RESUMEN – TRABAJO DE GRADO

AUTORES	**JOAQUIN GUERRERO MELO** **FRANCISCO JAVIER SUAREZ CASTRELLON**
FACULTAD	**INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**YESICA MARIA PEREZ PEREZ**
TÍTULO DE LA TESIS	**PLANEACION DEL SISTEMA DE GESTIÓN DE SEGURIAD DE LA INFORMACION APLICANDO LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN ÁREA CONTABLE EN LA EMPRESA TRANSFORMADORES CDM**

RESUMEN
(70 palabras aproximadamente)

ESTE PROYECTO DOCUMENTA LA PLANEACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN ALICANDO LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN EL ÁREA CONTABLE DE LA EMPRESA TRANSFROMADORES CDM, Y CADA UNO DE LOS PROCESOS NECESARIOS PARA ELLO; RESALTANDO EL PREVIO ANALISIS DE RIESGOS QUE PERMITIO ENCAMINAR EL DESARROLLO DEL PROYECTO A LAS ÁREAS MAS VULNERABLES DE LA UNIDAD.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:
76			

PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN ÁREA CONTABLE EN LA EMPRESA TRANSFORMADORES CDM.

JOAQUIN GUERRERO MELO
FRANCISCO JAVIER SUAREZ CASTRELLON

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
FACULTAD DE INGENIERIAS
OCAÑA
2016

PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN ÁREA CONTABLE EN LA EMPRESA TRANSFORMADORES CDM.

JOAQUIN GUERRERO MELO
FRANCISCO JAVIER SUAREZ CASTRELLON

Trabajo de grado presentado como requisito para optar el título de Especialista en Auditoría de Sistemas

MdE (c).Esp. YESICA MARIA PEREZ PEREZ
Ingeniera de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
FACULTAD DE INGENIERIAS
OCAÑA
2016

TABLA DE CONTENIDO

LISTA DE TABLAS

Pág.

LISTA DE GRAFICAS

Pág.

LISTA DE IMÁGENES

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados" Gene Spafford, con esta frase debemos reconocer que la información no está 100 % protegida pero si podremos minimizar el riesgo para que no sea objeto de ataques cibernético, robos de información y virus informáticos. Es por eso que en este proyecto de planeación del sistema de seguridad de la información, la norma internacional ISO/TEC 27001 fue aplicada en área contable en la empresa TRANSFORMADORES CDM para la protección de la información de esta área específica y poder realizar protocolos para no caer en los problemas e informar a los usuarios lo que deben saber para no caer fácilmente en ataques externos o virus informáticos y posible pérdida de información.

1 PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN ÁREA CONTABLE EN LA EMPRESA TRANSFORMADORES CDM.

1.1 PLANTEAMIENTO DEL PROBLEMA

Los procesos relacionados con garantizar la seguridad de la información de una empresa deben estar certificados y amparados en la aplicación de normas como la ISO 27001:2013 en la donde se establecen buenas prácticas en el manejo de la información. Pero ¿porque esta norma puede ser de utilidad para resolver del problema particular de este estudio? La respuesta este interrogante se puede orientar a que esta norma *"está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001*."[1]

Sin embargo, en la el área contable de la empresa transformadores CDM, no se encuentran implementados procesos ni políticas que protejan, controlen y salvaguarden la información y los activos correspondientes, lo cual representa una gran debilidad organizacional dada la importancia de los mismos. El sistema de hacer frente a los riesgos en esta área es reactivo, es decir es común, encontrar casos en los cuales se actúa cuando la amenaza se vuelve un problema real y la pérdida de información o entorpecimiento en los procesos diarios de la empresa empieza a aparecer. De tal forma, que estos daños solo son corregidos con la intervención de una empresa contratada, al identificar la falta de controles, sin embargo esta práctica también se convierte en un riesgo ya que equipos, discos duros y otros activos son traslados fuera de las instalaciones de CDM y la información queda expuesta a personas no autorizadas.

De otra parte, es clara la ineficiencia de la gestión de la seguridad de la información actual y se convierte en una carga financiera significativa para la empresa. En promedio, al día se presentan 4 altibajos del sistema eléctrico, además de inyección de virus por parte de proveedores, visitantes y clientes, lo cual afecta el funcionamiento de los equipos del área contable de transformadores CDM. Tomando como base la información registrada en los formatos de mantenimientos interno de la empresa, se ha llegado a establecer que por causa de daños informáticos se pierden alrededor de 15 horas al mes, que representan para la compañía un valor aproximado de 2.600.000 pesos mensuales en cambios de partes y mantenimientos correctivos de software.

[1] 27001 ACADEMY. ¿Qué es Norma ISO 27001? Una introducción simple a los aspectos básicos [en línea]. Actualizado en el 2015. [Citado en agosto 20 de 2015]. Disponible en Internet en: (http://advisera.com/27001academy/es/que-es-iso-27001/)

Como se expone anteriormente, el área de contabilidad se enfrenta a problemas relacionados con la frecuente de pérdida de información, falta de controles de acceso, falta de procedimientos para la gestión de activos, falta de control de acceso a conexiones wifi y medios de almacenamientos como USBs y discos duros externos, entre otros. Por tanto la implementación de un sistema de seguridad de información que garantice la confidencialidad, integridad y disponibilidad de los datos, en dicha área se hace relevante y urgente para la empresa transformadores.

La implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:13tiende a minimizar el impacto de los riesgos de la pérdida de información y daños en hardware, como los descritos anteriormente. El área contable de transformadores CDM se puede beneficiar sustancialmente de la adopción de la norma y generar un ahorro mensual en materia de daños informáticos, integrándose adecuadamente con el planteamiento estratégico y las políticas de mejoramiento continúo de la organización.

1.2 FORMULACION DEL PROBLEMA

¿Mediante un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013 se puede gestionar los riesgos asociados al uso de la información de los sistemas y servicios informáticos utilizados en el área de contabilidad la empresa transformadores CDM?

1.3 OBJETIVOS

1.3.1 General. Planificar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013 en el área de contabilidad de la empresa de transformadores CDM, que permita establecer mecanismos que mitiguen los riesgos asociados.

1.3.2 Objetivos específicos. Realizar un diagnóstico de la seguridad de la información en el área de contabilidad de la empresa de transformador CDM, basado en la norma ISO/IEC 27001:2013.

Realizar la planificación de la gestión riesgos asociados a la seguridad de la información en el área de contabilidad en la empresa transformadores CDM.

Documentar el plan de acción a seguir para la implementación del Sistema de Gestión de Seguridad de la Información en el área de contabilidad de la empresa transformadores CDM.

1.4 JUSTIFICACIÓN

¿Alguna vez ha intentado convencer a los directores de su empresa de que financien la implementación de la seguridad de la información? Si lo ha hecho, probablemente sepa qué se siente: le preguntarán cuánto cuesta y, si les parece muy caro, le dirán que no.

En realidad, no deberíamos culparlos; después de todo, su principal responsabilidad es la rentabilidad de la empresa. Esto quiere decir que cada decisión que tomen se basará en la relación entre inversión y beneficio; o, para expresarlo en el lenguaje de gestión, tendrá en cuenta el ROI (rendimiento de la inversión)[2]

Las empresas actualmente se enfatizan solo en lo tecnológico, sin tomar en cuenta que la seguridad de la información es un problema que se debe mitigar y generar controles para su buen uso y funcionamiento, esto con lleva a generaran inconvenientes que no se puedan afrontar con tiempo y rapidez.

La seguridad puede verse alertada en diferentes ángulos de vista: el mal uso de la tecnología y la falta de asesoría de expertos en seguridad de la información.

Desde el punto de vista de la alta gerencia, un SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) permite obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos, además de poder observar las medidas de seguridad aplicadas y los resultados obtenidos, para poder con todos estos elementos tomar mejores decisiones estratégicas. Otro punto importante es que un SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) debe estar documentado y ser conocido a distintos niveles por todo el personal, y estar incluido en un proceso global que permita la mejora continua.

Mediante El diseño del SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) la empresa transformadores ACM establecerá mecanismos para mitigar riesgos que afectan la productividad de la empresa debido a la ocurrencia de eventos que comprometan la confidencialidad, disponibilidad e integridad de la información.

En la forma que apliquemos la norma 27001 y las metodologías que utilicemos daremos un gran paso a la hora de garantizar que la información del área contable de la empresa mejorara y podrá ser capaz de saber qué hacer en determinados eventos que pasen en sus puestos de trabajo, teniendo unas políticas establecidas y con personal capacitado podrán

[2] 27001 ACADEMY. Cuatro beneficios claves de la implementación de la Norma ISO 27001. [en línea]. Actualizado en el 2015. [Citado en agosto 20 de 2015]. Disponible en Internet en: (http://advisera.com/27001academy/es/blog/2010/07/21/cuatro-beneficios-clave-de-la-implementacion-de-la-norma-iso-27001/)

tomar las decisiones de que hacer o a quien acudir para no permitir que personas no autorizadas realicen daños en sus sistema de información.

Una vez concluida esta investigación y si deciden implementarla hará una reducción significativa de problemas que puedan tener perdida de información, adulteraciones en sus datos o robo de los mismos.

1.5 HIPOTESIS

El diseño de un sistema de gestión de seguridad de la información será el punto de partida dar cumplimiento a las características de la seguridad de la información como son confiabilidad, integridad, disponibilidad, no repudio y trazabilidad.

El diseño del SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) será una carta de navegación que permitirá abarcar todos los procesos de la empresa inicialmente contable, investigando los procesos actuales que tiene la empresa analizar el planteamiento de las políticas de seguridad de la información y así mejorar la estructura actual que es casi nula en el área de contabilidad de transformadores CDM.

1.6 DELIMITACIONES

1.6.1 Geográficas. Este proyecto se desarrollara en el área contable de la empresa transformadores CDM ubicada en Villa del Rosario, (Norte de Santander).

1.6.2 Temporales. La realización de este proyecto tiene un tiempo estimado de 3 meses después de la aprobación de la propuesta.

1.6.3 Conceptuales. El proyecto se encuentra enmarcado dentro de los conceptos o lineamientos guiados por la norma ISO/IEC 27001:2013 aplicando políticas de seguridad de la información.

2 MARCO REFERENCIAL

2.1 MARCO HISTORICO

La información actualmente es considerada un activo que representa gran valor para cualquier organización. Por tal motivo, se hace necesario protegerla y darle un manejo adecuado a la misma con el fin de evitar impactos significativos que pueden ser causados por agentes externos o interno que permanentemente se encuentran a esperas para aprovechar las vulnerabilidades o puntos débiles que presentan los sistemas de información en las organizaciones. Cabe aclarar, que los sistemas de información están compuestos por activos que cumplen funciones dentro de los mismos. Estos activos son las personas, el hardware, el software, los procesos, la infraestructura y la misma información, entre otros. Para este proyecto se consideran activos de información los mencionados anteriormente.

Dichos activos están sujetos a ser atacados por amenazas que de no controlarse pueden causar impactos en la información y en efecto a la organización reflejándose en pérdidas económicas y de imagen. Así de esta manera, la alta dirección de cualquier organización debe ser consciente de que su información siempre se encontrará en riesgo y que debe tomar las medidas necesarias para enfrentarse a este tipo de adversidades. [3]

2.1.1 Antecedentes. Transformadores CDM una empresa colombiana dedicada a la fabricación, reparación, reconstrucción y mantenimiento de transformadores de distribución y media potencia.

A través de su experiencia de más de 20 años, ha logrado posicionarse en el mercado como una de las mejores empresas a nivel nacional que dedica su mayor atención a la reparación de transformadores de distribución y media potencia.
Cuenta con personal e instalaciones altamente calificadas, que le permiten ofrecer un producto y servicio de excelente calidad. Por el cumplimiento de sus compromisos y amplia experiencia, En octubre 21 de 1999 certifico el sistema de aseguramiento de la calidad por primera vez de conformidad con la norma ISO 9002, por parte de BUREAU VERITAS QUALITY INTERNATIONAL.

En diciembre de 2002 se renueva la certificación del sistema de gestión de calidad de conformidad con la norma ISO-9001 versión 2000 por parte del ICONTEC, con alcance para: producción, reconstrucción, reparación y venta de transformadores de distribución monofásicos y trifásicos. Producción y venta de soldadores por arco eléctrico y ensamble de medidores electrónicos.

[3] QUINTANA, Yesid. TORRADO, Wilson. Planeación del sistema de gestión de seguridad de la información para la empresa "katalinda shoes". Ocaña 2015. Trabajo de Grado. Especialización e Auditoria de Sistemas. UFPSO. Facultad de Ingenierías. Pág. 18

En Octubre del 2005 TRANSFORMADORES CDM LTDA se inscribe por primera vez al Registro de Evaluación de programas de Salud Ocupacional y Medio Ambiente para Contratistas, con el fin de lograr en conjunto con las empresas operadoras del sector el desarrollo armónico de la Seguridad, la Salud Ocupacional y la protección Ambiental.

En marzo del 2009 se obtiene la certificación del sistema de gestión de calidad bajo el modelo de la norma iso-9001 versión 2008 y en febrero del 2010 se logra obtener la certificación en sistema integrado de gestión (sig) en cumplimiento de los requisitos de las normas iso-9001:2008; sistema de gestión de calidad, iso-14001:2004; sistema de gestión ambiental y OHSAS 18001:2007; sistema de gestión en seguridad y salud ocupacional, con el ICONTEC. Definiendo el siguiente alcance: fabricación, reparación, reconstrucción, mantenimiento y comercialización de transformadores; fabricación y comercialización de equipos de soldadura por arco eléctrico; ensamble y comercialización de medidores de energía.

2.2 MARCO CONCEPTUAL

Seguridad de la Información. La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.[4]

La Información. La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en 20 películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida. [5]

[4] ISO/IEC 27001. Norma ISO sobre Seguridad Informática. Resumen. Estándar ISO/IEC Internacional 17799. Introducción. Que es la seguridad de la Información. Segunda edición 2015-06.15.
[5] Ibíd., ISO/IEC 27001.

Riesgo. Riesgo es una palabra antigua y de uso común en muchas lenguas. En su uso corriente denota incertidumbre asociada a un evento futuro o a un evento supuesto. Una descripción con sentido común del término riesgo debería incluir las circunstancias que amenacen con disminuir la seguridad, el bienestar social, la salud, el bienestar y la libertad de una entidad determinada. Esta descripción no apunta a definiciones técnicas o específicas del riesgo, pero ejemplifica el rango de aplicaciones que posee ese término y aclara que el concepto de riesgo está estrechamente ligado a valores humanos significativos. El riesgo puede consistir en la mera posibilidad de un hecho adverso, en la causa de un evento, en la magnitud de la consecuencia, en alguien o algo considerado como peligroso y también en la conceptualización de un procedimiento para la estimación de una cantidad. En un sentido genérico el riesgo incluye una variedad de aspectos, todos los cuales constituyen el concepto de riesgo. Es obvio el enfoque futuro de estas acepciones, aunque el riesgo puede también considerarse desde una perspectiva histórica cuando es interpretado desde el punto de vista de aquellos que están involucrados. [6]

Amenaza. Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. [7]

Control. Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.[8]

Riesgo Se refiere a la incertidumbre o probabilidad de que una amenaza se materialice utilizando la vulnerabilidad existente de un activo o grupo de activos, generándole pérdidas o daños.

Integridad. Se considera a la propiedad de salvaguardar la exactitud y estado completo de los activos.

Confidencialidad. Se refiere a la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad. Es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

2.3 MARCO CONTEXTUAL

El desarrollo de la investigación se llevara a cabo en el Área de Contabilidad de la Empresa Transformadores CDM de Villa del Rosario, Norte de Santander, Colombia, donde se realizará el diseño del Sistema de Gestión de Seguridad de la Información.

[6] ISO/IEC 27001. op. cit
[7] ISO 27000. El portal de ISO 27001 en español. Glosario. [en línea]. Actualizado en el 2012. [Citado en septiembre 2015]. Disponible en Internet en: (http://www.iso27000.es/glosario.html)
[8] ISO 27002. Norma Técnica Colombiana. Términos y definiciones. ICONTEC Internacional.

2.4 MARCO TEORICO

Dado que este trabajo se centrará en textos debemos basarnos en una norma que nos permita gestionar la seguridad de la información, esta norma es la ISO/IEC 27001:2013.

Esta norma puede ser implementada en cualquier empresa tanto privadas, grandes, pequeñas y proporciona una metodología de cómo realizar una gestión de la seguridad de la información en una empresa.

Pero porque llevar la aplicabilidad de la norma ISO/IEC 27001:2013 a la mitigación del problema de nuestra la empresa TRANSFORMADORES CDM LTDA? pues bien esta norma es catalogada como la principal norma para la seguridad de la información. Así que no es necesario nombrar otros modelos como el COBIT 4.5 ya que leyendo la 27001 nos damos cuenta que cumple con nuestra expectativas, pero a continuación daremos un vistazo de las que posiblemente cumplen con ciertas ayudas para la realización de la aplicación SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) en esta empresa

ISO/IEC 27001:2013.

ISO/IEC 27001:2013 tiene como prioridad proteger

a) La confidencialidad de la información
b) La integridad de la información
c) La Disponibilidad de la información

ISO/IEC 27001 se divide en 11 secciones las cuales se describen a continuación:

Sección 0 – Introducción – explica el objetivo de ISO/IEC 27001:2013 y su compatibilidad con otras normas de gestión.

Sección 1 – ***Alcance*** – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – ***Referencias normativas*** – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – ***Términos y definiciones*** – de nuevo, hace referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI).

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – ***Planificación*** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – ***Apoyo*** – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Otras normas relacionadas con seguridad de la información:

ISO/IEC 27002 proporciona directrices para la implementación de los controles indicados en ISO/IEC 27001:2013. ISO/IEC 27001:2013 especifica 114 controles que pueden ser utilizados para disminuir los riesgos de seguridad, y la norma ISO 27002 puede ser bastante útil ya que proporciona más información sobre cómo implementar esos controles. A la ISO 27002 anteriormente se la conocía como ISO/IEC 17799 y surgió de la norma británica BS 7799-1.
ISO/IEC 27004 proporciona directrices para la medición de la seguridad de la información; se acopla bien con ISO/IEC 27001:2013 ya que explica cómo determinar si el SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) ha alcanzado los objetivos.

ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de información. Es un muy buen complemento para ISO/IEC 27001:2013 ya que brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, probablemente la etapa más difícil de la implementación. ISO 27005 ha surgido de la norma británica BS 7799-3.

ISO 22301 define los requerimientos para los sistemas de gestión de continuidad del negocio, se adapta muy bien con ISO/IEC 27001:2013 porque el punto A.17 de esta última requiere la implementación de la continuidad del negocio aunque no proporciona demasiada información.

2.5 MARCO LEGAL

LEY 527 DE 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan disposiciones.

LEY ESTATUTARIA 1266 DEL 31 DE DICIEMBRE DE 2008. Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la seguridad de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

LEY 1273 DEL 5 DE ENERO DE 2009. Delitos informáticos 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.

LEY 1341 DEL 30 DE JULIO DE 2009. Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones como la importancia de la seguridad.

3 DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Teniendo en cuenta que es necesaria una investigación que describa de modo sistemático las características de un área de interés, donde se recojan datos sobre la base de una hipótesis, se exponga la información y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento; se realizara una investigación de tipo descriptiva para el desarrollo del proceso.

3.2 TECNICAS DE RECOLECCION DE LA INFORMACION

3.2.1 Fuentes primarias

Técnicas de recolección de información:

- Observación
- Entrevistas
- Revisión documental
- Encuestas
- Listas de chequeo

3.3 POBLACION

Para el desarrollo de esta investigación se tomara como población de estudio la totalidad de funcionarios del área Contable de Transformadores CDM, compuesta de la siguiente manera:

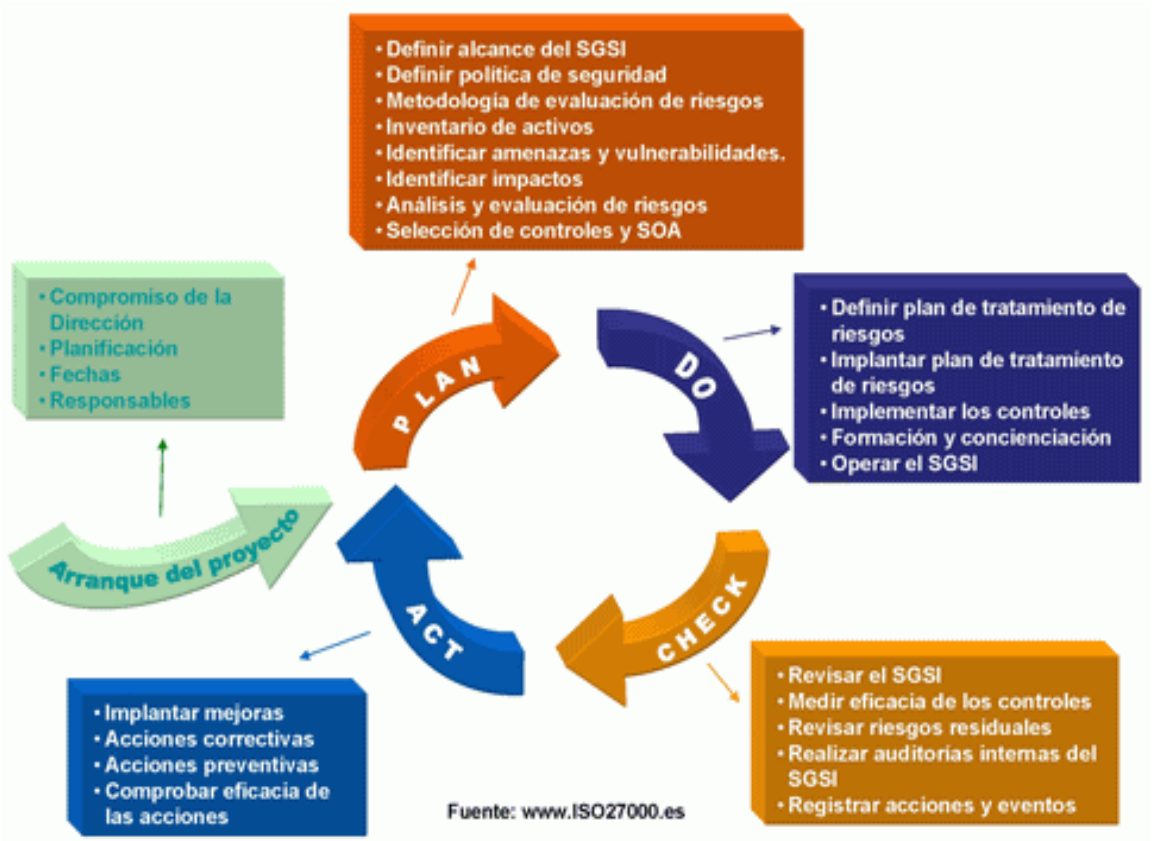
-Contadora
-Auxiliar Contable 1
-Auxiliar Contable 2
-Encargada de Compras
-Encargada de Facturación.

4. RESULTADOS

4.1 DIAGNÓSTICO DE LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE CONTABILIDAD DE LA EMPRESA DE TRANSFORMADOR CDM, BASADO EN LA NORMA ISO/IEC 27001:2013

Según la norma ISO/IEC 27001:2013, las etapas para el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información están dadas por el ciclo PHVA: Planear, Hacer, Verificar y Actuar.

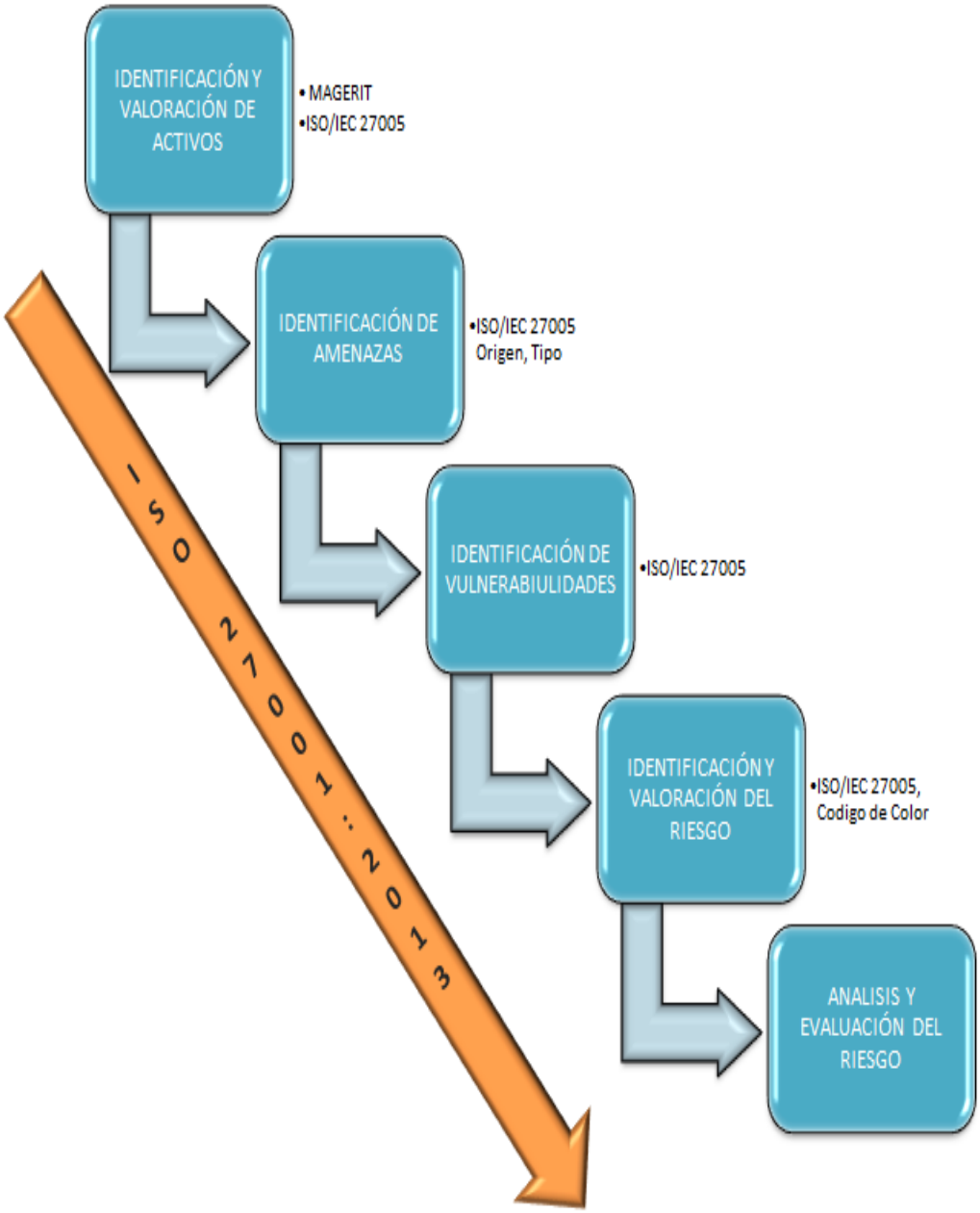
Imagen 1. Ciclo PHVA



Fuente. ISO/IEC 27001:2013

Teniendo en cuenta que el proyecto de investigación está limitado al área de contabilidad de la empresa TRANSFORMADORES CDM, se plantea una fase inicial que abarca la Planeación del Sistema de Gestión de Seguridad de la Información, con las siguientes fases:

Imagen 2. Metodología de Desarrollo del Proyecto



Fuente. ISO/IEC 27001:2013

4.1.1 Identificación de la organización.[9]

Imagen 3. Logo de la Empresa TRANSFORMADORES CDM

TRANSFORMADORES CDM es una empresa colombiana dedicada a la fabricación, reparación, reconstrucción y mantenimiento de transformadores de distribución y media potencia.

A través de su experiencia de más de 20 años, ha logrado posicionarse en el mercado como una de las mejores empresas a nivel nacional que dedica su mayor atención a la reparación de transformadores de distribución y media potencia.

Cuenta con personal e instalaciones altamente calificadas, que le permiten ofrecer un producto y servicio de excelente calidad. Por el cumplimiento de sus compromisos y amplia experiencia, En octubre 21 de 1999 certifico el sistema de aseguramiento de la calidad por primera vez de conformidad con la norma ISO 9002, por parte de BUREAU VERITAS QUALITY INTERNATIONAL.

En diciembre de 2002 se renueva la certificación del sistema de gestión de calidad de conformidad con la norma ISO-9001 versión 2000 por parte del ICONTEC, con alcance para: producción, reconstrucción, reparación y venta de transformadores de distribución monofásicos y trifásicos. Producción y venta de soldadores por arco eléctrico y ensamble de medidores electrónicos.

En octubre del 2005 TRANSFORMADORES CDM LTDA se inscribe por primera vez al Registro de Evaluación de programas de Salud Ocupacional y Medio Ambiente para Contratistas, con el fin de lograr en conjunto con las empresas operadoras del sector el desarrollo armónico de la Seguridad, la Salud Ocupacional y la protección Ambiental.

En Marzo del 2009 se obtiene la certificación del Sistema de Gestión de Calidad bajo el modelo de la norma ISO-9001 versión 2008 y en febrero del 2010 se logra obtener la certificación en Sistema Integrado de Gestión (SIG) en cumplimiento de los requisitos de las normas ISO-9001:2008; sistema de gestión de Calidad, ISO-14001:2004; Sistema de Gestión Ambiental y OHSAS 18001:2007; Sistema de Gestión en Seguridad y Salud

[9] TRANSFORMADORES CDM. Quienes somos. [en línea]. Actualizado en el 2016. [Citado en Octubre 10 de 2015]. Disponible en Internet en: (http://www.transformadorescdm.com/quienes-somos.html)

Ocupacional, con el ICONTEC. Definiendo el siguiente alcance: Fabricación, reparación, reconstrucción, mantenimiento y comercialización de transformadores; fabricación y comercialización de equipos de soldadura por arco eléctrico; ensamble y comercialización de medidores de energía.

En el área administrativa y contable manejan el software contable VISUAL TNS, con este sistema de información manejan las compras, facturación, contabilidad, tesorería, inventarios y nómina.

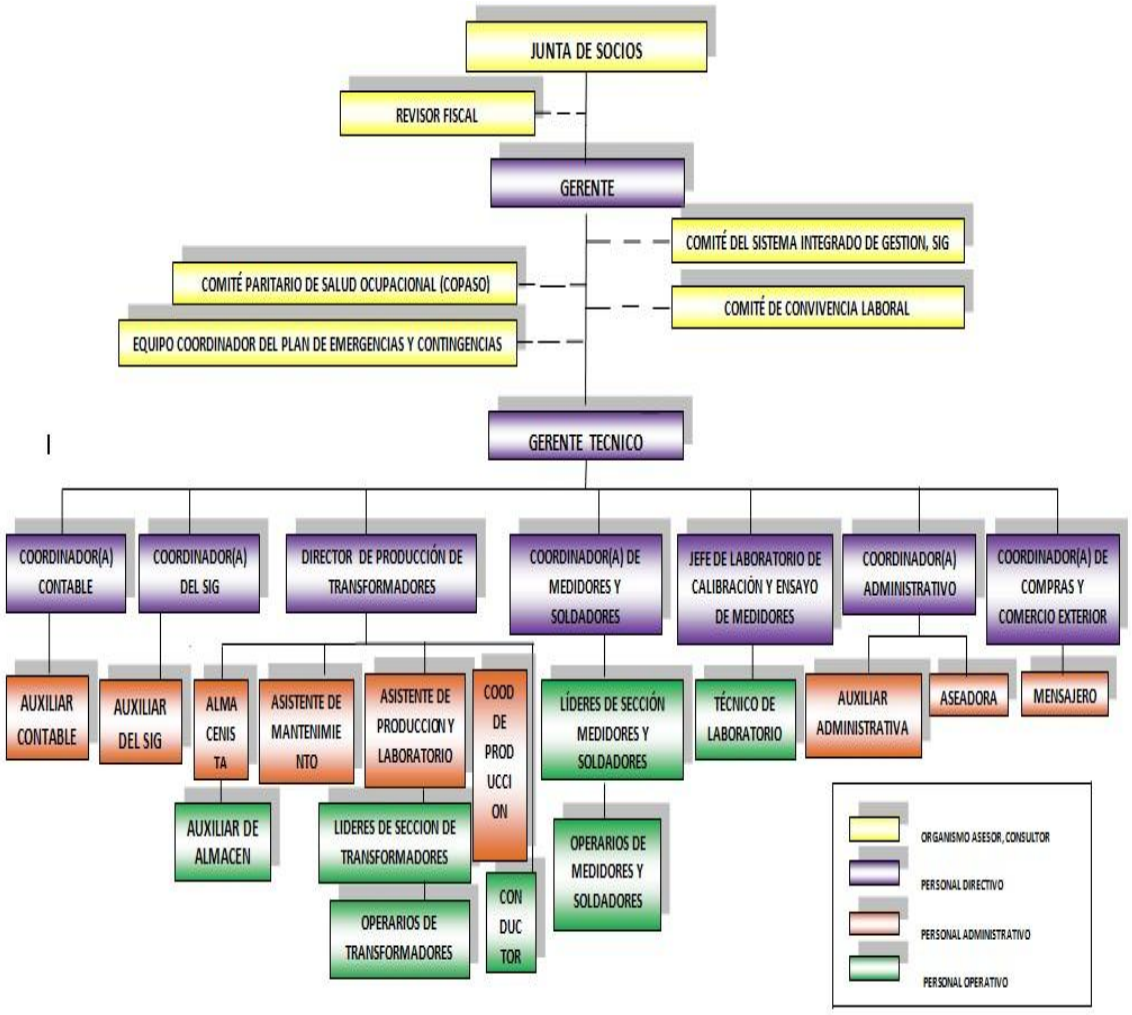
Sus áreas tecnológicas no cumplen los requisitos para la certificación en el manejo de la información por lo tanto estos estudios servirán para pasar una propuesta en la implementación de buenas prácticas en la información.

4.1.2 Misión. Somos una empresa dedicada a la fabricación, reparación, reconstrucción, mantenimiento y comercialización de transformadores; fabricación y comercialización de equipos de soldadura; ensamble y comercialización de medidores de energía. Contamos con un personal calificado y comprometido con la protección de la integridad física de nuestros trabajadores y visitantes, la conservación del medio ambiente y la satisfacción de nuestros clientes y demás partes interesadas, permitiéndonos ser una de las empresas líderes en el sector eléctrico, generadora de progreso y desarrollo para la economía de nuestro país.

4.1.3 Visión. En el 2019 consolidarnos en la fabricación de transformadores, mantenernos posicionados a nivel nacional e iniciar la participación en el mercado internacional en las líneas de transformadores, medidores y soldadores, generando recursos que nos permitan mejorar y mantener programas de gestión eficaces, cumpliendo nuestros compromisos con la calidad del producto y servicio, la prevención de lesiones y enfermedades de carácter laboral y la prevención de la contaminación, logrando que nuestro SIG sea coherente con los principios y lineamientos de nuestros clientes.

4.1.4 Estructura Orgánica. La estructura Orgánica de Transformadores CDM se encuentra dada de la siguiente manera:

Imagen 4. Estructura Orgánica TRANSFORMADORES CDM



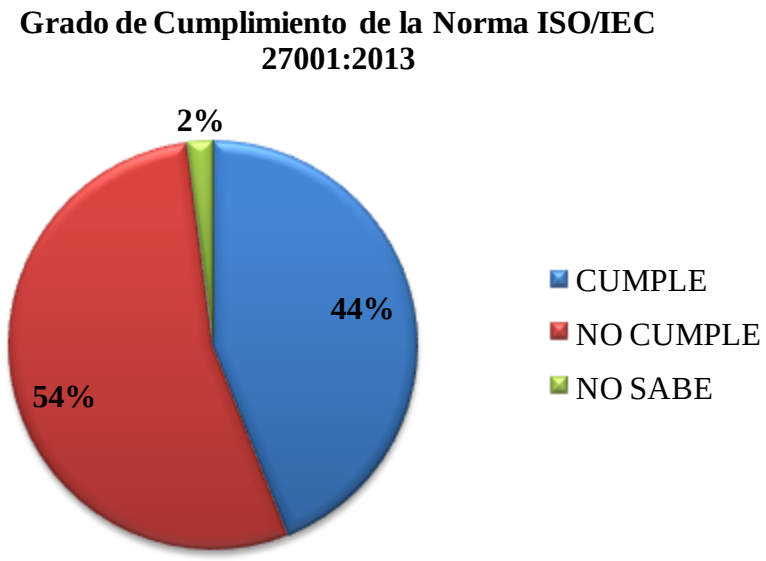
Fuente. TRANSFORMADORES CDM.

4.1.5 Análisis e interpretación de la información. Con el fin de determinar el estado actual de la seguridad de la información de TRANSFORMADORES CDM se realizaron visitas a la empresa donde se aplicaron los instrumentos de recolección de la información previamente seleccionados, tomando como base la matriz de cumplimiento, además de entrevista directa con el jefe de área y encuesta al personal del área. *Ver Anexo A, B, y C*

Luego de aplicar los instrumentos de recolección de la información seleccionados para determinar el estado de la seguridad de la información y el grado de cumplimiento de la Norma ISO/IEC 27001:2013, se obtuvieron las siguientes evidencias representadas de manera gráfica.

Frente a las entrevistas realizadas al personal de la unidad de Contabilidad de la Empresa CDM se evidencia:

Grafica 1. Grado de cumplimiento de la Norma ISO/IEC 27001:2013



Fuente. Autores del proyecto.

El grado de cumplimiento de la Norma ISO/IEC 27001 de 44% frente a la evaluación de cada uno de los controles definidos en la norma, con tan solo 44 controles que muestran cumplimiento parcial y 2 controles que muestran un cumplimiento satisfactorio representado un alto nivel de riesgo para la empresa.

Analizando el nivel de cumplimiento de la norma (44%) se evidencia que un 29% de los controles que no se cumplen al interior del área corresponden a aquellos encaminados a la seguridad física de la información, frente a un 12% de controles incumplidos con respecto a la seguridad lógica de la información; por tal motivo se decide encaminar el análisis de riesgo posterior a estas áreas de mayor incumplimiento.

4.2 PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE CONTABILIDAD EN LA EMPRESA TRANSFORMADORES CDM.

4.2.1 Análisis de riesgos.

Identificación y Valoración de Activos. Para cumplir con los objetivos del de la unidad contable de TRANSFORMADORES CDM, la empresa cuenta con 3 computadores y un servidor (no dedicado), los cuales se encuentran conectados por una red de comunicaciones LAN; con el fin de diagnosticar el estado de la seguridad de la información del área contable de TRANSFORMADORES CDM se realizó la correspondiente identificación y valoración de activos, como se muestra a continuación:

Tabla 1. Identificación y Valoración de Activos.

ESCALA DE VALORACIÓN	VALOR	DESCRIPCIÓN
MB: Muy Bajo	1	Irrelevante para el desarrollo de las actividades de la Empresa
B: Bajo	2	Importancia menor para el desarrollo de las actividades de la Empresa
M: Medio	3	Importante para el desarrollo de las actividades de la Empresa
A: Alto	4	Altanamente importante para el desarrollo de las actividades de la Empresa
MA: Muy Alto	5	De vital importancia para el desarrollo de actividades de la Empresa

Fuente. Norma ISO/IEC 27005

Con el fin de analizar los riesgos a los que se encuentra expuesta el área contable de Transformadores CDM, se partió de identificar los elementos relevantes que para el caso dado se conocen como Activos de Información, de igual manera se valoró la relevancia de cada uno de ellos dentro de la organización, tomando como base la escala de valoración que muestra la tabla para los objetivos de seguridad Disponibilidad, Integridad y Confidencialidad para finalmente obtener una valoración total para cada uno de los activos identificados:

Tabla 2. Descripción de Activos de Información

ACTIVO	DESCRIPCIÒN	FUNCIONES
SERVIDOR	Intel Atom D510 a 1.6 GHz, 250 GB HDD, Intel ® GMA 4500M , “GB DDR3 Memory, 802.11b/g/n, 14.0” 16:9 HD LCD	Almacenamiento y Distribución de información mediante peticiones cliente servidor
AUXILIAR 1	Intel Atom D510 a 1.6 GHz, 250 GB HDD, Intel ® GMA 4500M , “GB DDR3 Memory, 802.11b/g/n, 14.0” 16:9 HD LCD	Registro de Transacciones
AUXILIAR 2	Intel Atom D510 a 1.6 GHz, 250 GB HDD, Intel ® GMA 4500M , “GB DDR3 Memory, 802.11b/g/n, 14.0” 16:9 HD LCD	Registro de Transacciones
FACTURACIÒN	Intel Atom D510 a 1.6 GHz, 250 GB HDD, Intel ® GMA 4500M , “GB DDR3 Memory, 802.11b/g/n, 14.0” 16:9 HD	Registro de Transacciones Correspondientes a Facturación

	LCD	
GESTION DE TRANSACCIONES	N/A	Gestión de Ingresos Gestión de Egresos Gestión de notas contables

Fuente. Autores del proyecto

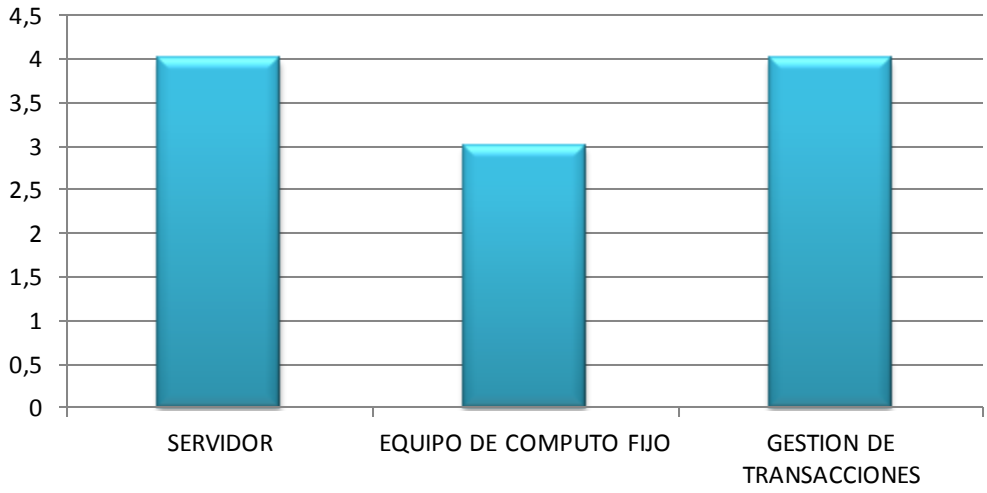
Tabla 3. Valoración de cada uno de los Activos dentro de la Organización.

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS			
			Valoración Cuantitativa			Valoración Total
Activo	**Tipo**	**Responsable / dueño**	**Disponibilidad**	**Integridad**	**Confidenciabilidad**	
SERVIDOR	Equipos de Procesamiento de Datos	JEFE CONTABLE	3	4	4	4
AUXILIAR 1	Equipos de Procesamiento de Datos	AUX DE CONTABILIDAD	2	3	3	3
AUXILIAR 2	Equipos de Procesamiento de Datos	AUX DE CONTABILIDAD	2	3	3	3
FACTURACION	Equipos de Procesamiento de Datos	JEFE FACTURACION	2	4	4	3
GESTION DE TRANSACCIONES	Procesos y Actividades del Negocio	JEFE CONTABLE	3	4	4	4

Fuente. Autores del Proyecto

Teniendo en cuenta la similitud de la configuración, funciones y procesos que se llevan a cabo con los equipos auxiliar 1, auxiliar 2 y facturación fueron agrupados en el activo "EQUIPO DE CÓMPUTO FIJO", con el fin de reducir la redundancia en la investigación.
La valoración de activos permite ratificar la importancia de vigilar la seguridad de la información al interior la unidad contable de TRANSFORMADORES CDM, teniendo en cuenta que la cualificación de cada uno de ellos se encuentra por encima de la media definida:

Grafica 2. Valoración de los Activos.



Fuente. Autores del Proyecto

Se observa que los activos con mayor valoración son equipo que funciona como "Servidor" a pesar de que en este se desarrollan tareas distintas a las funciones como servidor, y que su uso no se encuentra limitado al responsable del equipo, además del activo definido como "Gestión de Transacciones", el cual corresponde al registro de ingresos, egresos y notas contables .

4.2.2 Identificación de Amenazas. Tomando como referencia la Norma ISO/IEC 27005, se realiza la identificación de las amenazas que reposan sobre cada uno de los activos de información anteriormente identificados para así continuar con el proceso de gestión del riesgo. De acuerdo a la Norma, las amenazas pueden ser deliberadas (D), Accidentales (A) o Ambientales (E); la letra D se utiliza para todas las acciones deliberadas que tienen como objetivo los activos de la información, A se utiliza para las acciones humanas que pueden dañar accidentalmente los activos de la información y E se utiliza para todos los incidentes que no se basa en las acciones humanas. (ISO/IEC, 2009)

Tabla 4. Relación Origen- Sigla Amenazas

ORIGEN	SIGLA
Amenazas por Acción Deliberada	D
Amenazas por Acciones Accidentales	A
Amenazas por Acciones Ambientales	E

Fuente. Norma ISO/IEC 27005

Tabla 5. Amenazas para el activo: Servidor

ACTIVO	AMENAZA	ORIGEN	TIPO
SERVIDOR	Fuego	A,D,E	Daño Físico
	Contaminación	A,D,E	
	Polvo, corrosión	A,D,E	
	Fenómenos sísmicos	E	Eventos Naturales
	Fenómenos Climáticos	E	
	Falla en el sistema de suministro de agua o de aire acondicionado	A,D	Pérdida de los Servicios Esenciales
	Perdida del Suministro de Energía	A,D,E	
	Falla en el Equipo de Telecomunicaciones		
	Interceptación de Señales de Interferencia Comprometedoras	D	Compromiso de la Información
	Espionaje Remoto	D	
	Escucha Encubierta	D	
	Hurto de Medios o Documentos	D	
	Hurto de Equipo	D	
	Recuperación de Medios Reciclados o Desechados	D	
	Divulgación	A,D	
	Manipulación con Hardware	D	
	Manipulación con Software	A,D	
	Falla en el Equipo	A	Fallas Técnicas
	Mal Funcionamiento de Equipo	A	
	Mal funcionamiento del Software	A	
	Incumplimiento del Mantenimiento del Sistema de Información	A,D	
	Uso no Autorizado del Equipo	D	Acciones no Autorizadas

	Copia Fraudulenta del Software	D	
	Uso de Software Falso o Copiado	A,D	
	Corrupción de Datos	D	
	Error en Uso	A	Compromiso de las Funciones
	Abuso de Derechos	A,D	
	Falsificación de Derechos	D	
	Negación de Acciones	D	

Fuente. Norma ISO/IEC 27005

Tabla 6. Amenazas para los activos: Equipo de Computo Fijo

ACTIVO	AMENAZA	ORIGEN	TIPO
EQUIPO DE COMPUTO FIJO	Fuego	A,D,E	Daño Físico
	Contaminación	A,D,E	
	Polvo, corrosión	A,D,E	
	Fenómenos sísmicos	E	Eventos Naturales
	Fenómenos Climáticos	E	
	Falla en el sistema de suministro de agua o de aire acondicionado	A,D	Pérdida de los Servicios Esenciales
	Perdida del Suministro de Energía	A,D,E	
	Falla en el Equipo de Telecomunicaciones		
	Interceptación de Señales de Interferencia Comprometedoras	D	Compromiso de la Información
	Espionaje Remoto	D	
	Escucha Encubierta	D	
	Hurto de Medios o Documentos	D	
	Hurto de Equipo	D	
	Recuperación de Medios Reciclados o Desechados	D	

	Divulgación	A,D	
	Manipulación con Hardware	D	
	Manipulación con Software	A,D	
	Falla en el Equipo	A	Fallas Técnicas
	Mal Funcionamiento de Equipo	A	
	Mal funcionamiento del Software	A	
	Incumplimiento del Mantenimiento del Sistema de Información	A,D	
	Uso no Autorizado del Equipo	D	Acciones no Autorizadas
	Copia Fraudulenta del Software	D	
	Uso de Software Falso o Copiado	A,D	
	Corrupción de Datos	D	
	Error en Uso	A	Compromiso de las Funciones
	Abuso de Derechos	A,D	
	Falsificación de Derechos	D	
	Negación de Acciones	D	

Fuente. Norma ISO/IEC 27005

Tabla 7. Amenaza para el activo: Gestión de Transacciones

ACTIVO	AMENAZA	ORIGEN	TIPO
GESTION DE TRANSACCIONES	Hurto de Medios o Documentos	D	Compromiso de la Información
	Hurto de Equipo	D	
	Recuperación de Medios Reciclados o Desechados	D	
	Procesamiento Ilegal de los Datos	D	

Fuente. Norma ISO/IEC 27005

4.2.3 Identificación de Vulnerabilidades. Entendiendo Vulnerabilidad como la debilidad de un activo que puede ser explotada por una o más amenazas, se identifican las vulnerabilidades que afectan a cada uno de los activos de información tomando como base la Norma ISO/IEC 27005:

Tabla 8. Vulnerabilidades para el activo: Servidor

ACTIVO	AMENAZA	VULNERABILIDAES
SERVIDOR	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad
	Fenómenos sísmicos	Ubicación en un Área Susceptible
	Falla en el sistema de suministro de agua o de aire acondicionado	Calentamiento de Equipos Informáticos
	Perdida del Suministro de Energía	Susceptibilidad de Variaciones de Voltaje
		Red Enérgica Inestable
	Falla en el Equipo de Telecomunicaciones	Gestión Inadecuada de la Red
		Conexión deficiente de Cables
		Punto Único de Falla
		Ausencia de Planes de Continuidad
	Espionaje Remoto	Arquitectura Insegura de la Red
		Transferencias de Contraseñas en Claro
	Escucha Encubierta	Líneas de Comunicación sin Protección
		Trafico Sensible sin Protección
	Hurto de Medios o Documentos	Almacenamiento sin Protección
		Falta de Cuidado en la Disposición Final
		Ausencia de protección Física de la Edificación, puertas y Ventanas
		Trabajo no Supervisado del Personal Externo o de Limpieza
		Ausencia o

		Insuficiencia de Política Sobre Limpieza de Escritorio y Pantalla
		Ausencia de Autorización de los Recursos de Procesamiento de la Información
		Ausencia de Mecanismos de Monitoreo Establecidos para las Brechas en la Seguridad
	Hurto de Equipo	Ausencia de Protección Física del edificio
		Ausencia de Procesos Disciplinarios definidos en el Caso de Incidentes de Seguridad de la Información
	Divulgación	Falta de conciencia acerca de la seguridad
		Ausencia de Mecanismos de Monitoreo
	Manipulación con Software	Descarga y Uso no Controlado del Software
		Ausencia de Copias de Respaldo
	Falla en el Equipo	Ausencia de Planes de Continuidad
	Mal Funcionamiento de Equipo	Ausencia de Planes de Continuidad
	Mal funcionamiento del Software	Software Nuevo o Inmaduro
		Especificaciones Incompletas o no Claras para los Desarrolladores
	Incumplimiento del Mantenimiento del Sistema de Información	Mantenimiento Insuficiente/instalación fallida de medios de almacenamiento
		Respuesta Inadecuada de Mantenimiento del Servicio
	Uso no Autorizado del	Ausencia de Políticas

	Equipo	para el Uso Correcto de los Medios de Telecomunicaciones y Mensajería
	Uso de Software Falso o Copiado	Descarga y Uso no Controlado de Software
	Error en el Uso	Ausencia de Políticas Sobre el Uso de Correo Electrónico
		Ausencia de Registros en las Bitácoras (logs) de administrador y Operario
		Ausencia de Procedimientos para el Manejo de Información Clasificada
		Ausencia de Responsabilidades en la Seguridad de la Información en la Descripción de Cargos
	Abuso de Derechos	Ausencia de procedimiento Formal para el Registro y Retiro de Usuarios Ausencia de Proceso Formal para la Revisión (supervisión de los derechos de acceso) Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos Ausencia del Procedimiento del Monitoreo de los recursos de procesamiento de la información Ausencia de Auditorias

		(supervisiones) regulares
	Falsificación de Derechos	Gestión Deficiente de las Contraseñas

Fuente. Norma ISO/IEC 27005

Tabla 9. Vulnerabilidades para los activos: Equipo de Computo Fijo

ACTIVO	AMENAZA	VULNERABILIDAES
EQUIPO DE COMPUTO FIJO	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad
	Fenómenos sísmicos	Ubicación en un Área Susceptible
	Falla en el sistema de suministro de agua o de aire acondicionado	Calentamiento de Equipos Informáticos
	Perdida del Suministro de Energía	Susceptibilidad de Variaciones de Voltaje
		Red Enérgica Inestable
	Falla en el Equipo de Telecomunicaciones	Gestión Inadecuada de la Red
		Conexión deficiente de Cables
		Punto Único de Falla
		Ausencia de Planes de Continuidad
	Espionaje Remoto	Arquitectura Insegura de la Red
		Transferencias de Contraseñas en Claro
	Escucha Encubierta	Líneas de Comunicación sin Protección
		Trafico Sensible sin Protección
	Hurto de Medios o Documentos	Almacenamiento sin Protección
		Falta de Cuidado en la Disposición Final
		Ausencia de protección Física de la Edificación,

		puertas y Ventanas
		Trabajo no Supervisado del Personal Externo o de Limpieza
		Ausencia o Insuficiencia de Política Sobre Limpieza de Escritorio y Pantalla
		Ausencia de Autorización de los Recursos de Procesamiento de la Información
		Ausencia de Mecanismos de Monitoreo Establecidos para las Brechas en la Seguridad
	Hurto de Equipo	Ausencia de Protección Física del edificio
		Ausencia de Procesos Disciplinarios definidos en el Caso de Incidentes de Seguridad de la Información
	Divulgación	Falta de conciencia acerca de la seguridad
		Ausencia de Mecanismos de Monitoreo
	Manipulación con Software	Descarga y Uso no Controlado del Software
		Ausencia de Copias de Respaldo
	Falla en el Equipo	Ausencia de Planes de Continuidad
	Mal Funcionamiento de Equipo	Ausencia de Planes de Continuidad
	Mal funcionamiento del Software	Software Nuevo o Inmaduro
		Especificaciones Incompletas o no Claras para los Desarrolladores
	Incumplimiento del Mantenimiento del Sistema de	Mantenimiento Insuficiente/instalación fallida de medios de

	Información	almacenamiento
		Respuesta Inadecuada de Mantenimiento del Servicio
	Uso no Autorizado del Equipo	Ausencia de Políticas para el Uso Correcto de los Medios de Telecomunicaciones y Mensajería
	Uso de Software Falso o Copiado	Descarga y Uso no Controlado de Software
	Error en el Uso	Ausencia de Políticas Sobre el Uso de Correo Electrónico
		Ausencia de Registros en las Bitácoras (logs) de administrador y Operario
		Ausencia de Procedimientos para el Manejo de Información Clasificada
		Ausencia de Responsabilidades en la Seguridad de la Información en la Descripción de Cargos
	Abuso de Derechos	Ausencia de procedimiento Formal para el Registro y Retiro de Usuarios Ausencia de Proceso Formal para la Revisión (supervisión de los derechos de acceso) Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos Ausencia del Procedimiento del

		Monitoreo de los recursos de procesamiento de la información Ausencia de Auditorias (supervisiones) regulares
	Falsificación de Derechos	Gestión Deficiente de las Contraseñas

Fuente. Norma ISO/IEC 27005

Tabla 10. Vulnerabilidades para el Activo: Gestión de Transacciones

ACTIVO	AMENAZA	VULNERABILIDAD
GESTION DE TRANSACCIONES	Hurto de Medios o Documentos	Almacenamiento sin Protección
		Falta de Cuidado en la Disposición Final
		Copia No Controlada Ausencia de
		Protección Física de la Edificación
		Trabajo No Supervisado del Personal Externo o de Limpieza
		Ausencia o insuficiencia de Políticas Sobre Limpieza de Escritorio y pantalla
		Ausencia de Autorización de los Recursos de Procesamiento de la Información

	Hurto de Equipo	Protección Física de la Edificación
		Ausencia de Procesos Disciplinarios Definidos en el Caso de Incidentes de Seguridad de la Información
	Procesamiento Ilegal de los Datos	Ausencia de Mecanismos de Monitoreo
		Ausencia o Insuficiencia en las Disposiciones (con respecto a la seguridad de la Información) en los Contratos con los Empleados

Fuente. Norma ISO/IEC 27005

4.2.4 Identificación y Valoración del Riesgo. Con el fin de identificar la medida del riesgo que afecta a cada uno de los activos previamente definidos se toma como apoyo la siguiente matriz propuesta por la norma ISO/IEC 27005, donde se emplea la valoración de cada uno de los activos identificados frente a la probabilidad de ocurrencia de la amenaza y su respectiva facilidad de Explotación:

Tabla 11. Identificación y Valoración del Riesgo.

	PROBABILIDAD DE OCURRENCIA – AMENAZA	**BAJA**			**MEDIA**			**ALTA**		
	FACILIDAD DE EXPLOTACIÓN	**B**	**M**	**A**	**B**	**M**	**A**	**B**	**M**	**A**
VALORACION DEL ACTIVO	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Fuente. Norma ISO/IEC 27005

Teniendo en cuenta los valores proporcionados por la anterior matriz, se definen tres niveles para la medida del riesgo, los cuales se verán representados con un color significativo para el proceso de valoración del riesgo, así:

BAJO (0-2)	
MEDIO(3-5)	
ALTO(6-8)	

Tabla 12. Identificación y Valoración del Riesgo para el activo: Servidor

ACTIVO	AMENAZA	VULNERABILIDAES	IDENTIFICACION Y VALORACION DEL RIESGO
SERVIDOR	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad	Daño de equipo
	Fenómenos sísmicos	Ubicación en un Área Susceptible	Daño de equipo
	Falla en el sistema de suministro de agua o de aire acondicionado	Calentamiento de Equipos Informáticos	Daño de equipo
	Perdida del Suministro de Energía	Susceptibilidad de Variaciones de Voltaje	Daño de equipo
		Red Enérgica Inestable	
	Falla en el Equipo de Telecomunicaciones	Gestión Inadecuada de la Red	Daño de equipo
		Conexión deficiente de Cables	
		Punto Único de Falla	
		Ausencia de Planes de Continuidad	
	Espionaje Remoto	Arquitectura Insegura de la Red	Filtrado de información
		Transferencias de Contraseñas en Claro	
	Escucha Encubierta	Líneas de Comunicación sin Protección	Filtrado de información
		Trafico Sensible sin Protección	
	Hurto de Medios o Documentos	Almacenamiento sin Protección	Filtrado de información
		Falta de Cuidado en la	

		Disposición Final	
		Ausencia de protección Física de la Edificación, puertas y Ventanas	
		Trabajo no Supervisado del Personal Externo o de Limpieza	
		Ausencia o Insuficiencia de Política Sobre Limpieza de Escritorio y Pantalla	
		Ausencia de Autorización de los Recursos de Procesamiento de la Información	
		Ausencia de Mecanismos de Monitoreo Establecidos para las Brechas en la Seguridad	
	Hurto de Equipo	Ausencia de Protección Física del edificio	Filtrado de información
		Ausencia de Procesos Disciplinarios definidos en el Caso de Incidentes de Seguridad de la Información	
	Divulgación	Falta de conciencia acerca de la seguridad	Filtrado de información
		Ausencia de Mecanismos de Monitoreo	
	Manipulación con Software	Descarga y Uso no Controlado del Software	Daño de sistema Filtrado de información
		Ausencia de Copias de Respaldo	
	Falla en el Equipo	Ausencia de Planes de Continuidad	Detención de procesos
	Mal Funcionamiento de Equipo	Ausencia de Planes de Continuidad	Detención de procesos
	Mal funcionamiento del Software	Software Nuevo o Inmaduro	Detención de procesos
		Especificaciones Incompletas o no Claras para los Desarrolladores	

	Incumplimiento del Mantenimiento del Sistema de Información	Mantenimiento Insuficiente/instalación fallida de medios de almacenamiento	Detención de procesos
		Respuesta Inadecuada de Mantenimiento del Servicio	
	Uso no Autorizado del Equipo	Ausencia de Políticas para el Uso Correcto de los Medios de Telecomunicaciones y Mensajería	Filtrado de información
	Uso de Software Falso o Copiado	Descarga y Uso no Controlado de Software	Detención de procesos
	Error en el Uso	Ausencia de Políticas Sobre el Uso de Correo Electrónico	Detención de procesos
		Ausencia de Registros en las Bitácoras (logs) de administrador y Operario	
		Ausencia de Procedimientos para el Manejo de Información Clasificada	
		Ausencia de Responsabilidades en la Seguridad de la Información en la Descripción de Cargos	
	Abuso de Derechos	Ausencia de procedimiento Formal para el Registro y Retiro de Usuarios Ausencia de Proceso Formal para la Revisión (supervisión de los derechos de acceso) Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos	Filtrado de información

		Ausencia del Procedimiento del Monitoreo de los recursos de procesamiento de la información Ausencia de Auditorias (supervisiones) regulares	
	Falsificación de Derechos	Gestión Deficiente de las Contraseñas	Filtrado de información

Fuente. Autores del proyecto

Tabla 13. Identificación y valoración del riesgo para los activos: Equipo de Computo Fijo

ACTIVO	AMENAZA	VULNERABILIDAES	IDENTIFICACION Y VALORACION DEL RIESGO
EQUIPO DE COMPUTO FIJO	Polvo, corrosión	Susceptibilidad a la humedad, el polvo y la suciedad	Daño de equipo
	Fenómenos sísmicos	Ubicación en un Área Susceptible	Daño de equipo
	Falla en el sistema de suministro de agua o de aire acondicionado	Calentamiento de Equipos Informáticos	Daño de equipo
	Perdida del Suministro de Energía	Susceptibilidad de Variaciones de Voltaje	Daño de equipo
		Red Enérgica Inestable	
	Falla en el Equipo de Telecomunicaciones	Gestión Inadecuada de la Red	Daño de equipo
		Conexión deficiente de Cables	
		Punto Único de Falla	
		Ausencia de Planes de Continuidad	
	Espionaje Remoto	Arquitectura Insegura de la Red	Filtrado de información
		Transferencias de Contraseñas en Claro	
	Escucha Encubierta	Líneas de Comunicación sin Protección	Filtrado de información

		Trafico Sensible sin Protección	
	Hurto de Medios o Documentos	Almacenamiento sin Protección	Filtrado de información
		Falta de Cuidado en la Disposición Final	
		Ausencia de protección Física de la Edificación, puertas y Ventanas	
		Trabajo no Supervisado del Personal Externo o de Limpieza	
		Ausencia o Insuficiencia de Política Sobre Limpieza de Escritorio y Pantalla	
		Ausencia de Autorización de los Recursos de Procesamiento de la Información	
		Ausencia de Mecanismos de Monitoreo Establecidos para las Brechas en la Seguridad	
	Hurto de Equipo	Ausencia de Protección Física del edificio	Filtrado de información
		Ausencia de Procesos Disciplinarios definidos en el Caso de Incidentes de Seguridad de la Información	
	Divulgación	Falta de conciencia acerca de la seguridad	Filtrado de información
		Ausencia de Mecanismos de Monitoreo	
	Manipulación con Software	Descarga y Uso no Controlado del Software	Daño de sistema Filtrado de información
		Ausencia de Copias de Respaldo	
	Falla en el Equipo	Ausencia de Planes de Continuidad	Detención de procesos
	Mal Funcionamiento	Ausencia de Planes de	Detención de procesos

	de Equipo	Continuidad	
	Mal funcionamiento del Software	Software Nuevo o Inmaduro	Detención de procesos
		Especificaciones Incompletas o no Claras para los Desarrolladores	
	Incumplimiento del Mantenimiento del Sistema de Información	Mantenimiento Insuficiente/instalación fallida de medios de almacenamiento	Detención de procesos
		Respuesta Inadecuada de Mantenimiento del Servicio	
	Uso no Autorizado del Equipo	Ausencia de Políticas para el Uso Correcto de los Medios de Telecomunicaciones y Mensajería	Filtrado de información
	Uso de Software Falso o Copiado	Descarga y Uso no Controlado de Software	Detención de procesos
	Error en el Uso	Ausencia de Políticas Sobre el Uso de Correo Electrónico	Detención de procesos
		Ausencia de Registros en las Bitácoras (logs) de administrador y Operario	
		Ausencia de Procedimientos para el Manejo de Información Clasificada	
		Ausencia de Responsabilidades en la Seguridad de la Información en la Descripción de Cargos	
	Abuso de Derechos	Ausencia de procedimiento Formal para el Registro y Retiro de Usuarios Ausencia de Proceso Formal para la Revisión (supervisión de los	Filtrado de información

		derechos de acceso) Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos Ausencia del Procedimiento del Monitoreo de los recursos de procesamiento de la información Ausencia de Auditorias (supervisiones) regulares	
	Falsificación de Derechos	Gestión Deficiente de las Contraseñas	Filtrado de información

Fuente. Autores del proyecto

Tabla 14. Identificación y valoración del riesgo para el activo: Gestión de Transacciones

ACTIVO	AMENAZA	VULNERABILIDAD	IDENTIFICACION Y VALORACION DEL RIESGO
GESTION DE TRANSACCIONES	Hurto de Medios o Documentos	Almacenamiento sin Protección	Filtrado de Información
		Falta de Cuidado en la Disposición Final	
		Copia No Controlada Ausencia de	
		Protección Física de la Edificación	
		Trabajo No Supervisado del Personal Externo o de Limpieza	

		Ausencia o insuficiencia de Políticas Sobre Limpieza de Escritorio y pantalla	Vulneración de Información
		Ausencia de Autorización de los Recursos de Procesamiento de la Información	
	Hurto de Equipo	Protección Física de la Edificación	Filtrado de Información
		Ausencia de Procesos Disciplinarios Definidos en el Caso de Incidentes de Seguridad de la Información	
	Procesamiento Ilegal de los Datos	Ausencia de Mecanismos de Monitoreo	
		Ausencia o Insuficiencia en las Disposiciones (con respecto a la seguridad de la Información) en los Contratos con los Empleados	Filtrado de Información

Fuente. Autores del Proyecto

4.2.5 Análisis y Evaluación del Riesgo. Con el propósito de definir las acciones a emprender para tratar el riesgo identificado en el área contable de TRANSFORMADORES CDM, se realiza el proceso identificación de controles para cada uno de los riesgos previamente evaluados y de igual manera la medida en que dará respuesta la organización a dichos eventos:

Tabla 15. Análisis y evaluación del Riesgo: Servidor

SERVIDOR			
RIESGO	**EVALUACIÓN DEL RIESGO**	**MEDIDA DE RESPUESTA**	**CONTROL**
Daño de Equipo	Alta	Reducir el riesgo, evitar el riesgo, transferir	Establecer Lineamientos sobre áreas seguras Definir Lineamientos de respuesta a incidentes
Filtrado de Información	Alta	Reducir el riesgo, evitar el riesgo	Asignación de Responsabilidades de la seguridad de la información Instaurar procesos disciplinarios en el caso de incidentes de seguridad de la información Creación de planes de capacitación y concienciación sobre la seguridad de la información Localización de equipos en zona restringida Establecer lineamientos para el uso adecuado de los activos de información de la empresa
Daño de Sistema	Alta	Reducir el riesgo, evitar el riesgo	Definir directrices sobre la adquisición y mantenimiento de los sistemas de información
Detención de Procesos	Media	Reducir el riesgo, evitar el riesgo	Definir acciones para la continuidad del negocio

Fuente. Autores del proyecto

Tabla 16. Análisis y evaluación del Riesgo: equipo de cómputo fijo

EQUIPO DE COMPUTO FIJO			
RIESGO	**EVALUACIÓN DEL RIESGO**	**MEDIDA DE RESPUESTA**	**CONTROL**
Daño de Equipo	Alta	Reducir el riesgo, evitar el riesgo, transferir	Establecer Lineamientos sobre áreas seguras Definir Lineamientos de respuesta a incidentes
Filtrado de Información	Alta	Reducir el riesgo, evitar el riesgo	Asignación de Responsabilidades de la seguridad de la información Instaurar procesos disciplinarios en el caso de incidentes de seguridad de la información Creación de planes de capacitación y concienciación sobre la seguridad de la información Localización de equipos en zona restringida Establecer lineamientos para el uso adecuado de los activos de información de la empresa
Daño de Sistema	Alta	Reducir el riesgo, evitar el riesgo	Definir directrices sobre la adquisición y mantenimiento de los sistemas de información
Detención de Procesos	Media	Reducir el riesgo, evitar el riesgo	Definir acciones para la continuidad del negocio

Fuente. Autores del proyecto

Tabla 17. Análisis y evaluación del Riesgo: Gestión de Transacciones

GESTION DE TRANSACCIONES			
RIESGO	**EVALUACIÓN DEL RIESGO**	**MEDIDA DE RESPUESTA**	**CONTROL**
Filtrado de Información	Alta	Reducir el riesgo, evitar el riesgo	Asignación de Responsabilidades de la seguridad de la información Instaurar procesos disciplinarios en el caso de incidentes de seguridad de la información Creación de planes de capacitación y concienciación sobre la seguridad de la información Establecer lineamientos para el uso adecuado de los activos de información de la empresa
Vulneración de Información	Alta	Reducir el riesgo, evitar el riesgo	Asignación de Responsabilidades de la seguridad de la información Instaurar procesos disciplinarios en el caso de incidentes de seguridad de la información Establecer Lineamientos sobre áreas seguras

Fuente. Autores del Proyecto

El proceso de gestión de riesgo (identificación, valoración, análisis) permitió al grupo investigador determinar la orientación a seguir para la definición de las políticas de seguridad de la información tomando como fundamento los riesgos que mostraron un alto nivel en la evaluación del mismo; y de esta manera contribuir a la reducción de los niveles de riesgo evidenciados.

4.3 DOCUMENTACIÓN DEL PLAN DE ACCIÓN A SEGUIR PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE CONTABILIDAD DE LA EMPRESA TRANSFORMADORES CDM.

4.3.1 Objetivo del Sistema de Gestión de Seguridad de la Información para el Área Contable de la Empresa TRANSFORMADORES CDM

- El principal objetivo del sistema de gestión de seguridad de la información es mantener un ambiente seguro dentro de las restricciones que los riesgos representan, permitiendo la protección de los activos de la información que conforman el área

4.3.2 Alcance del Sistema de Gestión de Seguridad de la Información para el Área Contable de la Empresa TRANSFORMADORES CDM. El sistema de gestión de la seguridad de la información, está dado para el área contable de la empresa TRANSFROMADORES CDM, abarcando cada uno de los procesos que se desarrollan en su interior. Con el fin de proteger el más valioso activo para el área: la información.

4.3.3 Políticas de Seguridad de la Información para el Área Contable de la Empresa TRANSFORMADORES CDM.

EL JEFE DEL ÁREA CONTABLE DE TRANSFORMADORES CMD, CONSIDERA

1. PROPOSITOS

Que las políticas y prácticas de seguridad de la información establecidas, son de obligatorio cumplimiento para los empleados y contratistas de la empresa, ante su infracción se aplicaran los procedimientos sancionatorios administrativos, disciplinarios y penales según correspondan.

Que las buenas prácticas de seguridad tienen como propósito orientar a los usuarios frente a las responsabilidades que deben asumir en la seguridad, confidencialidad y salvaguarda de la información y recursos tecnológicos que se encuentren a su cargo.

RESUELVE

CAPITULO I

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

El Jefe del Área Contable de TRANSFORMADORES CDM estará en la obligación de velar por el cumplimiento de los siguientes objetivos de seguridad, en su área a cargo y será identificado como coordinador de seguridad:

1) Revisar y proponer al gerente de la empresa, para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad que fueren convenientes y apropiadas.

2) Monitorear cambios significativos en los riesgos que afectan los recursos de la información frente a posibles amenazas sean internas o externas.

3) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios que presta el área Contable, sean pres existentes o nuevos.

4) Promover la difusión y cumplimiento de las políticas de seguridad establecidas.

5) Aprobar y revisar semestralmente el plan de continuidad.

6) Aprobar el plan anual de auditorías a realizar.

3. GESTION DE ACTIVOS

El jefe del Área contable de TRANSFORMADORES CDM debe elaborar y mantener un inventario de los activos de la información que reposan en el área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

CAPITULO II

4. ENUNCIADOS DE LA POLITICA

4.1 DOCUMENTO DE POLITICAS DE SEGURIDAD

El coordinador de seguridad deberá diseñar un documento de políticas de la seguridad de la información el cual debe ser aprobado y publicado por la gerencia de la empresa a cada uno de los empleados y terceros que intervienen en los procesos del Área.

4.2 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Cada uno de los empleados del Área contable de TRANSFORMADORES CDM debe conocer la importancia del correcto uso de las herramientas tecnológicas y sus activos, como bases de datos, equipos de cómputo, comunicaciones, software, documentos reservados y clasificados, entre otros.

CONTROLES:

- El coordinador de seguridad desarrollará planes de capacitación de seguridad de la información, los cuales se realizaran periódicamente (semestralmente).

- Los empleados y contratistas son responsables de la información entregada para el desarrollo de sus funciones.

- Los empleados del área que utilicen recursos informáticos, tiene la responsabilidad de asegurad la integridad, confidencialidad, disponibilidad y confiabilidad de la información que administran.

- Todo empleado de la empresa debe abstenerse de ejecutar acciones encaminadas a eludir o violar Las Políticas de Seguridad de la Información.

4.3 SEGUIRIDAD FISICA Y AMBIENTAL

El factor ambiental muestra una importancia significativa para la empresa es por ello que crearan una serie de propuestas para impedir accesos no autorizados y evitar daños e interferencias sobre los activos de información:

CONTROLES

- Cada uno de los empleados debe velar que la información que esta consignada en documentos físicos debe ser protegidas en lugares que limiten el acceso a personal no autorizado.
- Todos los empleados de la empresa deben abstenerse de retirar equipos de cómputo, almacenamiento o equipamiento en general que contienen información del mismo.

- El coordinador de seguridad n cabeza de la gerencia de la empresa, se encargara de mantener seguras las estaciones de trabajo del área contable, mediante el uso de:
    - Controles de acceso y seguridad física.
    - Sistema de vigilancia (Cámaras, alarmas).
    - Sistema de detección de incendios.
    - Control de humedad temperatura.
    - Bajo riesgo de inundación.
    - Instalación de fuentes de potencia ininterrumpida (UPS)

- Ningún empleado podrá destapar equipos o impresoras para realizar cualquier clase de mantenimiento o instalación de hardware o software, sin una previa autorización por parte del coordinador de seguridad.

- Todos los empleados del área, deben limitar el uso de dispositivos de almacenamiento con puertos USB, tarjetas de memoria (SD, MMC, Micro SD, Mini SD Memory Stick, Compact flash1, Micro drive, entre otros) que se encuentran ubicados en los computadores o que pueden ser adaptados a los mismos.

- Ningún empleado debe descuidar documentos que contengan información, ya que esto ocasionara la consulta, copia o pérdida de la información por parte de personas no autorizadas.

- Todos los empleados de área deben abstenerse de dejar computadores de escritorio encendidos en horas no laborales, elevando con esto los niveles de riesgo frente a una posible pérdida o difusión no autorizada de la información.

- Es obligación de cada uno de los empleados destruir o desechar correctamente la documentación, evitando la posible reconstrucción de la misma.

- Los empleados deben tener especial cuidado con la seguridad de los inmuebles en cada uno de los puestos de trabajo, dejándolos bajo llave cuando se ausente de su puesto de trabajo.

- El coordinador de seguridad, establecerá un plan de mantenimiento preventivo para los equipos y velara por el cumplimiento del mismo.
- Cada uno de los empleados del área debe velar que los documentos impresos que contengan información, deben ser guardados de forma segura, no deben ser abandonados en lugares públicos o de fácil acceso a personas ajenas a dicha información.

4.4 GESTION DE COMUNICACIONES Y OPERACIONES

Diseñados para garantizar la seguridad y el respaldo de la información.

CONTROLES

- El Coordinador de Seguridad Informática o su delegado, instalará antivirus en los servidores y estaciones de trabajo y configurados para actualizaciones diarias.

- Todo empleado del área debe evitar el envío y transporte de información mediante equipos electrónicos y tecnológicos que a través de sistemas de interconexión inalámbrica permitan la transmisión y almacenamiento de datos.

- ❖ No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor, en especial la ley 23 de 1982 y su modificación, la ley 44 de 1993 y la Decisión 351 de 1993.

- ❖ Todo empleado debe abstenerse de hacer uso inadecuado de la red de datos (WANG y LAN) del establecimiento, para obtener, almacenar y difundir en los equipos de cómputo, material pornográfico, mp3, videos y películas comerciales, cadenas de correos no autorizados.

- ❖ Las instalaciones de software deben ser aprobadas por el Coordinador de Seguridad.

- ❖ Todo empleado del área debe abstenerse de realizar actividades que puedan alterar el desempeño de los sistemas de información y por ende generar posibles pérdidas o daños de la misma, como la instalación de software no licenciado, esta conducta igualmente genera riesgos, como el ingreso de virus, instalación de software espía, hurto o divulgación no autorizada de la información.

- ❖ El coordinador de seguridad garantizará la seguridad de los servicios prestados de comercio electrónico y de las transacciones en línea.

- ❖ Todos los empleados del área deben realizar copias de seguridad de los datos del computador asignado, en forma mensual o en intervalos de tiempo acordes con la necesidad del usuario y de criticidad de la información.

- ❖ El Coordinador de Seguridad Informática o su delegado, elaborará copias de seguridad semanales y las guardará en sitios bajo llave.

- ❖ Todo empleado del área debe abstenerse de efectuar la conexión de equipos de cómputo personales, a la red de datos de la empresa.

- ❖ En las oficinas donde se encuentren dispositivos de red como switch, tomas reguladas, canaletas, puntos de red y otros, los empleados deben tener cuidado de no desconcertarlos, apagarlos, no colocar objetos pesados sobre las canaletas, se deben proteger de caída de fluidos, evitar como equipos como grabadoras, cargadores y otros.

- ❖ Cuando el empleado deje el sitio de trabajo, debe cerrar las aplicaciones que se están ejecutando.

4.5 CONTROL DE ACCESOS

El control para el acceso a la información del área se regirá por una serie de directrices que aseguran que la esta no corra ningún riesgo de pérdida.

CONTROLES

- A los empleados que laboren en el área y que se les asigne un equipo de cómputo, el coordinador de seguridad les asignara una cuenta con clave de acceso, la cual tiene definido el perfil de usuario para adicionar, modificar, borrar y consultar información.

- El Coordinador de Seguridad Informática o su delegado, configurará alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataque e intentos de intrusión.

- Cuando un empleado se retire del área, debe informar al coordinador de seguridad con por lo menos un día de antelación, para realizar el correspondiente backup y cambios o eliminación de usuarios.

- Las contraseña es personal, por lo tanto no debe ser compartida ni revelada, además deben serán cambiadas periódicamente (Mínimo cada dos meses)

- Las contraseñas deben tener mínimo seis caracteres, y deben ser de orden alfanumérico.

- Está prohibido a todos los empleados del área, usar como contraseña el nombre, apellido, numero de documento, nombre de los hijos o fechas que se relacionen con el usuario, ni ninguna palabra que aparezca en un diccionario de cualquier idioma.

- Ningún empleado debe abrir archivos o ejecutar programas adjuntos a los correos si no se conoce el remitente o el asunto.

4.6 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

La seguridad de la información depende en gran parte de los controles de seguridad inmersos en las aplicaciones que se manejan.

CONTROLES:

- Las aplicaciones contarán con el Log de Auditoría, en el cual quedará registrado el usuario, la fecha, hora, módulo y opción a la que ingresó, facilitando al Coordinador de Seguridad Informática, la revisión de incidentes en el manejo de las aplicaciones.

- Se debe llevar una Bitácora con el control de cambios de las aplicaciones, indicando la fecha, hora, aplicación a la que se realizó el cambio, la causa, los cambios realizados y la persona que lo realizó.

4.7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Una adecuada gestión de incidentes le permitirá al establecimiento responder a los incidentes de manera sistemática, eficiente y rápida; volver a la normalidad en poco tiempo, perder muy poca información; realizar continuamente mejoras en la gestión y tratamiento de incidentes; generar una base de conocimientos sobre incidentes; evitar en lo posible, incidentes repetitivos.

CONTROLES:

- El Coordinador de Seguridad Informática ante una incidencia, debe diligencia el correspondiente formato donde quede consignados los datos de reporte del incidente y de la persona que reportó:

REPORTE DE INCIDENTES		
No.	**HORA**	**FECHA**
DESCRIPCION DEL INCIDENTE		
EFECTOS PRODUCIDOS		
RESPONSABLE DEL ACTIVO AFECTADO		
CAUSAS DEL INSIDENTE (Se diligencia una vez se recupere la normalidad del proceso afectado)		
DATOS DEL REPONRTANTE		
NOMBRE	**CARGO**	

- ❖ Una vez verificada la incidencia, el Coordinador de Seguridad de la Información recolectará la información que le permitirá determinar el alcance del incidente, qué redes y que sistemas y aplicaciones fueron afectados, y que fue lo que generó el incidente, como ocurrió o está ocurriendo, también nos permite saber que originó el hecho, cómo ocurrió y las herramientas utilizadas, qué vulnerabilidades fueron explotadas y el impacto negativo que pueda tener sobre la empresa.

  Para determinar el alcance, el Coordinador de Seguridad de la Información puede hacerse las siguientes preguntas:
  - ¿Cuántos equipos fueron comprometidos?
  - ¿Hasta qué punto de la red logró penetrar el atacante?
  - ¿Qué nivel de privilegio logró el atacante?
  - ¿Qué es lo que está en riesgo?
  - ¿Cómo impacta en las actividades de la universidad el compromiso de los equipos?
  - ¿Se encuentran en riesgo aplicaciones críticas?
  - ¿Cuán conocida es la vulnerabilidad explotada por el atacante?
  - ¿Hay otros equipos con la misma vulnerabilidad?

- ❖ Determinado el alcance del incidente de seguridad, el Coordinador de Seguridad de la Información procederá a la contención, respuesta y puesta en marcha de las operaciones afectadas por el incidente.

CAPITULO III

5 GLOSARIO

AMENAZA: Evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización.

BITÁCORA: Libro donde se registran las observaciones de un evento

CA NALETAS: Una canaleta es un canal que contiene cables en una instalación. Las canaletas incluyen conductos comunes de electricidad, bandejas de cables especializadas o bastidores de escalera, sistemas de conductos incorporados en el piso, y canaletas de plástico o metal para montar sobre superficies.

CONTRASEÑA: Conjunto de caracteres que permite el ingreso a un recurso informático.

CRIPTOGRAFÍA: Ciencia que se encarga de estudiar las distintas técnicas empleadas para transformar ("encriptar") la información y hacerla irreconocible a los usuarios no

autorizados de un sistema informático, de modo que sólo los legítimos propietarios puedan recuperar ("desencriptar") la información original

INCIDENTE DE SEGURIDAD: Es cualquier evento que pueda o pueda tener como resultado la interrupción de los servicios suministrados por un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

LOG DE AUDITORÍA: Término usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para una aplicación.

IMPACTO: Daño potencial sobre un sistema cuando una amenaza se presenta.

RIESGO: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización.

SERVIDOR: Computadora que ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones llamadas clientes.

SWITCH: dispositivo inteligente utilizado en redes de área local

SISTEMA DE INFORMACIÓN: Conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.

TI: Tecnología de la Información y Comunicaciones.

UPS: Uninterrumpible Power Supply

VULNERABILIDAD: Cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas para la organización.

WAN: es una red de computadoras de gran tamaño, generalmente dispersa en un área metropolitana, a lo largo de un país o incluso a nivel planetario.

6 HISTÓRICO DE REVISIONES, ACTUALIZACIONES Y APROBACIONES

Cada año la Política de Seguridad debe ser revisada y retroalimentada en los aspectos que sean necesarios y los cambios serán documentados en un Registro de Cambios de la Política de Seguridad Informática, se harán las modificaciones respectivas en el documento y posteriormente se socializara con los empleados del área.

REGISTRO DE CAMBIOS DE LA POLÍTICA DE SEGURIDAD INFORMÁTICA					
AÑO	**ASPECTO A MODIFICAR**	**CONTROL ACTUAL**	**CONTROL MODIFICADO**	**PERSONA QUE RELAIZA LA MODIFICACION**	**CARGO**

5. CONCLUSIONES

Al aplicar los instrumentos de recolección de la información diseñados, además de la matriz de comprobación de la Norma ISO/IEC 27001, se evidencio el estado real en el que se encuentra la seguridad de la información del área contable de TRANSFORMADORES CDM y el alto riesgo en que se encuentra, en su mayoría concentrado en los aspectos de seguridad física y lógica de la información, y así se logró determinar que el proceso de desarrollo del proyecto se orientara al estudio de estos aspectos.

Tomando como base los resultados del proceso de recolección de información y su posterior análisis, se llevó a cabo el proceso de gestión de riesgos asociados a la seguridad de la información en el área de contabilidad en la empresa TRANSFORMADORES CDM, identificando en cada una de sus fases los elementos correspondientes mediante el apoyo de la Norma ISO/IEC 27005, MAGERIT e ISO/IEC 27001.

Con el proceso de gestión de riesgos se corroboro el alto grado de riesgo al que se encuentra expuesta la seguridad física y lógica de la información del área contable de la empresa, permitiendo definir el direccionamiento para la política de seguridad de la información posteriormente planteada; así se concentró su desarrollo en la reducción del riesgo de los aspectos identificados como significativos.

Para la formulación de las políticas de la seguridad de la información, se tomaron en cuenta los dominios de la norma ISO/IEC 27001 encaminados a generar controles para mejorar el tratamiento de la información de acuerdo a las necesidades específicas del área.

6. RECOMENDACIONES

Se recomienda al jefe del área contable de TRANSFORMADORES CDM, asumir el rol del coordinador de seguridad con el fin velar por la seguridad de la información del área implementando los controles necesarios.

Socializar la política de seguridad de la información planteada como resultado del desarrollo de este proyecto, con cada uno de los empleados del área contable y directivos de la empresa.

Generar campañas de concientización sobre la importancia de la seguridad de la información al interior de la empresa.

Abordar las fases siguientes para el desarrollo del Sistema de Gestión de Seguridad de la Información, además de expandir su implementación a los procesos desarrollados por toda la empresa.

BIBLIOGRAFÍA

ISACA COBIT 5 [Libro]. - [s.l.] : ISACA, 2012.

ISO/IEC 27001. Norma ISO sobre Seguridad Informática. Resumen. Estándar ISO/IEC Internacional 17799. Introducción. Que es la seguridad de la Información. Segunda edición 2015-06.15.

ISO/IEC 27002. Norma Técnica Colombiana. Términos y definiciones. ICONTEC Internacional.

QUINTANA, Yesid. TORRADO, Wilson. Trabajo de Grado. Planeación del sistema de gestión de seguridad de la información para la empresa "katalinda shoes". Ocaña 2015. Especialización e Auditoria de Sistemas. UFPSO. Facultad de Ingenierías. Pág. 95. Norte de Santander.

Johnson Isabelle Redefining the concept of governance [Publicación periódica]. - [s.l.] : Canadian International Development Agency, 1997.

Management MIT/Sloan School of MIT/Sloan School of Management [Publicación periódica]. - 2004.

NTC- ISO/IEC 27001 [Libro]. - 2013.

P. Leonardo D. Timothy M. William Planeación Estrategica Aplicada [Libro]. - [s.l.] : Mc Graw Hill., 1998.

REFERENCIAS ELECTRONICAS

27001 ACADEMY. ¿Qué es Norma ISO 27001? Una introducción simple a los aspectos básicos [en línea]. Actualizado en el 2015. [Citado en agosto 20 de 2015]. Disponible en Internet en (http://advisera.com/27001academy/es/que-es-iso-27001/)

27001 ACADEMY. Cuatro beneficios claves de la implementación de la Norma ISO 27001. [En línea]. Actualizado en el 2015. [Citado en agosto 20 de 2015]. Disponible en Internet en: (http://advisera.com/27001academy/es/blog/2010/07/21/cuatro-beneficios-clave-de-la-implementacion-de-la-norma-iso-27001/)

ISO 27000. El portal de ISO 27001 en español. Glosario. [en línea]. Actualizado en el 2012. [Citado en septiembre 2015]. Disponible en Internet en: (http://www.iso27000.es/glosario.html)

TRANSFORMADORES CDM. Quienes somos. [En línea]. Actualizado en el 2016. [Citado en Octubre 10 de 2015]. Disponible en Internet en: (http://www.transformadorescdm.com/quienes-somos.html)

ANEXOS

Anexo A. Entrevista Simple

Entrevista Jefe de contabilidad del área de Contabilidad
Fecha: Miércoles 6 de mayo.
Entrevistado: Melba aponte
Entrevistador: Ing. Joaquín Guerrero, Ing. Javier Suarez
Entrevistador: Buenas tarde, Doctora Melba Aponte, Vengo a Conocer como está organizada la seguridad informática en el área contable de la empresa.
Entrevistado: Buenas tardes ingenieros, en nuestra área contable no con contamos herramientas ni software que nos permita tener copia de seguridad de los 6 equipos.
Entrevistador: ¿Existe algún software contable en la empresa, si existe, Como se llama?
Entrevistado: Si, nuestro software contable se llama TNS.
Entrevistador: ¿Como manejan los respaldos de seguridad de este software?
Entrevistado: Bueno, lo que se tiene entendido es que el software debe realizar una copia seguridad diaria, y la guarda en una carpeta interna del programa.
Entrevistador: ¿Confía usted en ese tipo de copias de seguridad automáticas?
Entrevistado: No, una vez tuvo una falla el servidor y solo lograron salvar una copia de seguridad del mes anterior, teniendo que digitar nuevamente la información.
Entrevistador: ¿Son muy recurrentes la pérdida de información del área contable?
Entrevistado: Si, Debido a que la planta de producción se genera variaciones en la electricidad.
Entrevistador: Debido a las variaciones que se presentan en esta área, ¿cuentan con un sistema de respaldo eléctrico?
Entrevistado: Solo existe uno para el servidor; el departamento técnico ya está trabajando en eso.
Entrevistador: ¿El área contabilidad cuenta con un antivirus de seguridad pago?
Entrevistado: No, Solo el servidor
Entrevistador: ¿Ha Tenido que recurrir al ingeniero de soporte por problemas de virus en sus archivos?
Entrevistado: Muchas veces, debido a esto hemos implementado una norma, de no ingresar memorias que no sean de la empresa y eliminado el acceso a internet en algunos equipos.
Entrevistador: ¿Algún comentario que desea agregar a la entrevista?
Entrevistado: Estamos armando un presupuesto para adquirir nueva tecnología y mejorar el área de sistemas de la empresa, a corto plazo.

Anexo B. Encuesta al personal del área contable

1. ¿Se tiene en cuenta el respaldo de los datos en el puesto trabajo?
Si
No
¿Por qué?

2. ¿Está permitido el acceso de personal no autorizado al puesto de trabajo?
Si
No
No sabe

3. ¿Se ha establecido un control para que los usuarios de otras dependencias no manipulen información sin ser autorizados?
Si
No
No sabe

4. ¿Existe un protocolo para hacer las copias de seguridad de los datos?
Si
No
No sabe

5. ¿Se tiene definido una restauración de sistemas informáticos, en caso de pérdida de información?
Si
No
No sabe

Anexo C. MATRIZ DE CUMPLIMIENTO CONTROLES ISO 27001

ITEM	DOMINIO			
5	**POLITICA DE SEGURIDAD**			
5.1	**Politica de Seguridad de la Información**	**Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.**		
5.1.1	Documento de la política de seguridad de la información	¿Se tiene una Política de seguridad de la información desarrollada y documentada?	NO CUMPLE	1
5.1.2	Revisión de la política de seguridad de la información	El documento de políticas de seguridad de la información se encuentra publicado? Este es revisado por la dirección constantemente?	NO CUMPLE	1
6	**ORGANIZACIÓN DE SEGURIDAD**			
6.1	**Organización de la SI**	**Se debería establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.**		
6.1.1	Compromiso de la dirección con la seguridad de la información	¿Se evidencia el compromiso demostrado de la dirección frente a la seguridad de la información en la organización?, Con una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información?	NO CUMPLE	1
6.1.2	Coordinación de la seguridad de la información	¿Ha sido establecido un proceso para coordinar la implementación o puesta en práctica de las medidas de seguridad de la información?	NO CUMPLE	1
6.1.3	Asignación de responsabilidades para la seguridad de la información	¿Las responsabilidades de la realización de los requisitos/requerimientos/responsabilidades de la seguridad de la información se definen claramente? ¿Han sido definidos?	NO CUMPLE	1
6.1.4	Proceso de autorización para los servicios de procesamiento de información	¿Se ha establecido un proceso de autorización de la dirección para nuevos servicios de procesamiento de información? (Punto de vista del negocio y técnico)	NO CUMPLE	1
6.1.5	Acuerdos sobre confidencialidad	¿Se ha definido un procedimiento de identificación y revisión de los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información?	NO CUMPLE	1
6.1.6	Contacto con las autoridades / contactos con grupos de interés especial	¿Existe un acuerdo o contactos con personal externo y/o organizaciones que maneje el tema de la seguridad de la información? incluyendo especialistas de la seguridad de la industria y/o de gobierno;	NO CUMPLE	1
6.1.7	Revisión independiente de la seguridad de la información	autoridades de ley; Proveedores de servicio TI; autoridades de telecomunicaciones?	NO CUMPLE	1
6.2	**Partes Externas**	**Mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso terceras partes o que son procesados, comunicados o dirigidos por éstas.**		
6.2.1	Identificación de los riesgos relacionados con las partes externas	¿Una revisión independiente de las prácticas de la seguridad de la información se ha conducido para asegurar viabilidad, eficacia, y conformidad con políticas escritas? ¿Esta establecida la revisión a intervalos de tiempo planificados?	NO CUMPLE	1
6.2.2	Riesgos conexiones con terceros	¿Se han analizado los riesgos para la información y los servicios de procesamiento de información en los procesos de negocio que incluyen o involucran a partes externas?	NO CUMPLE	1
6.2.3	Abordaje de la seguridad cuando se trata con los clientes	¿Se han identificado las medidas de seguridad específicas de combatir riesgos de la conexión de los terceros?	NO CUMPLE	1
6.2.4	Abordaje de la seguridad en los acuerdos con terceras partes	¿Se han identificado los requisitos de seguridad antes de dar acceso a los clientes a los activos o la información de la organización?	NO CUMPLE	1
6.3	Partes Externas (outsourcing)	¿Los requisitos de la seguridad se incluyen en contratos formales con terceras partes?	NO CUMPLE	1
7	**CONTROL DE ACTIVOS**			
7.1	**Responsabilidad por los activos**	**Lograr y mantener la protección adecuada de los activos de la organización. Todos los activos se deben incluir y deben tener un dueño designado**		
7.1.1	Inventario de activos	¿Los inventarios de activos importantes asociados a cada sistema de información se han creado?	CUMPLE PARCIALMENTE	2
7.1.2	Propiedad de los activos	¿La información y los activos asociados con los servicios de procesamiento de información tienen asignado un propietario parte de la organización?	CUMPLE PARCIALMENTE	2
7.1.3	Uso aceptable de los activos	¿Se han identificado, documentado e implementado reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información?	NO CUMPLE	1
7.2	**Clasificación de la información**	**Asegurar que la información recibe el nivel de protección adecuado**		
7.2.1	Directrices de clasificación	¿Las pautas de la clasificación de seguridad se han establecido para indicar la necesidad , y las prioridades, de la protección de la seguridad?	NO CUMPLE	1
7.2.2	Etiquetado y manejo de la información	¿Se ha implementado un procedimiento para el etiquetado y manejo de la información?	NO CUMPLE	1

8	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
8.1	**Antes de la Relación Laboral**	**Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.**		
8.1.1	Roles y responsabilidades	¿Las responsabilidades de la seguridad se incluyen en descripciones de las funciones del empleado?	NO CUMPLE	1
8.1.2	Selección	Son las aplicaciones de empleados para un trabajo revisadas de acuerdo al tipo de trabajo (Cargo) a realizar y los niveles de acceso a información sensible acorde con el cargo a cumplir?	CUMPLE PARCIALMENTE	2
8.1.3	Términos y Condiciones laborales	¿Los términos y las condiciones del empleo incluyen la responsabilidad del empleado de la seguridad de la información, incluyendo la duración después del empleo y consecuencias de la falta de satisfacer estos términos?	CUMPLE PARCIALMENTE	2
8.2	**Durante la Relación Laboral**	**Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respectos a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano**		
8.2.1	Responsabilidad de la dirección	Se evidencia una exigencia de la dirección para que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización?	NO CUMPLE	1
8.2.2	Educación, formación y concientización sobre la SI	Existe un programa de capacitación a empleados, contratistas, etc. de concientización de seguridad, políticas y procedimientos de seguridad , según sea pertinente para sus funciones laborales?	NO CUMPLE	1
8.2.3	Proceso disciplinario	¿Existe definido un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad?	NO CUMPLE	1
8.3	**Terminación o cambio**	**terceras partes salen de la organización o cambian su contrato**		
8.3.1	Responsabilidades en la terminación	¿Existe un proceso de terminación donde estén claramente definidas las responsabilidades para llevar a cabo la terminación o el cambio de la relación laboral con empleados?	NO CUMPLE	1
8.3.2	Devolución de activos	¿Existe establecido un procedimiento aplicado a los empleados, contratistas u usuarios de terceras partes donde se establezca como parte del mismo la devolución todos los activos de la organización que estén en su poder al finalizar su relación laboral, contrato o acuerdo?	CUMPLE PARCIALMENTE	2
8.3.3	Retiro de los derechos de acceso	¿Existe un procedimiento (Documentado) de retiro de acceso a los sistemas de procesamiento de información a empleados, contratistas o terceras partes al finalizar la relación laboral, contrato o acuerdo?	NO CUMPLE	1

9	**SEGURIDAD FISICA DEL ENTORNO**	**SEGURIDAD FÍSICA DEL ENTORNO**		
9.1	**Areas seguras**	**Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.**		
9.1.1	Perímetro de seguridad física	¿Existen elementos de seguridad física para proteger las áreas que contienen información y servicios de procesamiento?	CUMPLE PARCIALMENTE	2
9.1.2	Controles de acceso físico	¿Se emplean los controles de la entrada en áreas seguras para asegurar ingreso solamente a personal autorizado?	CUMPLE PARCIALMENTE	2
9.1.3	Seguridad de oficinas, recintos y servicios	¿Es la seguridad física para los centros de datos y las salas de cómputo conmensurada con amenazas? (Documentada)	NO CUMPLE	1
9.1.4	Protección contra amenzas externas y ambientales	¿Existen mecanismos de protección física contra daño por incendio, inundación, terremoto, explosión, malestar social y otras formas de desastre natural o artificial?	NO CUMPLE	1
9.1.5	Trabajo en áreas seguras	¿Se utilizan controles adicionales para el personal o los terceros que trabajan en el área segura?	CUMPLE PARCIALMENTE	2
9.1.6	Áreas de carga, despaho y acceso	¿Existen controles en los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones? Estos puntos se encuentran aislados de los servicios de procesamiento de información?	CUMPLE PARCIALMENTE	2
9.2	**Seguridad de los equipos**	**Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización**		
9.2.1	Ubicación y protección de los equipos	¿El equipo se localiza para reducir riesgos de peligros ambientales y del acceso no autorizado?	CUMPLE PARCIALMENTE	2
9.2.2	Servicios de soporte	¿El equipo electrónico se protege contra apagones y otras anomalías eléctricas?	CUMPLE PARCIALMENTE	2
9.2.3	Seguridad del cableado	¿El cable de la energía y de las telecomunicaciones se protege contra la interceptación o daño?	CUMPLE PARCIALMENTE	2
9.2.4	Mantenimiento de los equipos	¿Se han establecido procedimientos para correcto mantenimiento de equipos y de esta forma asegurar su disponibilidad e integridad de manera continua?	NO CUMPLE	1
9.2.5	Seguridad de los equipos fuera de las instalaciones	¿Se aplica la misma seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización?	NO CUMPLE	1
9.2.6	Seguridad en la reutilización o eliminación de los equipos	¿Existe algún mecanismo para tratamiento de equipos una vez estos se reutilizan o eliminan? (Procedimiento)	CUMPLE PARCIALMENTE	2
9.2.7	Retiro de propiedad	¿Existe un procedimiento definido para retiro de equipos, información o software bajo previa autorización de la gerencia?	CUMPLE PARCIALMENTE	2

10	**GESTION DE LAS COMUNICACIONES Y OPERACIONES**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**		
10.1	**Procedimientos de Op. y Resp.**	**Asegurar la operación correcta y segura de los servicios de procesamiento de información.**		
10.1.1	Procedimientos de operación documentados	¿Se documentan los procedimientos de operación (funcionamiento) para que todos los sistemas informáticos aseguren su operación correcta y segura?	CUMPLE PARCIALMENTE	2
10.1.2	Gestión del cambio	¿Hay un proceso para el control de los cambios a las instalaciones de IT y los sistemas para asegurar el control satisfactorio de los equipos, software o a los procedimientos?	CUMPLE SATISFACTORIAMENTE	3
10.1.3	Distribución de funciones	¿Están establecidas separaciones entre las funciones y las áreas de responsabilidad para reducir las oportunidades de la modificación no autorizada o el mal uso de datos o de servicios? Especifique.	NO CUMPLE	1
10.1.4	Separación de las instalaciones de desarrollo, ensayo y op	¿Las instalaciones de desarrollo, ensayo(Prueba) y producción (Operación) se separan para reducir el riesgo de cambios accidentales o del acceso no autorizado al software operacional y a los datos de negocio?	CUMPLE PARCIALMENTE	2
10.2	**Gestión servicios de terceros**	**Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes**		
10.2.1	Prestación del servicio	¿Los controles de seguridad, las definiciones del servicio y los niveles de prestación incluidos en el acuerdo de prestación del servicio por terceras partes, están siendo implementados, mantenidos y operados por las terceras partes?	NO CUMPLE	1
10.2.1	Monitoreo y revisión de los servicios por terceras partes	¿Se controlan y revisan los servicios, reportes y registros suministrados por terceras partes?	CUMPLE PARCIALMENTE	2
10.2.3	Gestión de los cambios en los servicios por terceras partes	¿Se posee un procedimiento de gestión de cambios en la prestación de servicios con terceras partes? Incluir mantenimiento, mejoras de políticas existentes de seguridad, procedimientos, sistemas, etc.	NO CUMPLE	1
10.3	**Planificación y aceptación del sistema**	**Minimizar el riesgo de fallas en los sistemas**		
10.3.1	Gestión de la capacidad	¿Se supervisan o hacen seguimiento los requisitos de la capacidad, y se proyectan los requisitos futuros, para reducir el riesgo de la sobrecarga del sistema?	NO CUMPLE	1
10.3.2	Aceptación del sistema	¿Los criterios de la aceptación para los nuevos sistemas se han establecido?, y las pruebas convenientes se han realizado antes de la aceptación?	NO CUMPLE	1
10.4	**Protección contra códigos móviles y maliciosos**	**Proteger la integridad del software y de la información**		
10.4.1	Controles contra código maliciosos	¿Se han implementado las medidas preventivas de detección y prevención de virus y los procedimientos del concientización de usuarios?	CUMPLE PARCIALMENTE	2
10.4.2	Controles contra códigos moviles	¿Existe una política de seguridad definida para la autorización y tratamiento de código móvil ?	CUMPLE PARCIALMENTE	2
10.5	**Respaldo**	**Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.**		
10.5.1	Respaldo de información	¿Se ha establecido un procedimiento para hacer copias de respaldo de los datos y del software esenciales de negocio para asegurarse de que puede ser recuperado después de un desastre de sistema de cómputo o de una falta de los medios?	CUMPLE PARCIALMENTE	2
10.6	**Gestión de Seguridad de las redes**	**Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.**		
10.6.1	Controles de las redes	¿Existen controles apropiados que aseguran la seguridad de datos en redes, y la protección de servicios conectados contra el acceso no autorizado?	NO CUMPLE	1
10.6.2	Seguridad de los servicios de red	Se tiene claro que en cualquier acuerdo sobre servicios de red se deberían identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red? ¿Se sigue esta práctica?	NO CUMPLE	1
10.7	**Manejo de los medios**	**Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada y la interrupción en las actividades de negocio**		
10.7.1	Gestión de los medios removibles	¿Existen procedimientos para la gestión de los medios removibles de las computadoras tales como cintas, discos, cassettes, e informes impresos?	CUMPLE PARCIALMENTE	2
10.7.2	Eliminación de los medios	la computadora son eliminados con seguridad cuando estos no se	NO CUMPLE	1
10.7.3	Procedimientos para el manejo de la información	tales datos contra acceso no autorizado o divulgación?	CUMPLE PARCIALMENTE	2
10.7.4	Seguridad de la documentación del sistema	¿La documentación del sistema se protege contra el acceso no autorizado?	CUMPLE PARCIALMENTE	2
10.8.	**Intercambio de Información**	**intercambian dentro de la organización y con cualquier entidad**		
10.8.1	Políticas y procedimientos para el intercambio de información	¿Existen establecidas políticas, procedimientos y controles formales de intercambio para proteger el intercambio de información a través del uso de todos los tipos de servicio de comunicación?	NO CUMPLE	1
10.8.2	Acuerdos para el intercambio	¿Existen acuerdos para el intercambio de información y software entre la organización y partes externas?	NO CUMPLE	1
10.8.3	Medios Físicos en Tránsito	¿Se aplican controles para salvaguardar a los medios de la computadora que son transportados entre sitios para reducir al mínimo su vulnerabilidad al acceso no autorizado, al mal uso, o a la corrupción durante el transporte?	NO CUMPLE	1
10.8.4	Mensajería electrónica	¿Se aplican controles cuando sea necesario reducir los riesgos de negocio y de seguridad asociados con el correo electrónico para dar frente a la interceptación, la modificación y errores?	CUMPLE PARCIALMENTE	2
10.8.5	Sistemas de información del negocio	¿Existen desarrolladas e implementadas políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio?	NO CUMPLE	1
10.9.	**Servicios de Comercio Electrónico**	**Garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.**		
10.9.1	Comercio Electrónico	¿Se aplican controles de la seguridad para proteger comercio electrónico (los datos electrónicos intercambian, correo electrónico, y las transacciones en línea a través de una red pública tal como el Internet) contra la interceptación o la modificación desautorizada?	CUMPLE PARCIALMENTE	2
10.9.2	Transacciones en línea	¿Se implementan mecanismos de protección de información en transacciones en línea para evitar transmisión incompleta, enrutamiento inadecuado, alteración no autorizada del mensaje, divulgación no autorizada, duplicación o repetición no autorizada del mensaje?	NO CUMPLE	1
10.9.3	Información disponible al público	¿Hay un proceso formal de la autorización antes de que la información se haga disponible al público?	CUMPLE PARCIALMENTE	2
10.10.	**Monitoreo**	**Detectar actividades de procesamiento de información no autorizada**		
		¿Existe procedimiento o disposición para mantener y elaboran durante		

11..	**CONTROL DE ACCESO**	**CONTROL DE ACCESO**		
11.1.	**Requisitos del negocio para el control de acceso**	**Controlar el acceso a la información**		
11.1.1	Política de control del acceso	¿Los requisitos del negocio se definen y se documentan para el control de acceso?	CUMPLE PARCIALMENTE	2
11.2.	**Gestión de Acceso de Usuarios**	**Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información**		
11.2.1	Registro de usuarios	¿Hay un procedimiento formal del registro y de la cancelación de registro del usuario para el acceso a todos los servicios de información?	NO CUMPLE	1
11.2.2	Gestión de privilegios	¿Hay restricciones y controles sobre la asignación y uso de privilegios de los usuarios en los sistemas de información (Multiusuario)? ¿Existe un proceso formal para esto?	CUMPLE PARCIALMENTE	2
11.2.3	Gestión de contraseñas para usuarios	¿Se ha establecido un proceso formal de gestión de las contraseñas?	CUMPLE PARCIALMENTE	2
11.2.4	Revisión de los derechos de acceso de los usuarios	¿Existe un proceso formal para la revisión periódica de los derechos de acceso de usuarios?	NO CUMPLE	1
11.3.	**Responsabilidades de los usuarios**	**Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información**		
11.3.1	Uso de contraseñas	¿Se han enseñado los usuarios buenas prácticas de la seguridad en la selección y el uso de contraseñas?	CUMPLE SATISFACTORIAMENTE	3
11.3.2	Equipo de usuario desatendido	¿Se concientiza a todos los usuarios y contratistas de los requisitos y de los procedimientos de la seguridad para proteger equipo desatendido? ¿Están todos los usuarios y contratistas concientizados de sus responsabilidades de poner tal protección en ejecución?	NO CUMPLE	1
11.3.3	Política de escritorio despejado y de Pantalla despejada	¿Se tiene adoptada una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información?	NO CUMPLE	1
11.4.	**Control de Acceso a redes**	**Evitar el acceso no autorizado a servicios en red**		
11.4.1	Política del uso de los servicios en red	¿Un proceso existe para asegurarse de que la red y los servicios informáticos que se pueden alcanzar por un usuario individual o de una Terminal particular son consistentes con la política del control de acceso del negocio?	NO CUMPLE	1
11.4.2	Autenticación de usuarios para conexiones externas	¿Las conexiones de los usuarios remotos vía redes públicas o no pertenecientes a la organización se autentican para prevenir el acceso no autorizado a las aplicaciones del negocio?	NO CUMPLE	1
11.4.3	Identificación de los equipos en las redes	¿Existe un mecanismo de identificación automática de los equipos que sirva para autenticar conexiones de equipos y lugares específicos? ¿Qué métodos se utilizan para dicha identificación?	NO CUMPLE	1
11.4.4	Protección de los puertos de configuración y diagnóstico remoto	¿Existe un proceso para controlar el acceso a los puertos de diagnóstico diseñados para el uso remoto por personal autorizado?	NO CUMPLE	1
11.4.5	Separación en las redes	¿Las redes grandes se han dividido en dominios separados para atenuar el riesgo del acceso no autorizado a los sistemas informáticos existentes que utilizan la red?	CUMPLE PARCIALMENTE	2
11.4.6	Control de las conexiones en red	¿Se han incorporado controles para restringir la capacidad de la conexión de usuarios en aquellas redes que se extienden mas allá de las fronteras de la organización? (Dando cumplimiento a la política de acceso y requisitos de aplicación del negocio)	CUMPLE PARCIALMENTE	2
11.4.7	Control del enrutamiento en la red	¿Se han incorporado controles de enrutamiento a través de los límites de organización para asegurarse de que las conexiones de los sistemas de cómputo y la información fluye de acuerdo con la política del acceso de las unidades de negocio?	NO CUMPLE	1
11.5.	**Control de Acceso al sistema Operativo**	**Evitar el acceso no autorizado a los sistemas operativos**		
11.5.1	Procedimientos de ingreso seguros	¿Existe un procedimiento de registro de inicio seguro en los sistemas operativos?	NO CUMPLE	1
11.5.2	Identificación y autenticación del usuario	¿Todos los usuarios tienen un identificador único (userID) para su uso personal y único, para asegurarse de que sus actividades se pueden rastrear?	CUMPLE PARCIALMENTE	2
11.5.3	Sistema de gestión de contraseñas	¿Un sistema de gestión eficaz de la contraseña se emplea para autenticar a usuarios?	NO CUMPLE	1
11.5.4	Uso de las utilidades del sistema	¿Se restringen los programas utilitarios de sistema que se podrían utilizar para pasar los controles de sistema y aplicaciones? Su uso es restringido?	CUMPLE PARCIALMENTE	2
11.5.5	Tiempo de inactividad de la sesión	¿Las terminales en localizaciones de riesgo elevado se les configurada bloqueo cuando son inactivos por cierto tiempo a fin de prevenir el acceso por personas no autorizadas?	NO CUMPLE	1
11.5.6	Limitación del tiempo de conexión	¿Se ha fijado un límite en el período durante el cual los terminales se pueden conectar con los sistemas de uso sensibles?	NO CUMPLE	1
11.6.	**Control de Acceso a las Aplicaciones y a la Información**	**Evitar el acceso no autorizado a la información contenida en los sistemas de información**		
11.6.1	Restricción del acceso a la información	¿El acceso a los datos y a las funciones del sistema de aplicaciones se restringe de acuerdo con la política de acceso definida y esta se basa en requisitos individuales?	NO CUMPLE	1
11.6.2	Aislamiento de sistemas sensibles	¿Según riesgos identificados, los sistemas de aplicaciones sensibles funcionan en un ambiente de proceso aislado?	NO CUMPLE	1
11.7.	**Computación Móvil y Trabajo Remoto**	**Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto**		
11.7.1	Computación y comunicaciones móviles	¿Se ha desarrollado una política formal que trata los riesgos del trabajo con las instalaciones de computación móvil, que incluyan los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, el respaldo, y la protección de virus?	NO CUMPLE	1
11.7.2	Trabajo remoto	¿Las políticas y los procedimientos se han desarrollado para controlar teleworking, las instalaciones existentes que abarcaban, el ambiente teleworking propuesto, requisitos de la seguridad de comunicaciones, y la amenaza del acceso no autorizado al equipo o a la red?	NO CUMPLE	1

12..	**ADQUISICIÓN, DESARROLLO y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	**ADQUISICIÓN, DESARROLLO y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**		
12.1.	**Requisitos de seguridad de los sistemas de información**	**Garantizar que la seguridad es parte integral de los sistemas de información**		
12.1.1	Análisis y especificación de los requisitos de seguridad	¿Se realiza un análisis de los requisitos de la seguridad como parte de la etapa del análisis de requisitos de cada proyecto del desarrollo?	NO CUMPLE	1
12.2.	**Procesamiento correcto de las aplicaciones**	**Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones**		
12.2.1	Validación de los datos de entrada	¿Los Datos que se ingresan en sistemas de aplicaciones se validan para asegurarse de que son correctos y apropiados?	NO CUMPLE	1
12.2.2	Control del procesamiento interno	¿Chequeos de validación se han incorporado en sistemas para detectar la corrupción causada por errores de proceso o por actos deliberados?	NO CUMPLE	1
12.2.3	Integridad del mensaje	¿La autentificación del mensaje se ha considerado para las aplicaciones que implican la transmisión de datos sensibles?	NO CUMPLE	1
12.2.4	Validación de los datos de salida	¿Los datos de salida de los sistemas de aplicación se validan para asegurarse de que son correctos y apropiados?	NO CUMPLE	1
12.3.	**Controles Criptográficos**	**Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos**		
12.3.1	Política sobre el uso de controles criptográficos	¿La gerencia ha desarrollado una política en el uso de controles criptográficos, incluyendo la gerencia de las llaves del cifrado, y se implementación eficaz?	NO CUMPLE	1
12.3.2	Gestión de llaves	¿Es un sistema de administración implementado para soportar el uso en la organización de lleves publicas y llevas privadas?	NO CUMPLE	1
12.4.	**Seguridad de los archivos del sistema**	**Garantizar la seguridad de los archivos del sistema**		
12.4.1	Control del software operativo	¿Se tiene un estricto control sobre la implementación de software en sistemas operacionales?	NO CUMPLE	1
12.4.2	Protección de los datos de prueba del sistema	¿Se protegen y se controlan todos los datos de la prueba de los sistemas de aplicación?	NO CUMPLE	1
12.4.3	Control del acceso al código fuente de programas	¿Para reducir el potencial para la corrupción de los programas de computadora, el acceso a las bibliotecas fuente del programa es estrictamente controlado?	NO CUMPLE	1
12.5.	**Seguridad en los procesos de desarrollo y soporte**	**Mantener la seguridad del software y de la información del sistema de aplicaciones**		
12.5.1	Procedimientos de control de cambios	¿Se ha implementado un procedimiento formal de control de cambios?	CUMPLE PARCIALMENTE	2
12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	¿Se revisan los sistemas de aplicaciones cuando ocurren cambios a nivel de los sistemas operativos?	CUMPLE PARCIALMENTE	2
12.5.3	Restricciones en los cambios a los paquetes de software	¿Se desalienta la realización de modificaciones a los paquetes de software? ¿Se limitan a los cambios necesarios, y todos los cambios se controlan estrictamente?	NO CUMPLE	1
12.5.4	Fuga de Información (Canales Encubiertos y Código Troyano)	¿Se consideran los siguientes aspectos para limitar el riesgo de fuga de información, por ejemplo, mediante el uso y explotación de los canales encubiertos?	NO CUMPLE	1
		a) exploración de los medios y comunicaciones de salida para determinar la información oculta;	NO CUMPLE	1
		b) comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento;	NO CUMPLE	1
		c) utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados (véase la norma ISO/IEC 15408);	NO CUMPLE	1
		d) monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes;	CUMPLE PARCIALMENTE	2
		e) monitoreo del uso de los recursos en los sistemas de computador	CUMPLE PARCIALMENTE	2
12.5.5	Desarrollo de software contratado externamente	¿Cuando desarrollo del software es por outsourcing, se definen los detalles para proteger, supervisar y monitorear el desarrollo?	CUMPLE PARCIALMENTE	2
12.6.	**Gestion de las Vulnerabilidades**	**Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.**		
12.6.1	Control de las vulnerabilidades técnicas	¿Se obtiene información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso? ¿Se evaluar la exposición de la organización a dichas vulnerabilidades y se toman las acciones apropiadas para tratar los riesgos asociados?	NO CUMPLE	1
13..	**GESTIÓN DE INCIDENTES - MONITOREO**			
13.1.	**Reporte sobre los eventos y las debilidades de seguridad de la información**	**Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente**		
13.1.1	Reporte sobre los eventos de seguridad de la información	¿Existen procedimientos formales de reportes y respuesta a incidentes para identificar las acciones a ser tomadas frente a la recepción de un reporte de incidentes?	NO CUMPLE	1
13.1.2	Reporte sobre las debilidades en la seguridad	¿Son los usuarios requeridos observar y reportar todas las debilidades de seguridad observadas o sospechadas o amenazas a los sistemas o a los servicios?	NO CUMPLE	1
13.2.	**Gestión de los incidentes y las mejoras en la seguridad de la información**	**Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.**		
13.2.1	Responsabilidades y procedimientos	¿Se ha establecido las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?	NO CUMPLE	1
13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Existen implementados mecanismos para monitorear los tipos, los volúmenes, y los costos de incidentes y de malfuncionamientos?	NO CUMPLE	1
13.2.3	Recolección de evidencias	¿Existen definidos procedimientos para se debería recolectar, retener y presentar evidencia para cumplir las reglas de la evidencia establecidas en la jurisdicción pertinente?	NO CUMPLE	1

14..	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
14.1.	**Aspectos de seguridad de la información en la Gestión de la Continuidad de Negocios**	**Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.**		
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	¿Se ha desarrollado y mantenido un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización?	CUMPLE PARCIALMENTE	2
14.1.2	Continuidad del negocio y evaluación de riesgos	¿Se han identificado los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información?	CUMPLE PARCIALMENTE	2
14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	¿En el proceso del planeamiento de la continuidad del negocio ha incluido la identificación y el acuerdo de todas las responsabilidades y procedimientos de emergencia?	NO CUMPLE	1
14.1.4	Estructura para la planificación de la continuidad del negocio	¿Se mantiene un único marco (framework) del plan de la continuidad del negocio para asegurarse de que todos los niveles del plan son consistentes?	NO CUMPLE	1
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	¿Los planes de la continuidad del negocio se prueban regularmente para asegurarse de que son actuales y eficaces?	NO CUMPLE	1
15..	**CUMPLIMIENTO**	**CUMPLIMIENTO**		
15.1.	**Cumplimiento de los requisitos legales**	**Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad**		
15.1.1	Identificación de la legislación aplicable	¿Todos los requisitos estatutarios, reguladores, y contractuales relevantes son específicamente definidos y se documentan para cada sistema de información?	NO CUMPLE	1
15.1.2	Derechos de propiedad intelectual (DPI)	¿Hay conformidad con restricciones legales en el uso de material con copyright asegurándose que solamente el software se desarrolló en la organización, o licenciado o proporcionado por el desarrollador a la organización, es utilizado?	NO CUMPLE	1
15.1.3	Protección de los registros de la organización	¿Los registros de la organización importantes se mantienen con seguridad para dar cumplimiento a requisitos estatutarios, así como para apoyar actividades económicas esenciales?	NO CUMPLE	1
15.1.4	Protección de los datos y privacidad de la información personal	¿Las aplicaciones que procesan datos personales dan cumplimiento a la legislación aplicable de la protección de los datos?	NO CUMPLE	1
15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	¿Las instalaciones de IT se utilizan solamente para los propósitos del negocio?	NO CUMPLE	1
15.1.6	Reglamentación de los controles criptográficos	¿El asesoramiento jurídico se ha buscado en la conformidad de la organización con leyes nacionales e internacionales sobre controles criptográficos?	NO CUMPLE	1
15.2.	**Cumplimiento de las Políticas y las normas de seguridad y cumplimiento técnico**	**Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización**		
15.2.1	Cumplimiento con las políticas y las normas de seguridad	¿Todas las áreas dentro de la organización son consideradas para revisiones con regularidad que asegure conformidad con políticas y estándares de la seguridad?	NO CUMPLE	1
15.2.2	Verificación del cumplimiento técnico	¿Las instalaciones de IT se comprueban regularmente para saber si hay conformidad con los estándares seguridad implementados?	NO CUMPLE	1
15.3.	**Consideraciones de la Auditoría de los sistemas de Información**	**Maximizar la eficacia de los procesos de auditoría de los sistemas de información y maximizar su interferencia**		
15.3.1	Controles de auditoría de los sistemas de información	¿Las auditorias y las actividades que implican chequeos en sistemas operacionales se planean y se arreglan cuidadosamente?	CUMPLE PARCIALMENTE	2
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	¿El acceso a las herramientas de auditoria del sistema es controlado?	NO CUMPLE	1
				187
		GRADO O NIVEL DE CUMPLIMIENTO NORMA ISO27001		**44%**