4 | Confidencialidad | E | Reducir el riesgo, evitar, compartir o transferir | Crear un comité de mejoras para los proceso de contratación de terceros y políticas de acceso a los mismos | Correctivo | 1 | 2 | B | Asumir el riesgo |
| C6 | Equipos de Cómputo | Falta de buenas prácticas en el uso de contraseñas en el SIC y al Sistema Operativo | 4 | 4 | Confidencialidad | E | Reducir el riesgo, evitar, compartir o transferir | Realizar capacitación al personal de cada dependencia involucrada | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C7 | Equipos de Cómputo | Ausencia de un protocolo seguro para las copias de seguridad y restauración | 4 | 4 | Disponibilidad | E | Reducir el riesgo, evitar, compartir o transferir | Hacer capacitación al personal involucrado | Correctivo | 1 | 3 | M | Asumir el riesgo |
| C8 | Equipos de Cómputo | No se cuenta con un procedimiento adecuado para la eliminación de información de manera segura de los equipos de cómputo y demás dispositivos | 3 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Crear un Comité de Mejora de las políticas de SI que involucre el borrado seguro | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C9 | Equipos tecnológicos | No existe un control adecuado para el acceso al Rack de equipos ubicado en la oficina del Contador. | 3 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Sugerir la adquisición en el 2020 de nuevos equipos de control | Correctivo | 2 | 4 | A | Reducir el riesgo, evitar, compartir o transferir |
| C10 | Equipos de Cómputo | Ausencia de un informe mensual de los cambios o soportes en hardware/sofwtare por parte del Ingeniero de Soporte contratista | 4 | 4 | Confidencialidad | E | Reducir el riesgo, evitar, compartir o transferir | Diseñar un procedimiento donde se registren los cambios en hardware y/o software | Correctivo | 2 | 4 | A | Reducir el riesgo, evitar, compartir o transferir |

| Cód | Activo | Riesgo | Calificación | | Tipo | Evaluación Zona de Riesgo | Medida de Respuesta | Controles | Tipo de Control | Nueva Calificación | | Evaluación zona de riesgo | Medida de Respuesta |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Probabilidad | Impacto | | | | | | Probabilidad | Impacto | | |
| C11 | Equipos de Cómputo | Los equipos de Ultraline Electrónica no cuentan con un antivirus licenciado o algún dispositivo firewall que controle accesos a la red. Usan el antivirus de Microsoft | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Plantear la posibilidad de adquirir un antivirus licenciado para los equipos de Ultraline Electróncia | Correctivo | 1 | 4 | B | Asumir el riesgo |
| C12 | Equipos de Cómputo | Falta de políticas de control y detección de Ransomware y Malware | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Capacitación sobre amenazas dentro de la red y equipos a todo el personal usuario | Correctivo | 1 | 4 | A | Asumir el riesgo, reducir el riesgo |
| C13 | Equipos de seguridad Incendios | No se cuenta con un sistema de seguridad contra incendios (detección de humo) | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Proponer a la Gerencia General la implementación de un sistema de seguridad contra incendio | Correctivo | 1 | 3 | M | Asumir el riesgo, reducir el riesgo |
| C14 | Equipos de seguridad Incendios | Existen extintores pero no son suficientes para la zona y el control de cambios/mtto no existe | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Diseñar políticas de seguridad para controlar el tiempo y cambio de extintores | Correctivo | 1 | 3 | M | Asumir el riesgo, reducir el riesgo |
| C15 | Equipos de seguridad Incendios | No existe un plan de contingencia en caso de emergencias o desastres naturales | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Diseñar e implementar un plan de contingencia para evacuación y emergencias | Correctivo | 2 | 4 | A | Reducir el riesgo, evitar, compartir o transferir |
| C16 | Equipos de seguridad | No existe un método de cifrado de información para el manejo de datos de alto riesgo | 4 | 4 | Confidencialidad | E | Reducir el riesgo, evitar, compartir o transferir | Comprar herramientas que permitan cifrado de datos e implementar en las dependencias que lo requieran | correctivo | 1 | 4 | A | Asumir el riesgo, reducir el riesgo |
| C17 | Equipos tecnológicos | No se cuenta con un control permanente para el manejo de dispositivos pendrive. | 3 | 4 | Disponibilidad | E | Reducir el riesgo, evitar, compartir o transferir | Crear un control para el no uso de pendrive | Correctivo | 2 | 4 | A | Reducir el riesgo, evitar, compartir o transferir |
| C18 | Información | No existen políticas de seguridad de lainformación | 4 | 4 | Confidencialidad | E | Reducir el riesgo, evitar, compartir o transferir | Diseñar e implementar un plan de contingencia para evacuación y emergencias | correctivo | 2 | 4 | A | Asumir el riesgo |
| C19 | Infrestructura física y tecnológica | Malas condiciones de espacio en la oficina TI ubicada en la oficina de la Contadora sin ninguna restricción | 3 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Realizar el traslado de los equipos y herramientas para conformar una oficina en un lugar más adecuado optimizando la labor del Responsable de TI | correctivo | 2 | 4 | A | Asumir el riesgo |
| C20 | Infrestructura física y tecnológica | Se carecen de restricción y políticas para la seguridad de acceso a la oficina del contador y TI | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Crear una política de ingreso a áreas restringidas como la oficina del contador y otras que manipulen información | Correctivo | 1 | 4 | A | Asumir el riesgo |

| Cód | Activo | Riesgo | Calificación | | Tipo | Evaluación Zona de Riesgo | Medida de Respuesta | Controles | Tipo de Control | Nueva Calificación | | Evaluación zona de riesgo | Medida de Respuesta |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Probabilidad | Impacto | | | | | | Probabilid | Impacto | | |
| C21 | Infrestructura física y tecnológica | No se han realizado auditorías de sistemas a la red ni al cableado estructurado | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Diseñar y desarrollar un plan de auditoría a funcionarios encargados de áreas donde llevan actividad de mayor concentración de información | Correctivo | 1 | 2 | B | Asumir el riesgo |
| C22 | Infrestructura física y tecnológica | Las instalaciones no cuentan con la señalización adecuada para establecer las rutas de evacuación y demás | 3 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Plantar la adquisión e implementación de una señalización adecuada de rutas de evacuación y demás | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C23 | Medios de almacenamiento extraíbles | Malos manejos en los almacenamientos de información utilizando medios magnéticos en diferentes dependencias | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Capacitación al personal de las dependencias en el tema del riesgo al usar medios magnéticos sin las precauciones adecuadas | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C24 | Nodos de comunicación | No existe un control o bitácora para cambios y acceso a los rack de comunicación | 4 | 4 | Disponibilidad | E | Reducir el riesgo, evitar, compartir o transferir | Implementar controles de registro y cambios | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C25 | Nodos de comunicación | No existen herramientas para la protección contra código malicioso | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Crear las Políticas de seguridad | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C26 | Recurso humano | No existe una oficina de sistemas o soporte específica para el trabajo del Ingeniero contratista que soporte el Sistema de Seguridad de la Inform | 3 | 4 | Disponibilidad | E | Reducir el riesgo, evitar, compartir o transferir | Crear una oficina para el ingeniero responsable de TI y un comité como apoyo para controlar el tema de gestión de seguridad de la información | Correctivo | 2 | 4 | A | Reducir el riesgo, evitar, compartir o transferir |
| C27 | Recurso humano | Falta de entrenamiento y capacitación al personal administrativo y operativo sobre la seguridad de la información | 4 | 4 | Disponibilidad | E | reducir el riesgo, evitar, compartir o transferir | Crear una capacitación para informar sobre gestión de seguridad de la información | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C28 | Red de Datos | No se tiene documentado los acontecimientos dentro de la red de datos por falas | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Diseñar e implementar política para el registro de cada acontecimiento dentro de la red que reciba atención y monitoreo constante | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |
| C29 | Servicios Pùblicos | No se cuenta con un sistema de contingencia en caso de falla la energía eléctrica. | 4 | 4 | Integridad | E | Reducir el riesgo, evitar, compartir o transferir | Proponer una propuesta de implementación de un sistema de contingencia y socializarlo con el área involucrada | Correctivo | 1 | 3 | M | Reducir el riesgo, evitar, compartir o transferir |

Apéndice J – Acta de reunión capacitación y establecimiento de controles

| UltraLine | ULTRLINE ELECTRONICA S.A.S.<br>ACTA DE REUNIÓN | SGI – FOR02-Actas<br>VERSIÓN 1<br>PAG 1 DE 1<br>Fecha: Diciembre 16 de 2019 |
|---|---|---|

Oficina de Tecnologías de Información

Empresa: Ultraline Electrónica S.A.S.
Proceso: Proyecto Sistema de Gestión de Seguridad de la Información
Fecha:16 diciembre de 2019
Lugar: Salón principal Ultraline Electrónica S.A.S.
Duración : 4 horas
Participantes:
CARLOS JULIO CUELLO – Gerente General, KAREN JIMENEZ – Asistente Administrativa, MARIA JOSE OROZCO – Asistente Administrativa, CATHERINE SAGBINI – Gerente Comercial, GERMAN NAVARRO- Jefe de Almacén, JEAN CARLOS RODRIGUEZ - Aux de Almacén, LUCY IGLESIAS- Contadora, MARIA LUISA TORRES-Auxiliar Contable, OSCAR RUBIO-Jefe de Producción, LUIS PERUZ, DEIRAN OJEDA, ESTEVEN RIQUET, JULIO MUÑOZ, WILBER MUÑOZ, STEVEN RIQUET – Técnicos. Por parte de la empresa Novarrety: JAIME VELASQUEZ- Responsable TI y JUAN SEBASTIAN MERCADO-practicante SENA, JENIS SAGBINI Y JEFFERSON FARELO- Líderes del proyecto SGSI

***Objetivo de la Capacitación:***

Analizar y establecer el ciclo de controles pertinenetes para aplicar la política de seguridad de la información en la oficina del Responsable TI de Ultraline Electrónica S.A.S.

**DESARROLLO**

1. La señora Catherine Sagbini inició la jornada elevando una oración a Dios y agradeciendo la presencia de todo el personal convocado. Hizo presentación del personal del proyecto y del Responsable de TI, representante de la empresa Navarrety.
2. Los ingenieros Jenis Sagbini y Jefferson Farello dieron inicio a la reunión donde resumieron de forma abreviada el objetivo del proyecto, los avances alcanzados a la fecha y la fase en que se encuentran conr especto a la prueba piloto.
3. La ingeniera Jenis Sagbini leyó la política de seguridad de la información y por cada punto que se leía, se hizo una lluvia de ideas. El señor Jaime Velasquez, Responsable de TI preguntó como se evidenciará cada parte de esa políaca. El ingeniero Jefferson Farelo explicó que cada 3 meses sería necesario hacer un seguimiento . Igualmente explicó que con base a la política, se debe establecer un control asociado.
4. Después de realizar la sensibilización sobre las políticas, riesgos y la recopilación de ideas, los ingenieros directores del proyecto, le pidieron al seño Jaime Velasquez que leyera la conclusión que estableció el ingeniero Jefferson Farelo y estimaran conveniente explicar las dudas que quedaran al final. El resumen quedó de la siguiente forma:

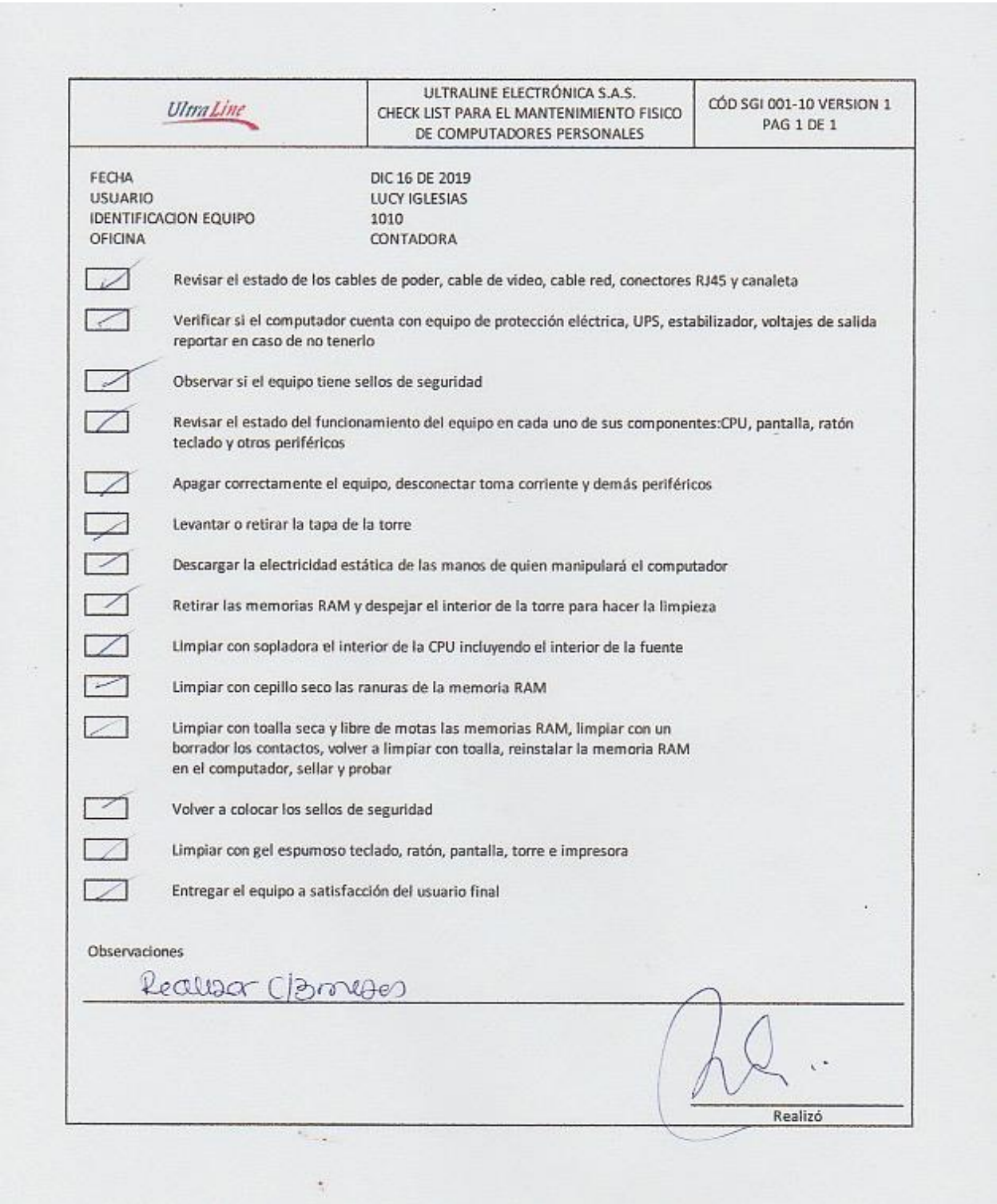
Minimizar los riesgos pertinentes con la seguridad de la información a través de aplicar controles en cuanto a mantenimientos preventivos, cumplimiento de los principios de seguridad de la información, concientización de todos los empleados en cuanto a tomar conciencia de sus responsabilidades de en el tema de las políticas de seguridad de la información y a su cumplimiento.
Brindar un apoyo constante y la conformación del comité de protección de la seguridad de la información como soporte al Responsable de TI.
Se estableció como factor importante, el seguimiento y control a través del Check list diseñado y el cumplimiento de los indicadores que serán diseñados con apoyo de la Gerencia General.

Se dijo la importancia sobre la continuidad de la implementación del Plan de Capacitación de manera frecuente y que los controles deberán ser actividades importantes para cada cargo dentro de la organización.

Siendo las 12 m, se dio por terminada la reunión, firman los asistentes:

| Nombre y Apellido | Cargo | Firma |
|---|---|---|
| CARLOS JULIO CUELLO | GERENTE GENERAL | |
| CATHERINE SAGBINI | GERENTE COMERCIAL | |
| MARIA JOSE OROZCO | ASISTENTE ADTIVA | |
| KAREN JIMENEZ | ASISTENTE ADTIVA | |
| LUCY IGLESIAS | CONTADORA | |
| MARIA LUISA TORRES | AUXILIAR CONTABLE | |
| OSCAR RUBIO | JEFE DE PRODUCCION | |
| GERMAN NAVARRO | JEFE DE ALMACEN | |
| LUIS PERTUZ | TECNICO | |
| DEIRAN OJEDA | TECNICO | |
| ESTEVEN RIQUET | TECNICO | |
| JULIO MUÑOZ | TECNICO | |
| WILBER MUÑOZ | TECNICO | |
| JULIO MUÑO JUNIOR | TECNICO | |
| JAIME VELASQUEZ | RESPONSABLE TI | |
| JUAN SEBASTIAN MERCADO | ESTUDIANTE PRACTICANTE | |
| JENIS SAGBINI | LIDER PROYECTO SGSI | |
| JEFFERSON FARELLO | LIDER PROYECTO SGSI | |

Apéndice K – Aplicación del Check List para el cumplimiento del mtto físico de computadores



| UltraLine | ULTRALINE ELECTRÓNICA S.A.S.<br>CHECK LIST PARA EL MANTENIMIENTO FISICO DE COMPUTADORES PERSONALES | CÓD SGI 001-10 VERSION 1<br>PAG 1 DE 1 |
|---|---|---|

| | |
|---|---|
| FECHA | DIC 16 DE 2019 |
| USUARIO | LUCY IGLESIAS |
| IDENTIFICACION EQUIPO | 1010 |
| OFICINA | CONTADORA |

- [x] Revisar el estado de los cables de poder, cable de video, cable red, conectores RJ45 y canaleta
- [x] Verificar si el computador cuenta con equipo de protección eléctrica, UPS, estabilizador, voltajes de salida reportar en caso de no tenerlo
- [x] Observar si el equipo tiene sellos de seguridad
- [x] Revisar el estado del funcionamiento del equipo en cada uno de sus componentes:CPU, pantalla, ratón teclado y otros periféricos
- [x] Apagar correctamente el equipo, desconectar toma corriente y demás periféricos
- [x] Levantar o retirar la tapa de la torre
- [x] Descargar la electricidad estática de las manos de quien manipulará el computador
- [x] Retirar las memorias RAM y despejar el interior de la torre para hacer la limpieza
- [x] Limpiar con sopladora el interior de la CPU incluyendo el interior de la fuente
- [x] Limpiar con cepillo seco las ranuras de la memoria RAM
- [x] Limpiar con toalla seca y libre de motas las memorias RAM, limpiar con un borrador los contactos, volver a limpiar con toalla, reinstalar la memoria RAM en el computador, sellar y probar
- [x] Volver a colocar los sellos de seguridad
- [x] Limpiar con gel espumoso teclado, ratón, pantalla, torre e impresora
- [x] Entregar el equipo a satisfacción del usuario final

Observaciones

Realizar Cambios

Realizó