RESUMEN – TRABAJO DE GRADO

AUTORES	**KERLY YULIETH CLARO LUNA** **EDGAR LEÓN LÓPEZ**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
DIRECTOR	**YESICA MARÍA PÉREZ PÉREZ**
TÍTULO DE LA TESIS	**EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACION EN EL CENTRO DE CÓMPUTO DE LA EMPRESA EL APOSTADOR**

RESUMEN
(70 palabras aproximadamente)

.LA PRESENTE INVESTIGACION DENOMINADA EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACION EN EL CENTRO DE CÓMPUTO DE LA EMPRESA EL APOSTADOR PERMITIO PROVEER LAS CONDICIONES DE GOBERNABILIDAD, OPORTUNIDAD Y VIABILIDAD NECESARIAS PARA QUE LA SEGURIDAD DE LA INFORMACIÓN APOYE Y EXTIENDA LOS OBJETIVO ESTRATÉGICOS DEL NEGOCIO, MEDIANTE LA PROTECCIÓN Y ASEGURAMIENTO DE SU INFORMACIÓN QUE ES FUNDAMENTAL PARA GARANTIZAR LA DEBIDA GESTIÓN FINANCIERA, ADMINISTRATIVA Y OPERATIVA DE LA ENTIDAD, Y CON ELLO ASEGURAR EL CUMPLIMIENTO DE SU MISIÓN.

CARACTERÍSTICAS

PÁGINAS: 78	PLANOS:	ILUSTRACIONES:	CD-ROM:

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACION EN EL CENTRO DE CÓMPUTO DE LA EMPRESA EL APOSTADOR

AUTORES

KERLY YULIETH CLARO LUNA

EDGAR LEÓN LÓPEZ

Trabajo de grado presentado para obtener el título de especialista en Auditoria de Sistemas

DIRECTOR

YESICA MARÍA PÉREZ PÉREZ

Magister en Direccionamiento Estratégico en Telecomunicaciones (C)

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS

Ocaña, Colombia **Mayo 2017**

A Dios.
Por permitirme lograr esta meta sin desfallecer, además de su infinita bondad y amor.

A mi esposa e hijos.
A mi esposa, por su constante motivación, apoyo incondicional, sus consejos y sus valores, que me alentaron en todo momento a culminar esta meta.

A mis hijos, que aceptaron mi ausencia debido a mis continuos viajes, con comprensión y sin reproches.

A mis padres.
Porque gracias a sus buenos ejemplos y enseñanzas he logrado salir adelante.

A mi amiga Kerly
Mi compañera de proyecto. Por su compañía durante los continuos viajes, por su apoyo en la realización de trabajos y porque siempre fue mi guía.

Att: Edgar

A Dios.

Por darme la vida y la fortaleza para aprender con amor, que todo es posible, si crees y tienes fe.

A mis padres y hermanos.

A mis padres, porque con su unión y nobleza, me enseñaron el mejor de los valores, "el amor", constante, incondicional, luchador y duradero. A mis hermanos, por sus cuidados, buenos ejemplos y consejos.

A mi esposo e hija.

A mi esposo, por su comprensión, apoyo y motivación. Gracias mi amor, porque tu gran confianza en mí, me impulsó a lograr esta meta. A mi hija, mi mayor motivador, quien comprendió poco a poco, las razones de mis constantes ausencias. Hija, fuiste la mejor compañía, cuando fue posible llevarte conmigo a Ocaña. Por ti y para ti todos mis logros.

A mi amigo Edgar

Mi compañero inseparable en los viajes y en las aulas de clases. Disfrutamos juntos cada instante en la Universidad. Te admiro, por tu tenacidad para salir adelante. Doy gracias a Dios porque te puso a mi lado para vivir y lograr juntos está meta, admiro tu gran tenacidad para salir adelante, me demostraste muchas veces, que no existen limitaciones cuando se tiene la fuerza necesaria para superar cada obstáculo. Eres un gran ser humano y un gran amigo.

A mi amiga Magda Milena

Al enterarme de tu partida al cielo, supe que no podía desfallecer y que la meta debía ser cumplida. Amiga, tus palabras hicieron eco en mí, "sigue, sigue, tu eres capaz". Para ti este logro, mi gorda.

Att: Kerly

Índice

Pág

.

Lista de Tablas

Lista de Ilustraciones

Lista de Aprendices

Introducción

Actualmente las organizaciones mantienen una estrecha dependencia con las computadoras, tecnología y controles que se emplean en los centros de procesamiento de datos, los cuales apoyan la labor administrativa y la toma de decisiones en la medida que la capacidad de respuesta de procesamiento de la información sea más segura.

La información, considerada como un activo importante dentro de las empresas, requiere cada vez más de una protección adecuada, especialmente cuando la dinámica de los negocios hace que diferentes empresas permanezcan interconectadas, compartiendo información entre sí, lo que expone a dicha información a un gran número de vulnerabilidades y amenazas.

Por lo anterior, es fundamental concientizar a las organizaciones sobre la necesidad e importancia de implementar un conjunto apropiado de controles de seguridad de la información que minimicen la ocurrencia de riesgos, aseguren la continuidad del negocio y maximicen el retorno de inversiones y oportunidades del negocio.

Capítulo 1. Evaluación de la seguridad de la información en el Centro de Cómputo de la empresa EL APOSTADOR

1.1 Planteamiento del Problema

EL APOSTADOR, es una empresa del sector de los juegos de suerte y azar que presta sus servicios a lo largo y ancho del departamento Norte de Santander, a través de más de 400 puntos de venta, con locales debidamente identificados y estandarizados.

En sus inicios, la empresa EL APOSTADOR, solo ofrecía una modalidad de juego autorizado conocido como CHANCE. Sin embargo, con el pasar del tiempo y en pro de generar un mejor servicio a la ciudadanía y obtener mayores ganancias, la empresa ha venido realizando convenios con otras empresas para ofrecer nuevos productos. En consecuencia, en este momento la empresa EL APOSTADOR, ofrece a sus clientes no sólo el Chance tradicional en sus diversas modalidades, sino también recaudo de facturas de servicios públicos, recaudo de expensas de condominios, recaudos de facturas de celulares, Giros a cualquier ciudad del país, recargas a celulares, Apuestas deportivas, etc.

Teniendo en cuenta que todo lo anterior involucra un flujo de efectivo con sus respectivos registros digitales, hace obligatorio que la empresa EL APOSTADOR, cuente con herramientas que brinden garantías y confianza tanto a sus clientes, como a las entidades que la vigilan y regulan.

Para brindar dicha tranquilidad, la empresa cuenta con un Centro de Cómputo propio, ubicado dentro de sus instalaciones, para salvaguardar y administrar la información, de la cual debe garantizar su confiabilidad, integridad y disponibilidad.

1.2. Formulación del Problema

Los conocimientos adquiridos durante el programa de la Especialización en Auditoría de Sistemas de la Universidad Francisco de Paula Santander Ocaña, permiten realizar una evaluación a la seguridad de la información del Centro de Cómputo de la Empresa el Apostador, mediante el uso de herramientas de auditoría basadas en los controles de seguridad de la NTC ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942. Una vez realizada la evaluación a la seguridad de la información, se dará respuesta al siguiente interrogante:

¿La información guardada en el Centro de Cómputo de la empresa El Apostador, mantiene la Integridad, confiabilidad y disponibilidad de acuerdo a los estándares dados por la NTC ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942?

1.3. Objetivos

1.3.1. Objetivo General

Verificar si los controles de seguridad existentes en el Centro de Cómputo de la Empresa El Apostador, mitigan la ocurrencia de afectaciones a la integridad, confidencialidad y disponibilidad de la información.

1.3.2. Objetivos Específicos

Realizar un estudio preliminar a los controles existentes en el Centro de Cómputo para la identificación de posibles riesgos.

Evaluar los controles de seguridad del Centro de Cómputo con base en los criterios establecidos en la Norma Técnica Colombiana ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942, para conocer el nivel de implementación de los mismos.

Elaborar un informe final de auditoría con las oportunidades de mejora y las recomendaciones necesarias para optimizar la seguridad en el Centro de Datos de la empresa El Apostador.

A continuación, la **tabla 1** presenta un resumen de las diferentes actividades propuestas, de acuerdo a los objetivos planteados y los resultados esperados.

Tabla 1.

Actividades a realizar para el logro de objetivos

Objetivos Específicos	Actividades	Resultados
Realizar un estudio preliminar a los controles existentes en el Centro de Cómputo para la identificación de posibles riesgos	1. Estudio de archivos permanentes (Procedimientos, instructivos, manuales, guías, etc.). 2. Elaboración de Encuesta y realización de entrevista. 3. Elaboración y aplicación de lista de chequeo	* Estudio de la Empresa y Área de Sistemas. * Encuesta diligenciada * Lista de chequeo diligenciada * Matriz de riesgos * Programa de auditoría * Definición de pruebas

Evaluar los controles de seguridad del Centro de Cómputo con base a los criterios establecidos en la Norma Técnica Colombiana ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942, para conocer el nivel de implementación de los mismos.	1. Realizar un análisis de diferencias GAP que muestre el nivel de implementación de los controles de la NTC ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942 2. Documentar los Papeles de trabajo de las pruebas	* Herramienta de análisis Gap * Papeles de trabajo
Elaborar un informe final de auditoría con las oportunidades de mejora y las recomendaciones necesarias para optimizar la seguridad en el Centro de Datos de la empresa El Apostador.	1. Elaborar informe o dictamen de auditoría	*Informe de auditoría

Nota fuente: Autores del Proyecto

1.4. Justificación

El presente proyecto, se realiza con el fin de aplicar el conocimiento y las capacidades para enfrentar un problema y lograr la satisfacción de las necesidades y requerimientos, ofreciendo un documento de análisis y diagnóstico a los componentes del SGSI que apliquen al Centro de Cómputo en el área de sistemas de la Empresa el Apostador, que garantice la confidencialidad, integridad y disponibilidad en el manejo de la información, según la normatividad vigente.

El resultado de la evaluación mediante un informe de auditoría que verifique tanto el cumplimiento de las normas como la identificación de las falencias en la seguridad de la información que puedan existir en el Centro de Cómputo de la Empresa el Apostador, le permitirá a la alta dirección definir e implementar medidas correctivas que ayuden a mitigar las amenazas y vulnerabilidades que allí se encuentren. Así mismo, ayudará a conocer el estado de los controles existentes y evaluar la pertinencia de cada uno de ellos, para determinar su

efectividad tal como están implementados o si deben ser mejorados, reemplazados o eliminados, con el fin de alcanzar los niveles de seguridad deseados.

La evaluación de la seguridad de la información del Centro de Cómputo El Apostador, basado en un modelo de buenas prácticas de seguridad conocido a nivel mundial, como es la norma ISO/IEC 27001:2013, proveerá las condiciones de gobernabilidad, oportunidad y viabilidad necesarias para que la seguridad de la información apoye y extienda los objetivo estratégicos del negocio, mediante la protección y aseguramiento de su información que es fundamental para garantizar la debida gestión financiera, administrativa y operativa de la entidad, y con ello asegurar el cumplimiento de su Misión.

Un Sistema de Gestión de Seguridad de la Información, demuestra el compromiso de la organización hacia la Seguridad de la Información y provee los elementos requeridos para gestionar de manera eficiente los riesgos que puedan atentar con la seguridad de su información, lo cual, brindará la confianza a la alta dirección, a sus clientes y a sus asociados, aspecto fundamental para el crecimiento y la sostenibilidad de la entidad.

Establecer un Sistema de Gestión de Seguridad de la Información, significa que la Empresa el Apostador enfocará sus procesos basados en el ciclo de Deming o el ciclo de mejora continua, consistente en Planificar-Hacer-Verificar-Actuar (PHVA), conocido con las siglas en inglés PDCA. La norma ISO-27001 presenta relación con otras normas que constituyen el modelo de gobierno y la gestión de las TIC.

La implementación de los Sistemas de Gestión hace que se gestione la calidad y la seguridad de los servicios de Tecnologías de la Información y la Comunicación (TIC), con lo que se consigue disminuir los riesgos en torno a la Seguridad de la Información y aumentar la seguridad de las TIC.

La norma ISO 27001, es el framework más utilizado dentro del marco de la ciberseguridad, que según resultados de la Encuesta Global de Seguridad de la Información 2015 de PwC, ubicaría a la entidad en el 14% de las organizaciones a nivel de América del Sur que son pioneras en adoptar este tipo de modelos de seguridad. (PWC, 2016).

1.5. Hipótesis

La información guardada en el Centro de Cómputo de la empresa El Apostador, mantiene la Integridad, confiabilidad y disponibilidad de acuerdo a los estándares dados por la NTC ISO/IEC 27001.

El Centro de Cómputo de la Empresa El Apostador, cumple con los mínimos estándares de seguridad física definidos por la NTC ISO/IEC 27001 y el estándar ANSI/TIA/EIA-942.

Es posible que una vez aplicadas las técnicas de auditoría para el estudio y validación de información, como la observación, encuestas, muestras y pruebas sustantivas, la seguridad de la información en el Centro de Cómputo el Apostador presente un nivel de riesgo alto, al entenderse que el control proporciona una seguridad razonable pero no absoluta, lo que requiere

de una evaluación constante y un seguimiento periódico de los controles existentes, que permita la optimización de los mismos, y la mitigación del impacto de los riesgos, los cuales son dinámicos y se robustecen día a día.

1.6. Delimitaciones

La Empresa el Apostador es consciente que mantener un Centro de Cómputo con una seguridad absoluta, es una labor difícil, por no decir imposible, teniendo en cuenta las diferentes amenazas y vulnerabilidades inherentes a las que se expone la información almacenada y procesada en los servidores y transferida a los diferentes puntos de la red. La Evaluación de la seguridad de la información en el Centro de Cómputo de la empresa EL APOSTADOR, permitirá que la Alta Dirección conozca el estado o nivel de madurez de las prácticas aplicadas del Sistema de Gestión de Seguridad de Información, con el fin de brindar una mayor confianza a sus asociados y clientes, en la operación de la información de los juegos de suerte y azar. Los alcances establecidos para la evaluación están definidos de la siguiente manera:

1.6.1. Geográficas.

A pesar que la empresa El Apostador cuenta con múltiples puntos de venta distribuidos por todo el departamento Norte de Santander, el proyecto se realizará en las instalaciones de la oficina principal, ubicada en la Ciudad de Cúcuta.

1.6.2. Conceptuales.

El desarrollo del proyecto requiere de la aplicación teórica en conceptos relacionados con: Centro de Cómputo, Información, Seguridad Física, Seguridad lógica, Auditoria, Controles,

Vulnerabilidad, Amenaza y Riesgo.

1.6.3. Operativas.

El proyecto se realizará basándose en las buenas prácticas de auditoría, norma ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942 aplicables a la evaluación de un Centro de Cómputo.

1.6.4. Temporales.

La elaboración del proyecto, se estima una duración máxima de 9 meses, cuya ejecución se cuenta a partir de la fecha de aprobación del anteproyecto.

La evaluación al Centro de Cómputo de la Empresa el Apostador, se realizará a los controles que apliquen a la seguridad de la información del Centro de Cómputo, las conclusiones, observaciones y recomendaciones se presentarán al personal directivo para la definición de acciones de mejora.

Capítulo 2. Marco Referencial

2.1. Marco Histórico

2.1.1 Antecedentes

Para entender la relevancia que ha tenido la seguridad de la información en los Centros de Cómputo, debe hacerse un recorrido histórico a los diversos avances tecnológicos que se han implementado.

En los años 60´s las empresas comienzan a utilizar macro computadoras para el procesamiento de sus datos, convirtiéndose esto en una herramienta primordial a nivel de automatización. La empresa IBM hace un importante aporte con la creación del IBM 360, cuya fabricación electrónica está basada en circuitos integrados y su manejo es por medio de los lenguajes de control de sistemas operativos. Con el IBM 360, se dio inicio a la Tercera Generación de computadoras y también fue, el IBM 360, el primer computador atacado por un virus informático.

En los años 70’s no había capacidad para soportar aplicaciones ni nuevos lenguajes de programación, y el desarrollo parece estancarse. Surge el uso de computadoras más pequeñas, pero igualmente potentes y se crean centrales de trabajo, es entonces que aparecen las computadoras de tamaño mediano, o minicomputadoras que no son tan costosas como las grandes (mainframes), pero disponen de gran capacidad de procesamiento. Algunas minicomputadoras fueron las siguientes: la PDP-8 y la PDP -11 de Digital Equipment Corporation, también aparecen las microcomputadoras, un gran adelanto de la microelectrónica.

En los años 80’s surgen algunos profesionales en informática y con ello la construcción de Centros de Cómputo con personal más capacitado. Se reducen costos al usar computadoras más pequeñas a diferencia de las grandes que requerían de instalaciones costosas y especiales, pero aun así la presencia del mainframe era ya ineludible en prácticamente todas las esferas de control gubernamental, militar y de la gran industria, encontramos aquí las enormes computadoras de las series CDC, CRAY, Hitachi o IBM, las cuales eran capaces de atender a varios cientos de millones de operaciones por segundo.

En los 90’s aparecen técnicas modernas de comunicación vía telefónica, microondas y satélite que permitieron la incorporación de nuevas técnicas de manejo de datos (BD’s, Teleproceso, Software) lo que inicia con los Sistemas Distribuidos y Centros de Cómputo intercomunicados.

En el año 2000, las técnicas creadas en los 90’s hicieron que aumentaran las posibilidades de servicios en línea (tiempo real). Esto trajo consigo la Administración de los Centros de Cómputo y la Administración del Área de Informática. Es en el 2005, que el concepto de Centro de Cómputo cambia por Área de Informática, destacándola a nivel de dirección dentro de cualquier organización.

En abril de 2005, la American National Standard Institute, creó el estándar ANSI/TIA 942, que presenta una clasificación de cuatro niveles llamados TIER. Esta clasificación está basada en el nivel de disponibilidad de los servicios tecnológicos que conforman el Centro de Datos.

De acuerdo al Uptime Institute, entidad que expide certificaciones TIER alrededor del mundo, en Colombia sólo hay 9 Centros de Datos certificados, como se muestra en la **Tabla 2.** (Uptime Institute)

Tabla 2.

Centro de Datos TIER en Colombia

Empresa	Nombre del centro de datos	Ubicación	Certificación Tier
Cotel SA	Data Ceneter BT Naos	Bogotá	Tier IV
GTD FLYWAN	El Poblado, Phase 1	Medellín	Tier III
Empresa de Telecomunicaciones de Bogota S.A. E.S.P.	Alma Data Center ETB	Bogotá	Tier III
GTD FLYWAN	El Poblado	Medellín	Tier III
Desarrolladora de Zonas Francas S.A.	ZF Towers DC16A 2nd Flr – Telefonica	Bogotá	Tier III
Desarrolladora de Zonas Francas S.A.	ZF Towers DC16A 3rd Flr - DZF	Bogotá	Tier III
Desarrolladora de Zonas Francas S.A.	ZF Towers DC38 2nd Flr - BT Nimbus	Bogotá	Tier III
Desarrolladora de Zonas Francas S.A.	ZF Towers DC38 3rd Flr - Telefonica	Bogotá	Tier III
Level 3 Colombia S.A.	Colombia XV	Bogotá	Tier III

Nota Fuente: Según Uptime Institute, en colombia sólo hay 9 Centros de Datos Certificados.

De acuerdo al periódico EL TIEMPO, en su edición del 5 de enero de 2015, Colombia es el cuarto país de América Latina, después de Perú, Chile y Argentina, con mayor crecimiento de inversión en Centros de Datos. Además, la nota señala que Colombia ha alcanzado la 5 posición entre los países con mayor cantidad de metros cuadrados destinados a Centros de Datos.

En razón a estos avances tecnológicos, se hace necesario evaluar los controles con los que cuentan las empresas e implementar un Sistema de Gestión de Seguridad de la Información que cumpla con los requisitos básicos de confiabilidad, integridad y disponibilidad para la

protección de la información contra una gran variedad de amenazas, con el fin de asegurar la continuidad del negocio, minimizar los riesgos y maximizar el retorno de inversiones.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. De ahí la importancia que los controles sean establecidos, implementados, monitoreados, revisados y mejorados, para asegurar que se cumplen los objetivos específicos de seguridad y del negocio de la organización.

La Empresa El Apostador dedicada a la operación de apuestas permanentes, implementó en el año 2013, un Sistema de Gestión de Seguridad de la Información ISO 27001:2005, mediante un conjunto de políticas de administración de la información, para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de la información minimizando a la vez los riesgos de seguridad de la información, sin embargo, las practicas implementadas del Sistema de Gestión de Seguridad de la Información ISO 27001:2005, no han sido revisadas, y hoy día, la Alta Dirección ha manifestado su interés en conocer el nivel de madurez en la gestión de seguridad de la información, razón por la cual, este estudio se enmarca en la evaluación de los controles de seguridad existentes en el Centro de Cómputo de la Empresa el Apostador bajo la NTC ISO/IEC 27001:2013.

2.2 Marco Conceptual

Centro de Cómputo. Conocido también como Centro de Procesamiento de Datos (CPD), que se entiendo como aquella ubicación exclusiva donde las organizaciones concentran y operan las infraestructuras de tecnología de Información de Computador para el procesamiento y almacenamiento de su información.

El diseño de un Centro de Datos debe contar con algunas características especiales en su infraestructura, tales como: Falsos suelos y falsos techos, Cableado de red y teléfono, Doble cableado eléctrico, Generadores y cuadros de distribución eléctrica, Alarmas, control de temperatura y humedad con avisos , Facilidad de acceso (pues hay que meter en él aires acondicionados pesados, muebles de servidores grandes, etc.), Cerraduras electromagnéticas, Torniquetes, Cámaras de seguridad, Detectores de movimiento, Tarjetas de identificación.

Los centros de cómputo pueden ubicarse en las propias instalaciones de la empresa o bien en un proveedor externo.

Información. Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Seguridad física. La seguridad física de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware.

Este tipo de seguridad se enfoca a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el sistema. Algunas amenazas que se prevén son: Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales, como son: Amenazas ocasionadas por el hombre como robos o sabotajes, Disturbios internos o externos deliberados.

Seguridad Lógica. La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permita acceder a ellos a quienes tengan autorización para hacerlo.

Algunos de los objetivos de la seguridad lógica pueden ser: (i). Restringir el acceso a programas y archivos, (ii). Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan, (iii) Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto, (iv) Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada, (v) Que la información recibida sea la misma que ha sido transmitida.

Auditoría de Sistemas. Consiste en la verificación de controles en el procesamiento de información, desarrollo de sistemas e instalación para evaluar su efectividad y presentar recomendaciones a la alta dirección. (Naranjo, 2009)

Controles. Es un mecanismo preventivo y correctivo adoptado por la administración de una dependencia o entidad que permite la oportuna detección y corrección de desviaciones, ineficiencias o incongruencias en el curso de la formulación, instrumentación, ejecución y evaluación de las acciones con el propósito de procurar el cumplimiento de la normatividad que las rige, las estrategias, políticas, objetivos, metas y asignación de recursos. (Definicion Org, s.f)

Vulnerabilidad. Es la debilidad de control que facilita las afectaciones y la materialización del riesgo. En informática, la vulnerabilidad hace referencia a una debilidad en un sistema, que permite a un atacante violar la confiabilidad, integridad o disponibilidad de la información. La vulnerabilidad en la mayoría de los casos es producto de fallas en el diseño del sistema.

Amenaza. Es un evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, proceso, proyecto, cosa y personas. En términos de seguridad de la información, las amenazas pueden afectar de manera negativa la confidencialidad, integridad, disponibilidad y autenticidad de los datos e información, lo que tendría un impacto a los recursos financieros de las empresas.

Riesgo. Representa la posibilidad de ocurrencia de un evento que pueda desviar el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos. Las empresas deben evaluar los riesgos periódicamente debido a que sus cambios son dinámicos, esto les permite identificar los riesgos, medirlos, valorar controles, mitigar los riesgos, monitorear el control y valorar su desempeño, marcando así un ciclo para la administración del riesgo.

2.3 Marco Contextual

En 1982 el gobierno a través de la primera ley de ese año, legaliza el juego de Chance o apuestas permanentes, es así que otorgó la primera licencia en el país para la explotación de este tipo de juego, siendo beneficiaria la Empresa El Apostador.

Misión: Comercializar juegos de suerte y azar, generando recursos a la salud en el departamento Norte de Santander, recaudo y pago de servicios; contribuyendo al progreso de la empresa y la comunidad, teniendo como principios la inversión en responsabilidad social empresarial, la eficacia, seguridad, transparencia, cumplimiento, innovación y calidad humana; apoyados en una infraestructura tecnológica propia y un sistema de gestión integral que nos permita un mejoramiento continuo.

Visión: Ser conocidos en el 2018 como empresa generadora de nuevos productos, servicios y como aliados estratégicos en el aprovechamiento de nuestra infraestructura tecnológica, con personal altamente calificado para superar las expectativas de los clientes a nivel nacional. Manteniendo el liderazgo en la comercialización de juegos de suerte y azar.

Objetivos Gestión Integral:

Mantener, revisar y probar medidas necesarias para garantizar el correcto funcionamiento de los Planes de Continuidad del Negocio establecidos por la organización.

Garantizar que los procesos críticos son recuperados dentro de los márgenes de tiempo, requeridos en los Planes de Continuidad de Negocio.

Aumentar la satisfacción y expectativas de nuestros clientes.

Incrementar las alianzas estratégicas para obtención de nuevos productos y/o servicios.

Mejorar la eficacia y eficiencia de los procesos.

Promover la formación que fortalezca las competencias del talento humano conforme al

sistema de gestión integral.

Establecer controles que prevengan el riesgo del lavado de activos y de la financiación del terrorismo al interior de la organización.

Mitigar la mayoría de riesgos identificados para garantizar la disponibilidad, integridad y confidencialidad de los activos de la información de la empresa.

2.4. Marco Teórico

La evolución permanente de las tecnologías y las constantes amenazas que hoy día atentan contra la seguridad de la información, conducen a las organizaciones a contar con un modelo o Sistema de Gestión de Seguridad de la Información basado en estándares de seguridad reconocidos a nivel mundial, con el propósito de establecer y mantener un gobierno de seguridad alineado a las necesidades y objetivos estratégicos del negocio, compuesto por una organización de roles y responsabilidades, así como un conjunto coherente de políticas, procesos y procedimientos, que permiten gestionar de manera adecuada, los riesgos que puedan afectar la integridad, confidencialidad, disponibilidad, trazabilidad y no repudio de la seguridad de la información.

El trabajo de Evaluación de la Seguridad de Información del Centro de Cómputo de la Empresa el Apostador, se basa en la normatividad vigente planteada en la ISO/IEC 27001:2013, que conduce a un análisis de los controles existentes mediante una metodología estructurada y una adecuada valoración y tratamiento de los riesgos de seguridad, con el objetivo de conocer el estado real de la seguridad de los activos de información, a través de los cuales, se gestiona la

información del negocio, permitiendo no solo identificar y valorar las amenazas que puedan comprometer la seguridad de la información, sino que también determinar los mecanismos y medidas de seguridad a implementar para minimizar el impacto en caso de las posibles pérdidas de confiabilidad, integridad y disponibilidad de la información. (ICONTEC, 2013)

Los conceptos fundamentales, específicamente en lo que tiene que ver con el sistema de gestión de seguridad de la información a los controles del Centro de Cómputo de la Empresa el Apostador, según la norma ISO/IEC 27001:2013 y para Colombia la Ley 1273/2009, están basados en la preservación de su confidencialidad, integridad y disponibilidad:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

2.4.1 Estándares Internacionales

Estándar ISO 27001.

Norma internacional emitida por la Organización Internacional de Normalización (ISO), que describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013, su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005. (Kosutic, 2015)

Estándar oficial. Título completo es BS 7799-2:2005 (ISO/IEC 27001:2005) (www.iso27000.es). El conjunto de estándares que aportan información de la familia ISO-2700x son:

ISO/IEC 27002- Mejores prácticas en la gestión de seguridad de la información. Brinda recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. (ISO/IEC 27002, 2013)

ISO/IEC 27003: ISMS Guía para la Implementación. (ISO/IEC 27003, 2010)

ISO/IEC 27004: Medición de la Seguridad de la Información. (ISO/ IEC 27004, 2009)

ISO/IEC 27005: Gestión de riesgos de la Seguridad la Información. (ISO/ IEC 27005, 2001)

ANSI/TIA/EIA-606-A: Estándar de Administración para la infraestructura de Telecomunicaciones de Edificios Comerciales.

ANSI/TIA/EIA-758-A Norma Cliente-propietario de Cableado de Planta Externa de telecomunicaciones.

EIA/TIA 607 Requerimientos para Telecomunicaciones de puestas a tierra y para distribuir los seriales a tierra a través de un edificio.

TIA/ANSI. Organizaciones de Estados Unidos que coordinan la creación y publicación conjunta de estándares.

TIA/EIA 568-A: En octubre de 1995, el modelo 568 fue corregido por el TIA/EIA 568-A que absorbió entre otras modificaciones los boletines TSB-36 y TSB-40.

Esta norma, regula todo lo concerniente a sistemas de cableado estructurado para edificios

comerciales.

EIA/TIA 569-A: Esta norma se creó en 1990 como el resultado de un esfuerzo conjunto de la Asociación Canadiense de Normar (CSA) y Asociación de las Industrias Electrónicas (EIA). La versión actual es de febrero de 1998. La norma indica los siguientes elementos para espacios de telecomunicaciones en construcciones: Recorridos horizontales, armarios de telecomunicaciones, sala de equipos, estación de trabajo y sala de entrada de servicios.

ANSI/TIA/EIA-942: Estándar desarrollado por la Telecomunication Industry Association (TIA) para integrar criterios en el diseño de data center. Considera la estructura de un data center en su conjunto y contiene requerimientos sobre infraestructura de cableado, instalación, accesorios de montaje y la identificación de los sitios para el tendido de cables. Además, se centra en el diseño de la red, características arquitectónicas de los edificios, condiciones para la energía, la iluminación, las condiciones climáticas, la seguridad contra incendios y protección contra la humedad, entre otros.

ANSI/TIA/EIA-607: Puesta a tierra y requisitos para telecomunicaciones de la vinculación

en edificios comerciales.

IEEE: Instituto de ingenieros electricistas y electrónicos.

RETIE: Reglamento Técnico de Instalaciones Eléctricas.

NFPA 70B. Practica recomendada para mantenimientos de equipos electrónicos

NFPA-72. Código de alarmas contra incendios.

NFPA-75. Estándar para la protección de equipos de cómputo.

NFPA 731. Instalación de Sistemas de Seguridad en establecimientos.

2.5. Marco Legal

Ley 603 de 2000.

Por medio de la cual se regula el tipo de software que usan las empresas, con el fin de proteger la propiedad intelectual y evitar el incremento de la piratería en el país.

Ley 1581 de 2012 y Decreto 1377 de 2013.

La cual trata el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política.

Ley 643 de 2001.

Por la cual se fija el régimen propio del monopolio rentístico de juegos de suerte y azar.

SIPLAFT. Sistema de Prevención y Control de Lavado de Activos y Financiación del Terrorismo.

Contempla un mecanismo para prevenir la financiación del terrorismo, delito tipificado en el artículo 345 del Código Penal, que advierte: El que directa o indirectamente provea, recolecte, entregue, reciba, administre, aporte, custodie o guarde fondos, bienes o recursos, o realice cualquier otro acto que promueva, organice, apoye, mantenga, financie o sostenga

económicamente a grupos de delincuencia organizada, grupos armados al margen de la ley o a sus integrantes, o a grupos terroristas nacionales o extranjeros, o a terroristas nacionales o extranjeros, o a actividades terroristas, incurrirá en prisión de trece (13) a veintidós (22) años y multa de mil trescientos (1.300) a quince mil (15.000) salarios mínimos legales mensuales vigentes. (Congreso de la Republica , 2000)

EL SIPLAFT, También permite detectar el lavado de Activos, delito tipificado en el artículo 323 del Código Penal, que dice: El que adquiera, resguarde, invierta, transporte, transforme, almacene, conserve, custodie o administre bienes que tengan su origen mediato o inmediato en actividades de tráfico de migrantes, trata de personas, extorsión enriquecimiento ilícito, secuestro extorsivo, rebelión, tráfico de armas, tráfico de menores de edad, financiación del terrorismo y administración de recursos relacionados con actividades terroristas, tráfico de drogas tóxicas, estupefacientes o sustancias sicotrópicas, delitos contra el sistema financiero, delitos contra la administración pública, o vinculados con el producto de delitos ejecutados bajo concierto para delinquir, o les dé a los bienes provenientes de dichas actividades apariencia de legalidad o los legalice, oculte o encubra la verdadera naturaleza, origen, ubicación, destino, movimiento o derecho sobre tales bienes o realice cualquier otro acto para ocultar o encubrir su origen ilícito, incurrirá por esa sola conducta, en prisión de diez (10) a treinta (30) años y multa de seiscientos cincuenta (650) a cincuenta mil (50.000) salarios mínimos legales vigentes. (Congreso de la Republica, 2000)

RETIE – Reglamento Técnico de Instalaciones Eléctricas.

Es el Reglamento Técnico de Instalaciones Eléctricas y fue creado por el Decreto 18039 de 2004, del Ministerio de Minas y Energía. El objetivo de este reglamento es establecer medidas

que garanticen la seguridad de las personas, vida animal y vegetal y la preservación del medio ambiente, previniendo, minimizando o eliminado los riesgos de origen eléctrico.

El Ministerio de Minas y Energía, ha realizado correcciones al reglamento por medio de las Resoluciones 90907 de 2013, 90795 de 2014 y 40492 de 2015 donde se aclaran algunos artículos del Anexo General del RETIE de la Resolución 90708 de 2013.

Ley 1273 Del 2009

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (Ministerior de las TIC, 2009)Dicha ley decreta:

CAPITULO I:

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos:

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático

Artículo 269B: **Obstaculización ilegítima de sistema informático o red de telecomunicación**. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático.

Artículo 269D: Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Artículo 269F: **Violación de datos personales**. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Artículo 269G: **Suplantación de sitios web para capturar datos personales**. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

CAPITULO II:

De los atentados informáticos y otras infracciones

Artículo 269I: **Hurto por medios informáticos y semejantes**. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante.

Artículo 269J: **Transferencia no consentida de Activos**. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no

consentida de cualquier activo en perjuicio de un tercero.

Capítulo 3. Diseño Metodológico

3.1 Tipo de Investigación

En este proyecto se utilizará la investigación descriptiva o de diagnóstico, tipo cuantitativa. Su objetivo consiste en conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son solo tabuladores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

3.2 Población y Muestra

La población objeto de estudio que se tendrá en cuenta para la realización de esta investigación está conformado por todo el personal que labora en el Área de Sistemas, los cuales no superan los 5 profesionales, por lo tanto, la población es igual a la muestra.

En la **tabla 3** se muestra el número de la población a estudiar.

Tabla 3.

Población a estudiar

Cargo personal del Área de Sistemas	Cantidad de personas
Jefe de Sistemas	1
DBA	1
Profesionales	3

Nota Fuente: Autores del Proyecto

3.3 Técnicas de Recolección de la Información

3.3.1 Técnicas Primarias.

Entre las metodologías internas se tiene la observación, estudio de los archivos permanentes, entrevistas, listas de chequeo, cuestionarios, herramientas de evaluación y la realización de pruebas sustantivas.

3.3.2 Técnicas Secundarias.

Resultados de auditorías de los entes de vigilancia.

Capítulo 4. Administración del proyecto

4.1 Recurso Humano.

4.1.1 Proponentes

LEON LOPEZ, Edgar, y, CLARO LUNA, Kerly Yulieth. Estudiantes de la Especialización en Auditoría de Sistemas de la Universidad Francisco de Paula Santander Ocaña.

4.1.2 Director

PÉREZ PÉREZ, Yesica María. Ingeniera de Sistemas, Especialista en Auditoria de Sistemas y Magister en Direccionamiento Estratégico en Telecomunicaciones (C).

4.2 Recursos Institucionales

Los recursos de carácter físico e institucional para el desarrollo del proyecto son:

Empresa El Apostador, de la ciudad de Cúcuta, Norte de Santander.

El servicio de biblioteca de la Universidad Francisco de Paula Santander Ocaña.

4.3 Recursos Financieros

4.3.1 Ingresos.

Los ingresos contemplados para la realización del proyecto son de $3'000.000 aportados por los autores del mismo.

4.3.2 Egresos

Los gastos que se tiene previstos para la realización del presente trabajo son $3’000.000, los cuales se distribuyen como se muestra en las **Tablas 4 y 5**.

Tabla 4.

Distribución de Costo profesional por horas

Nombre	Función en el proyecto	Costo Hora	Dedicación Horas	Total
Yesica Pérez Pérez	Director del Proyecto	$ 12.500	10	$ 125.000
Edgar León López	Autor del proyecto	$ 7.000	32	$ 224.000
Kerly Y. Claro Luna	Autor del proyecto	$ 7.000	32	$ 224.000
			TOTAL	**$ 573.000**

Nota Fuente: Autores del Proyecto

Tabla 5.

Distribución de gastos

CONCEPTO	VALOR
Asesoría y trabajo profesional	$ 573.000
Fotocopias e Impresiones	$ 327.000
Alquiler de Internet y Computadores	$ 500.000
Transporte	$ 700.000
Llamadas	$ 150.000
Papelería	$ 350.000
Otros	$ 400.000
TOTAL	**$ 3.000.000**

Nota fuente: Autores del Proyecto

4.5 Cronograma de actividades

		2016						2017			
Objetivos	**Actividades**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**	**4**
Realizar un estudio preliminar a los controles existentes en el Centro de Cómputo para la identificación de posibles riesgos	1. Estudio de archivos permanentes (Procedimientos, instructivos, manuales, guías, etc)	**x**	**x**	**x**	**x**	**x**	**x**				
	2. Elaboración de Encuesta y realización de entrevista						**x**	**x**			
	3. Elaboración y aplicación de lista de chequeo						**x**	**x**			
Evaluar los controles de seguridad del Centro de Cómputo con base a los criterios establecidos en la Norma Técnica Colombiana ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942, para conocer el nivel de implementación de los mismos.	1. Realizar un análisis de diferencias GAP que muestre el nivel de implementación de los controles de la NTC ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942 p							**x**	**x**	**x**	
	2. Documentar los Papeles de trabajo de las pruebas								**x**	**x**	

Elaborar un informe final de auditoría con las oportunidades de mejora y las recomendaciones necesarias para optimizar la seguridad en el Centro de Datos de la empresa El Apostador.	1. Elaborar informe o dictamen de auditoría									**x**	**x**

Nota fuente: Autores del Proyecto

Capítulo 5. Análisis de la Información

Para desarrollar el estudio preliminar de los controles existentes en el Centro de Cómputo y posteriormente identificar los posibles riesgos, se realizaron las siguientes actividades:

a. **Comunicación a la empresa El Apostador informando sobre el inicio de la auditoría.**

Cúcuta, enero 29 de 2017

Señores
El Apostador
Jefe de Sistemas
Norte de Santander (Cúcuta)

Asunto: Informar la realización de un trabajo de auditoría sobre "EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL CENTRO DE CÓMPUTO DE LA EMPRESA EL APOSTADOR."

Le informamos que, en cumplimiento con el programa de la Especialización en Auditoría de Sistemas de la Universidad Francisco de Paula Santander Ocaña, requerimos realizar un trabajo de auditoría, el cual, se basará en la "Evaluación de la seguridad de la información en el Centro de Cómputo de la Empresa el Apostador", cuyo objetivo principal consiste en verificar si los controles de seguridad existentes, mitigan la ocurrencia de afectaciones a la integridad, confidencialidad y disponibilidad de la información.

El trabajo será desarrollado por profesionales, Kerly Yulieth Claro Luna (Ingeniera de Sistemas), Edgar León López (Ingeniero de Sistemas) en un tiempo estimado de dos meses.

Para determinar los posibles riesgos y controles a evaluar, llevaremos a cabo una primera fase, la cual consistirá en conocer la documentación que soportan los procesos manejados por el área Gestión de sistemas. Para ello, le solicitamos su colaboración designando un trabajador que actúe como guía para el suministro de la información que se pueda necesitar para el desarrollo del trabajo.

Una vez esta primera fase termine, se programará una reunión de apertura, para divulgar los resultados de la planeación, los riesgos y controles que serán objeto de la evaluación.

La entrega del informe preliminar se proyecta para el jueves 07 de abril del 2017.

Agradecemos la colaboración prestada y disposición y colaboración que brindan para la ejecución del trabajo.

EDGAR LEÓN LOPEZ (Auditor Líder) KERLY YULIETH CLARO LUNA (Auditor de campo) INGENIEROS DE SISTEMAS

b. **Estudio de la unidad auditable.** A continuación, se listan los archivos permanentes que hicieron parte del material de estudio de la auditoría:

AUDITORES EXTERNOS **Archivos Permanentes**	
Contenido	
Manual institucional	AP1-1/58
Organigrama de la Empresa	AP1-1/1
Misión, Visión y Objetivos	AP2-1/1
Manual de Funciones	AP4-1/35
Cronograma de mantenimientos preventivos	AP5-1/1
Inventario de Hardware área de informática y de activos fijos	AP6-1/10
Hojas de vida ordenadores, servidores, equipos de comunicación y demás equipos tecnológicos.	AP7-1/20
Plan de contingencia	AP8-1/40
Políticas Backups y Restauraciones	AP9-1/2

El área de sistemas de la Empresa el Apostador, cuenta con una estructura jerárquica donde se ubican los equipos que intervienen en el cumplimiento de la misión. Seguidamente se muestra de manera sucinta la información revisada.

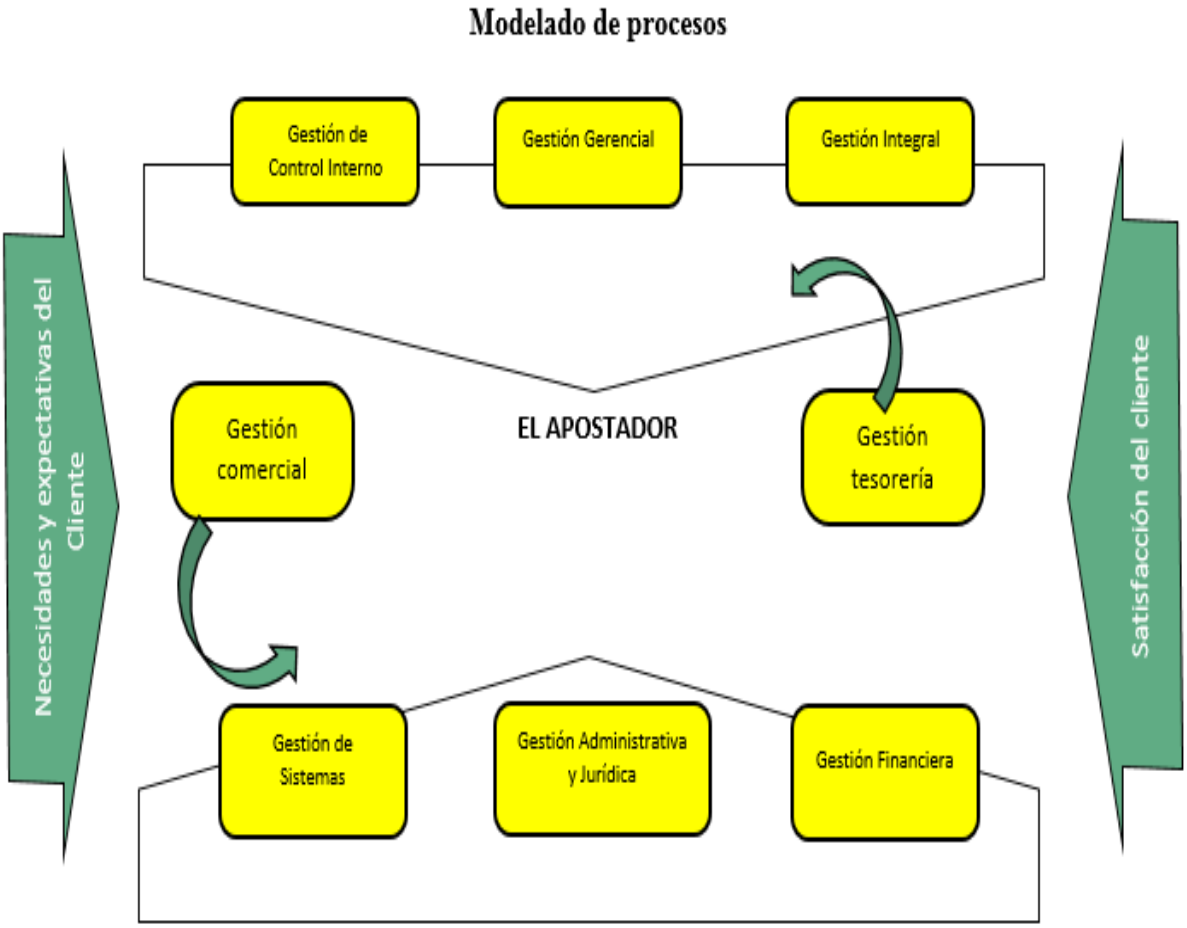

Ilustración 1. Dependencia: Sistemas

Proceso	GESTION DE SISTEMAS			
Objetivo del proceso	• Satisfacer los requerimientos de los clientes internos. • Asegurar la continuidad de los servicios de TI según lo requerido y en caso de falla minimizar el impacto sobre el funcionamiento del sistema. • Mantener la disponibilidad, integridad y confidencialidad de los sistemas de información, mediante la implementación de controles de seguridad. • Capacitar al usuario en el uso de la tecnología, los riesgos y las responsabilidades involucradas.			
Responsable	Director de Sistemas		AUTORIDAD: Gerente General	
Objetivo integral relacionado	• Adoptar la gestión de riesgos como una actividad continua en cada uno de los procesos de la empresa. • Aumentar la eficacia de los sistemas de información y tecnología para la óptima prestación del servicio.			
PLANEAR: Asegurar el correcto funcionamiento del Software, el Hardware y las comunicaciones, logrando la eficacia y el buen funcionamiento de todo el sistema operacional y organizacional.				
PROVEEDOR	ENTRADAS	HACER	SALIDAS	CLIENTES
Todos los proceso del SGI	Base de Datos Oracle	Administración de la base de datos y Backups en línea	Base de datos administrada y backups en cintas	Gerencia
Todos los proceso del SGI	Toma de Requerimientos	Desarrollo de nuevos aplicativos y mejoramiento del software existente	Sistemas en óptimas condiciones de funcionamiento	Todos los proceso del SGI
Gestión Comercial	Solicitud de comunicación	Establecimiento y mantenimiento de los medios de comunicación entre las oficinas y puntos de ventas	Establecimiento de la comunicación	Todos los procesos del SGI
Todos los proceso del SGI	Servicios y servidores	Administración de los servidores y los servicios	Servidores y servicios administrados	Todos los procesos del SGI
Gestión Administrativa y Jurídica	Personal administrativo	Creación de usuarios en el dominio, correo electrónico corporativo, asignación de permisos a las aplicaciones y dirección de red.	Dotación de Herramientas Sistematizadas.	Todos los proceso del SGI
Todos los proceso del SGI	Registro de incidentes Solicitudes de seguridad	Implementación controles de seguridad para la protección de la información y sistemas de información.	Información/ sistemas de información protegidos Incidentes mitigados Solicitudes implementadas	Todos los proceso del SGI
Gerencia (Aux. de compras)	Equipos para reparación	Reparación de máquinas, pc, impresoras y equipos de comunicación	Equipos reparados	Todos los proceso del SGI
Todos los proceso del SGI	Ciclo de mantenimiento programado	Mantenimiento preventivo de maquinitas, equipos de cómputo y comunicación	Cumplimiento de los ciclos de mantenimiento programados	Todos los procesos del SGI
VERIFICAR-SEGUIMIENTO: Auditoría Interna integral Control Servicio no Conforme Seguimiento Indicadores de Gestión				
ACTUAR: Acción Preventiva, Correctiva y Mejora.				
RECURSOS	DOCUMENTOS RELACIONADOS		INDICADORES	REQUISITOS
PC Servidores Equipos de comunicación maquinitas Sim Card Repuestos Suministros Cintas Software de protección Licencias	Ver: Listado Maestro de Documentos Ver: Listado Maestro de Registros		Ver: Manual de Indicadores de Gestión	NORMA ISO 9001:2008 Capitulo: 4, 8 Requisitos:6.3 7.1 , 7.2 NORMA ISO 27001:2005 Capitulo: 4 ANEXO A (ISO 27002) Objetivos de Control y Controles: A.6.2, A.7.1.3, A.7.2.2, A.9.2, A.10, A.11, A.12, A.13, A.15.2 REQUISITOS LEGALES: Ley 23 de 1982 Ley 44 de 1993 Ley 1273 de 2009 Constitución Política: Art. 15, 61, 150-24, 189-27

Ilustración 2. Caracterización del Proceso

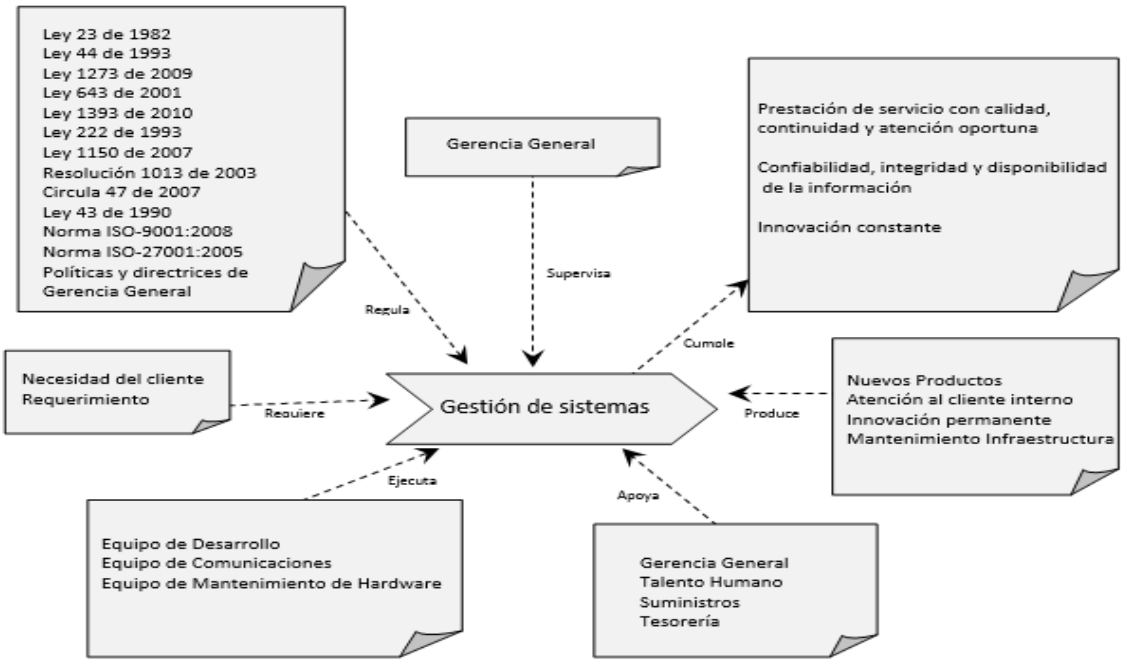

Ilustración 3. Diagrama Descripción del Proceso

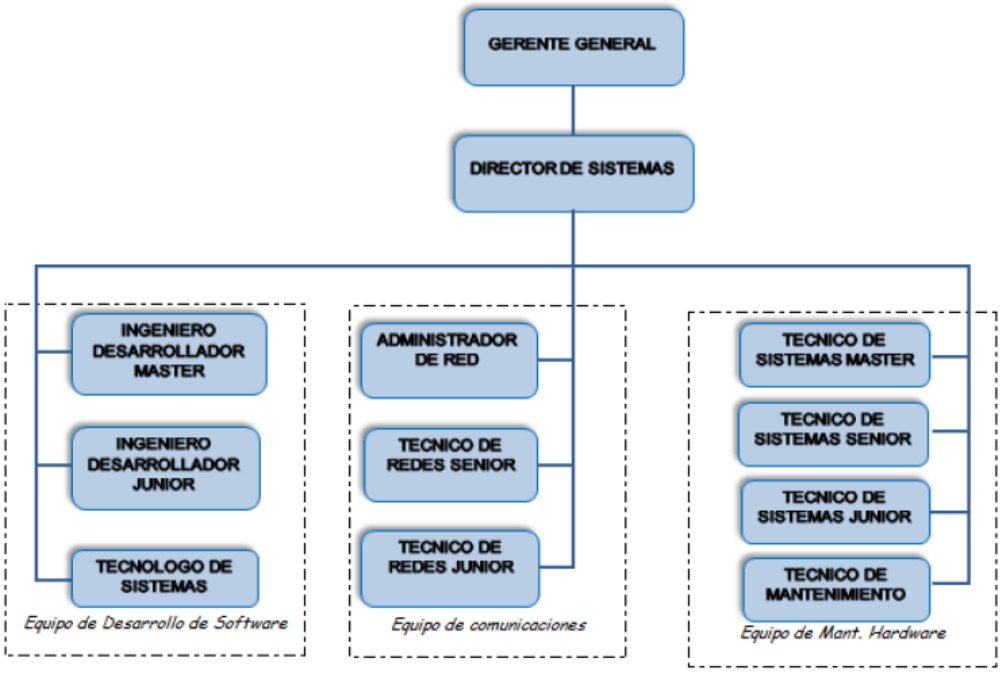

Ilustración 4. Estructura Área Sistemas

Infraestructura Tecnológica:

La actividad comercial de la empresa se apoya en la tecnología y, por lo tanto, es de gran importancia para la empresa EL APOSTADOR mantener una infraestructura tecnológica sólida y moderna.

Su Infraestructura tecnológica está conformada por un Centro de cómputo con servidores de alta disponibilidad. Una comunicación WAN propia que cubre todo el departamento y un software adecuado para el manejo de sus bases de datos como también un aplicativo hecho a la medida.

Características del Data Center

- Servidor IBM Power 5
- Servidor IBM 445
- Servidor de Dominio IBM X3250
- Librería para copias de seguridad TSM 3200
- Ups de 10Kva, 6Kva Con su respectivo respaldo
- Detectores de humo
- Sensores de movimiento
- Cámaras de grabación 7 / 24
- Planta eléctrica
- Sensores de humedad y temperatura
- Detector de líquidos
- Control de acceso mediante biométrico

Comunicaciones

- Enlaces propios que cubren el área metropolitana y municipios
- Alta disponibilidad en Fail-over Seguridad

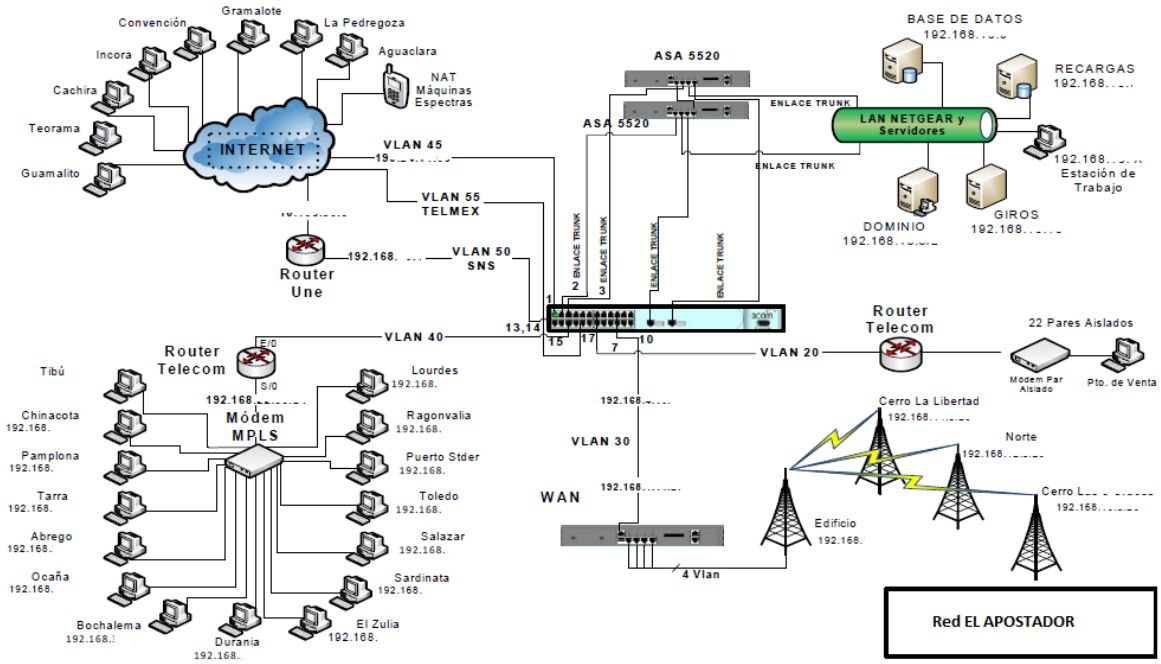

Ilustración 5. Mapa de Red

- Arquitectura del Software
- Punto de venta en JAVA por desarrollo propio
- Base de datos RAC de Alta disponibilidad

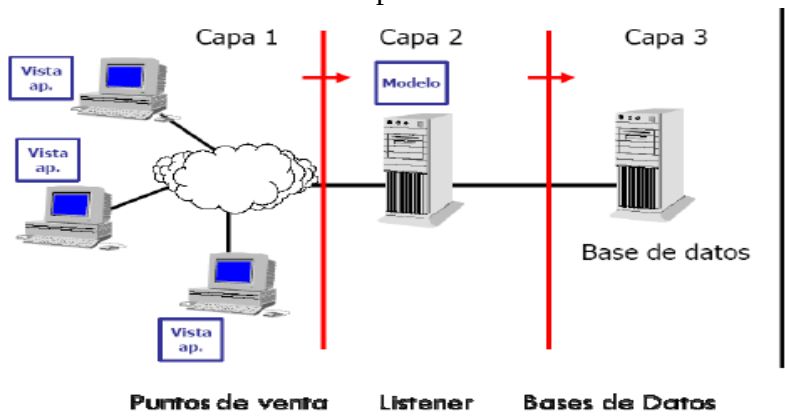

Ilustración 6. Software

5.1 Técnicas de Recolección

Dentro de las técnicas y herramientas implementadas para el estudio del área de sistemas, se utilizó la observación, lista de chequeo y entrevista.

5.1.1 Lista de chequeo: Este documento se elaboró dentro de la fase de planeación con la finalidad de conocer si el control definido en los documentos permanentes existe, es aplicado y funciona:

Tabla 6.

Lista de Chequeo

	AUDITORES EXTERNOS **LISTA DE CHEQUEO**			
Dirigida a:	Director de Sistemas			
Objetivo:	Recolectar información necesaria sobre aspectos principales de control definidos en los procesos que soportan el manejo de la infraestructura tecnológica, con el fin de determinar su cumplimiento.			
Verificar el cumplimiento de los procesos de monitoreo del Centro de Datos				
DESCRIPCION DEL CONCEPTO				**CUMPLE**
Existe monitoreo permanente de la consola SNMPC a los dispositivos de la red				**SI**
La consola Cisco ASDM Launcher se monitorea permanentemente				**SI**
La consola PRTG se monitorea de forma permanente				**SI**
Se está haciendo la revisión diaria del Antivirus				**SI**
Verificar el Cumplimiento de los procesos de mantenimiento WLAN Y Torres				
Calificar el grado de cumplimiento de:	**25%**	**50%**	**75%**	**100%**
Se hace revisión de señal, mástil, cableado externo e interno			**X**	
Se revisa el correcto funcionamiento de las luces de emergencia			**X**	
Se hace análisis de espectro y medidas de voltaje			**X**	

Se hace Bypass manual a las UPS		X		
Se revisa el estado de las baterías de las UPS		X		
Se realiza el cambio de encripción de los punto a punto			X	
Se hace anualmente el cambio de claves de los equipos de comunicaciones				X
Se registra el mantenimiento en la hoja de vida del punto				X
Verificar el Cumplimiento de los procesos de Acceso físico al Centro de Cómputo				
Calificar el grado de cumplimiento de:	**25%**	**50%**	**75%**	**100%**
Todo acceso al Centro de Cómputo se comunica al Director de Sistemas			X	
Todo ingreso de un tercero debe ser autorizado por el Director de Sistemas				X
Todo ingreso de un tercero debe hacerse acompañado permanentemente por un funcionario de sistemas				X
Los accesos al Centro de Cómputo se registran en el formato F-GS-19 de Control de Ingreso				X
La puerta de ingreso se cierra inmediatamente al ingresar alguien al Centro de Cómputo				X
Solo se puede ingresar al Centro de Cómputo utilizando el control remoto para abrir la puerta		X		
Verificar el Cumplimiento de los procesos de Registro de Usuarios y gestión de privilegios				
Calificar el grado de cumplimiento de:	**25%**	**50%**	**75%**	**100%**
Las solicitudes se hacen a través del módulo de requerimientos		X		
Toda solicitud debe ser aprobada por un Jefe de Proceso		X		
Las claves de los usuarios de aplicaciones y equipos críticos se cambian periódicamente (Según documentación cada 3 meses)			X	
Las claves se resguardan en un sobre sellado				X
Los sobres con la claves reposan en la caja fuerte				X

Nota fuente: Autores del Proyecto

5.1.2 Entrevista: Este documento se elaboró dentro de la fase de planeación con la finalidad de conocer la existencia y funcionamiento de los controles de seguridad de la información físicos y lógicos del centro de cómputo.

Tabla 7.

Entrevista

	**AUDITORES EXTERNOS** **ENTREVISTA**
Entrevistador:	Auditores
Cargo:	Director de Sistemas

La presente entrevista contiene preguntas que hacen referencia al Centro de Cómputo de la Empresa EL APOSTADOR y se divide en 2 partes: Seguridad Física y Seguridad Lógica.

El objetivo de la entrevista está enmarcado en conocer aspectos de seguridad tanto física y lógica del Centro de Cómputo.

Seguridad física:

1. **Del personal que conforma el área de sistemas, ¿quiénes y cómo ingresan al Centro de Cómputo?**

Rta. Al Centro de Cómputo puede ingresar todo el personal que registrado, en razón a que el acceso al Centro de cómputo exige la lectura de la huella mediante un biométrico dactilar y el paso de la tarjeta electrónica. Así mismo se lleva un registro de los accesos al Centro de Cómputo.

2. **En la infraestructura física de su empresa, ¿dónde está ubicado el Centro de Cómputo?**

Rta. El Centro de Cómputo se encuentra ubicado en el segundo piso de una estructura física de tres pisos.

3. **Al implementar el Centro de Cómputo en su empresa, ¿hubo algunos diagnósticos previos y especificaciones técnicas para su diseño?**

Rta. Creo que no lo hubo ya que existe la parte eléctrica, tableros eléctricos y UPS junto a los servidores. Estos deberían estar separados. Además, no hay aires acondicionados que sean adecuados para el Centro de Cómputo.

4. **¿Las instalaciones del Centro de Cómputo cuentan con sistemas de alarmas que informen oportunamente eventos como inundaciones, incendios, cambios de temperatura entre otros?**

Rta. El Centro de Cómputo cuenta con sensores de humedad, movimiento y humo. Sin embargo, en caso de incendio, no hay un sistema de extinción automático, este debe apagarse de forma manual con los extintores.

5. **¿Cuál es la formación académica del personal que labora en el área de sistemas que usted lidera?**

Rta. Todos deben ser profesionales en Informática. Entiéndase profesional: técnicos, ingenieros y tecnólogos

6. **Del personal que conforma su área de sistemas, ¿existe personal designado para ejercer la responsabilidad de administración del Centro de Cómputo?**

Rta. No hay un responsable directo. Hay una persona responsable de Infraestructura y un responsable de la red o de comunicaciones. Yo como director soy responsable de la plataforma.

7. **Para la correcta administración del Centro de Cómputo, ¿existen planes de mantenimientos preventivos de los equipos que lo conforman?**

Rta. Si existe y se ejecuta 2 veces al año.

8. **¿Los equipos que hacen parte del Centro de Cómputo son activos fijos de la empresa y están respaldados por alguna aseguradora?**

Rta. Si son activos fijos y si están asegurados.

9. **¿Los equipos que hacen parte del Centro de Cómputo cuentan con contrato vigente para cubrir eventuales emergencias?**

Rta. En este momento solo están respaldados los equipos de comunicaciones: Routers, Switches y Firewalls

10. **¿Actualmente se lleva un registro o bitácora de los accesos al Centro de Cómputo?**

Rta. Si existe un registro para el ingreso al Centro de Cómputo

<u>Seguridad lógica</u>

1. **¿El Centro de Cómputo cuenta con herramientas de seguridad para el acceso a la información como firewall, encriptación, antivirus u otros?**

Rta. Sí. Actualmente se cuenta con Firewall y un Antivirus de Symantec.

2. **En cuanto a los accesos de los usuarios, ¿existen políticas adecuadas de accesos e inhabilitación de cuentas a personal retirado?**

Rta. Si existen unos procesos para permitir y restringir el acceso de los usuarios

3. **¿La información procesada y almacenada en el Centro de Cómputo cuenta con cronogramas de backups y restauraciones?**

Rta. Si existen cronogramas de backups. La restauración se ha probado de forma parcial, en razón a que se requiere máquinas similares para realizar restauraciones completas.

4. **En su empresa, ¿las copias de seguridad de información se almacenan internamente o existe un lugar externo para su custodia?**

Rta. Si se realizan copias de seguridad, pero estas son guardadas en la bóveda de seguridad del edificio principal.

5. **¿El motor de base de datos cuenta con un contrato de soporte vigente para cubrir eventuales fallas del sistema?**

Rta. No. Se decidió no mantener el contrato de soporte por costos

6. **Para el manejo adecuado de las claves de acceso, por favor indíquenos si existe un control y cómo funciona.**

Rta. Si existe y está soportado en restablecimientos periódicos de claves

Nota fuente: Autores del Proyecto

5.2. Herramienta de Riesgos y Controles

La calificación del riesgo sin control o absoluto, se realizó mediante una herramienta de evaluación de nivel de riesgos basada en la NIST 800 30 y la ISO 31000 del 2009, permitiendo la calificación de la probabilidad y ocurrencia del riesgo *Afectación a la integridad, confidencialidad y disponibilidad de la información,* cuyo objeto relevante es la Información.

Descripción del riesgo: La probabilidad de pérdida de integridad se presenta cuando se modifica o se borra información, la probabilidad de falta de confidencialidad se presenta cuando

personal no autorizado accede a la información y la probabilidad de indisponibilidad se presenta cuando las personas autorizadas no pueden acceder a la información.

Tabla 8.

Listado de riesgos y controles

Código	Riesgos	Controles
1	Afectación a la integridad, confidencialidad y disponibilidad de la información.	- Mantenimientos preventivos - Inventarios de hardware y software - Política de seguridad y calidad de la información - Plan de contingencia - Backups y restauraciones - Segregación de funciones - Gestión de privilegios - Monitoreos periódicos - Registro de auditorías - Control de acceso físico y lógico - Buenas prácticas de la NTC ISO/IEC 27000:2015 y el estándar ANSI/TIA/EIA-942

Nota fuente: Autores del proyecto

Tabla 9.

Valoración del riesgo

Criterios de valoración de las consecuencias, teniendo como objeto de impacto relevante la Información.

CRITERIOS DE VALORACIÓN DE LAS CONSECUENCIAS		
Valor	**Clasificación**	**Información**
16	**Máxima**	* Genera pérdida de confidencialidad de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos con efectos no recuperables. * Genera uso de información no íntegra ya sea a nivel interno o externo con efectos no recuperables. * Genera pérdida de disponibilidad de información con efectos no recuperables.
8	**Mayor**	* Genera pérdida de confidencialidad de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos con efectos mitigables o recuperables en el largo plazo. * Genera uso de información no íntegra ya sea a nivel interno o externo con efectos mitigables o recuperables en el largo plazo. * Genera pérdida de disponibilidad de información con efectos mitigables o recuperables en el largo plazo.

4	**Moderada**	* Genera pérdida de confidencialidad de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos con efectos mitigables o recuperables en el mediano plazo. * Genera uso de información no íntegra ya sea a nivel interno o externo con efectos mitigables o recuperables en el mediano plazo. , * Genera pérdida de disponibilidad de información con efectos mitigables o recuperables en el mediano plazo.
2	**Menor**	* Genera pérdida de confidencialidad de información que puede ser de utilidad para la competencia o individuos o grupos internos o externos con efectos mitigables o recuperables en el corto plazo. * Genera uso de información no íntegra ya sea a nivel interno o externo con efectos mitigables o recuperables en el corto plazo. * Genera pérdida de disponibilidad de información con efectos mitigables o recuperables en el corto plazo.
1	**Mínima**	* Genera pérdida de confidencialidad de información que no es de utilidad para la competencia o individuos o grupos internos o externos. * Genera uso de información no íntegra ya sea a nivel interno o externo sin efectos negativos. * Genera pérdida de disponibilidad de información sin efectos negativos.

Nota fuente: Autores del proyecto

Tabla 10.

Criterios de Valorización de la probabilidad

Valor	Clasificación	Descripción	Probabilidad de ocurrencia en el período del proyecto
5	**Muy alta**	Muy alta probabilidad de ocurrencia Es probable que ocurra muchas veces	Mayor del 85%
4	**Alta**	Alta probabilidad de ocurrencia Es probable que ocurra varias veces	60.1% - 85%
3	**Media**	Mediana probabilidad de ocurrencia Es probable que ocurra algunas veces	25.1% - 60%
2	**Baja**	Baja probabilidad de ocurrencia Es poco probable que ocurra, pero es posible.	5.1% - 25%
1	**Muy baja**	Es casi imposible que ocurra Puede ocurrir en circunstancias excepcionales	Menor o igual al 5%

Nota fuente: Autores del proyecto

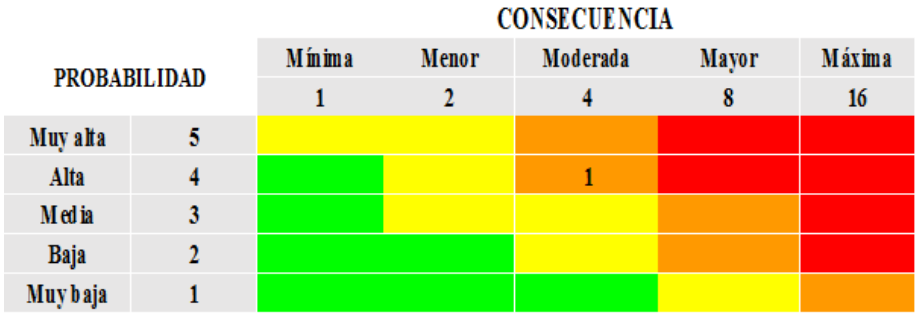

Ilustración 7. Matriz de Riesgos
Nota fuente: Autores del proyecto

Tabla 11.

Niveles de Riesgo

NIVELES DE RIESGO		
32-80	**Extremo**	Máxima prioridad; se requiere de acciones inmediatas. Debe ponerse en conocimiento de la gerencia general (para análisis de riesgos en proyectos o procesos, en conocimiento de la vicepresidencia o gerencia). Para controles o medidas de tratamiento que impliquen inversión económica, realizar estudios de Costo-Beneficio. Seguimiento continuo. Transferir el riesgo a los aseguradores o a terceros vía contratos.
16-24	**Alto**	Alta prioridad; se requiere de acciones a corto plazo. Debe ponerse en conocimiento de la vicepresidencia (para análisis de riesgos en proyectos o procesos, en conocimiento de la dirección). Para controles o medidas de tratamiento que impliquen inversión económica, realizar estudios de Costo-Beneficio. Seguimiento periódico convenido (mínimo tres veces en el año). Transferir el riesgo a los aseguradores o a terceros vía contratos. Estudiar posibles alternativas de retención parcial de riesgos.
5-12	**Tolerable**	Prioridad moderada, se requiere de acciones a mediano plazo. A cargo de las de la direcciones y gerencias. Seguimiento periódico convenido (mínimo dos veces en el año). Evaluar la posibilidad de retener el riesgo, parcial o totalmente.
1-4	**Aceptable**	Baja prioridad; no son necesarias acciones adicionales. Requiere de monitoreo anual. Evaluar la posibilidad de retener el riesgo.

Nivel de riesgo: Es el producto de la probabilidad y el impacto.

0,37	**0**	**Bajo**
0,53	**0,37**	**Medio**
0,67	**0,53**	**Alto**
1	**0,67**	**Muy Alto**

Ilustración 8. Escala de Evaluación
Nota fuente: Autores del proyecto

5.3 Acta reunión de apertura de la auditoría.

ACTA DE REUNIÓN

No: 01

NOMBRE DEL TRABAJO	**EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACION EN EL CENTRO DE CÓMPUTO DE LA EMPRESA EL APOSTADOR**

LUGAR	**FECHA**			**HORA**	
	Día	**Mes**	**Año**	**Inicio**	**Fin**
Sede principal empresa el Apostador	15	02	2017	17:30	18:00

ELABORADA POR:	Kerly Yulieth Claro Luna Edgar León López

ASISTENTES POR PARTE DE LOS AUDITADOS			
NOMBRE	**CARGO**	**DEPENDENCIA**	**FIRMA**
Freddy López Luna	Jefe de Sistemas	Sistemas	

ASISTENTES POR PARTE DEL EQUIPO DE AUDITORÍA			
NOMBRE	**CARGO**	**DEPENDENCIA**	**FIRMA**
Kerly Yulieth Claro Luna	Ingeniera de Sistemas	N.A	
Edgar León López	Ingeniero de Sistemas	N.A	

TEMAS A DESARROLLAR	
No.:	**DESCRIPCIÓN**
1	**Presentación de la planeación del trabajo**

DESARROLLO DE LOS TEMAS

Los auditores dan inicio a la reunión presentando la planeación del trabajo de auditoría Evaluación de la seguridad de la información en el Centro de Cómputo de la empresa el Apostador.

Riesgo Identificado: Afectación a la integridad, confidencialidad y disponibilidad de la información.

Descripción del Riesgo: La probabilidad de pérdida de integridad se presenta cuando se modifica o se borra información, la probabilidad de falta de confidencialidad se presenta cuando personal no autorizado accede a la información y la probabilidad de indisponibilidad se presenta cuando las personas autorizadas no pueden acceder a la información.

Objetivo General: Verificar si los controles de seguridad existentes en el Centro de Cómputo de la Empresa El Apostador, mitigan la ocurrencia de afectaciones a la integridad, confidencialidad y disponibilidad de la información.

Objetivo Específico:

Realizar un estudio preliminar a los controles existentes en el Centro de Cómputo para la identificación de posibles riesgos.

Evaluar los controles de seguridad del Centro de Cómputo con base a los criterios establecidos en la Norma Técnica Colombiana ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942, para

conocer el nivel de implementación de los mismos.

Elaborar un informe final de auditoría con las oportunidades de mejora y las recomendaciones necesarias para optimizar la seguridad en el Centro de Datos de la empresa El Apostador.

Las pruebas se realizarán utilizando técnicas de observación, indagación, encuestas, muestras y pruebas sustantivas. Las recomendaciones resultantes del trabajo de auditoría permitirán evaluar de forma proactiva los controles definidos para prevenir el riesgo de seguridad de la información del proceso Gestión de Sistemas y la mejora del mismo, las cuales son facultativas de su adopción, en todo caso deben primar el análisis de causa que se efectué en caso de formularse un plan de mejora por parte del Área responsable.

CONCLUSIONES
El auditado manifestó estar de acuerdo con lo expuesto por los auditores en la presente reunión y acepta la realización del trabajo.

COMPROMISOS			
No.	**TEMA**	**RESPONSABLE**	**FECHA DE ENTREGA**
1	Presentación de Informe de auditoría	Auditores	15 de abril del 2017

ANEXOS
N.A.

5.4 Programa de Auditoría

Auditores Externos	**Programa de Auditoría**

NOMBRE DE LA AUDITORÍA	EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACION EN EL CENTRO DE CÓMPUTO DE LA EMPRESA EL APOSTADOR
VERSIÓN DEL PROGRAMA	01
FECHA	03/2017
OBJETIVOS	
GENERAL	
Verificar si los controles de seguridad existentes en el Centro de Cómputo de la Empresa El Apostador, mitigan la ocurrencia de afectaciones a la integridad, confidencialidad y disponibilidad de la información.	
ESPECÍFICOS	
* Realizar un estudio preliminar a los controles existentes en el Centro de Cómputo para la identificación de posibles riesgos. * Evaluar los controles de seguridad del Centro de Cómputo con base en los criterios establecidos en la Norma Técnica Colombiana ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942, para conocer el nivel de implementación de los mismos. * Elaborar un informe final de auditoría con las oportunidades de mejora y las recomendaciones necesarias para optimizar la seguridad en el Centro de Datos de la empresa El Apostador.	
CRITERIOS Y GUIAS	
Se identificarán las brechas de seguridad de la información en el Centro de Cómputo El Apostador con base en la Norma Técnica Colombiana ISO/IEC 27001:2013 y el estándar ANSI/TIA/EIA-942	
NECESIDADES TECNICAS	
*Estudio de la documentación del área de Sistemas y del Centro de Cómputo del Apostador *Entrevistas con los responsables *Observación *Validación de Información	
¿Requiere utilizar Técnicas de Auditoría Asistidas por Computador -TAAC´s?	SI
PRUEBA RELACIONADA	

NOMBRE DE LA PRUEBA	ANALISIS GAP ANALISIS GAP - Medición del Nivel de Madurez del SGSI
OBJETIVO DE LA PRUEBA	Analizar y diagnosticar el estado de la seguridad del Centro de Cómputo el Apostador mediante la utilización de buenas prácticas de la norma técnica colombiana ISO 27001:2013.
DESCRIPCIÓN DE LA PRUEBA	Aplicación de una herramienta de análisis GAP con los criterios de la NTC ISO/EIC 27001:2013
PROCEDIMIENTO DE LA PRUEBA	Mediante el Anexo A de la Norma ISO 27001:2013 que contiene una guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a seguridad de la información, se evaluará aspectos de seguridad del Centro de Cómputo de la Empresa el Apostador.

Capítulo 6. GAP Análisis

Para poder conocer el nivel de cumplimiento del Sistema de Gestión de la Seguridad de la Información en la empresa El Apostador y poder determinar las deficiencias o necesidades del sistema, que requieren atención, se hace uso del GAP análisis.

La realización de un análisis de deficiencias ayuda a identificar los puntos débiles del SGSI de la compañía y ayudará a la alta dirección a conocer de manera precisa las falencias y estimar unos plazos realistas para su mejora.

Este análisis se basa en una técnica de muestreo, mediante la cual se evalúa el sistema de gestión existente o sus procedimientos, contra todos los requisitos de la norma ISO/IEC 27001.

6.1 Escala

La escala utilizada para calificar la evaluación realizada, se encuentra especificada a continuación

Tabla 12.

Análisis GAP

Auditores Externos		**AUDITORÍA EL APOSTADOR**	
		ANALISIS GAP	Versión 01
Escala de valoración			
Valor	**Nivel**	**Descripción**	
n	**No aplica**	* El control no puede definirse por alguna restricción propia de la empresa evaluada	

0	**Inexistente**	* El control no existe
1	**Muy bajo**	* El control se ejecuta de forma manual, su frecuencia de aplicación es esporádica, no hay responsable asignado y está sin documentar en sus componentes y/o su aplicación. * Los controles no cumplen ningún tipo de normativa.
2	**Bajo**	* El control se ejecuta de forma manual o semiautomática, su frecuencia de aplicación es esporádica o periódica, hay responsable asignado sin formalizar y está deficientemente documentado en sus componentes y/o su aplicación. * Los controles cumplen parcialmente requerimientos normativos mínimos.
3	**Medio**	* El control se ejecuta de forma semiautomática, su frecuencia de aplicación es periódica, hay responsable asignado sin formalizar y está parcialmente documentado en sus componentes y/o su aplicación. * Los controles cumplen requerimientos normativos mínimos.
4	**Alto**	* El control se ejecuta de forma semiautomática o sistematizada, su frecuencia de aplicación es periódica o continua, hay responsable asignado formalmente y está cerca de documentarse completamente en sus componentes y/o su aplicación. * Se han implementado los controles desde la perspectiva Costo/ Beneficio.
5	**Muy alto**	* El control se ejecuta de forma sistematizada, su frecuencia de aplicación es continua, tiene responsable asignado formalmente, está completamente documentado en sus componentes y se documenta su aplicación. * Aplicación de mejores prácticas.

En la sección de Apéndices se encontrara la información pertinente donde se evalúan los controles que hacen parte de cada uno de los trece dominios que conforman en Anexo A de la norma ISO/IEC 27001, y de acuerdo a lo evidenciado en el Centro de Cómputo de la empresa El Apostador, se determina la escala de calificación para cada control.

6.2 Resultados

Una vez realizada la evaluación del anexo A de la norma ISO/IEC 27001, se procede a su calificación, obteniendo el siguiente resultado:

Tabla 13.

Resultados Evaluación

ASPECTO	CALIFICACIÓN	VALORACIÓN
A5-Políticas de Seguridad de la Información	**2,00**	**Bajo**
A6-Organización de la Seguridad de la Información	**1,25**	**Muy Bajo**
A7-Seguridad Ligada a los Recursos Humanos	**3,33**	**Medio**
A8-Administración de Activos	**2,11**	**Bajo**
A9-Control de Acceso	**3,08**	**Medio**
A10-Criptografía	**-**	**No Aplica**
A11-Seguridad Física y del Ambiente	**3,46**	**Medio**
A12-Seguridad de las Operaciones	**2,64**	**Bajo**
A13-Seguridad de las Comunicaciones	**4,00**	**Alto**
A14-Adquisición, desarrollo y mantenimiento	**2,30**	**Bajo**
A15-Relaciones con el proveedor	**-**	**No Aplica**
A16-Gestión de Incidentes de Seguridad de la información y mejoras	**2,00**	**Bajo**
A17-Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**2,00**	**Bajo**
A18-Cumplimiento	**3,50**	**Medio**

Nota fuente: Autores del proyecto

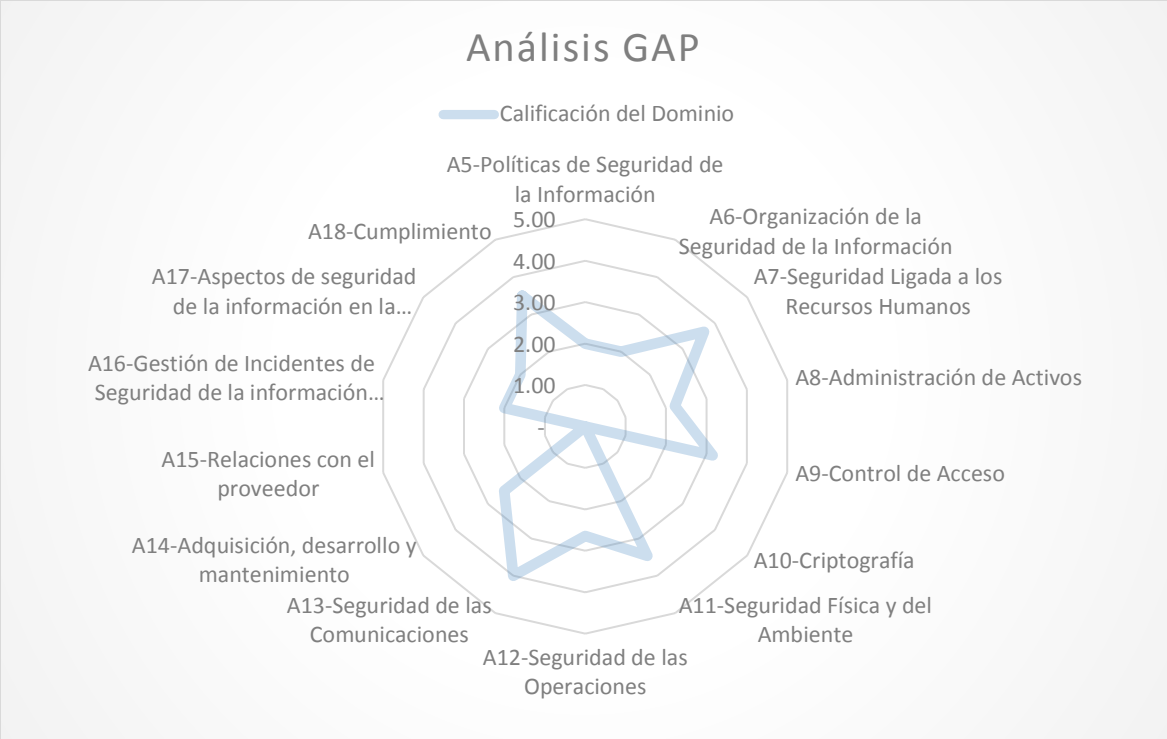

Ilustración 9. Análisis Gap

Teniendo en cuenta los resultados obtenidos, se observa que los dominios con deficiencias en el SGSI de la empresa El Apostador, son:

Tabla 14.
Dominios con Deficiencias en el SGSI

ASPECTO	CALIFICACIÓN	VALORACIÓN
A5-Políticas de Seguridad de la Información	**2,00**	**Bajo**
A6-Organización de la Seguridad de la Información	**1,25**	**Muy Bajo**
A8-Administración de Activos	**2,11**	**Bajo**
A12-Seguridad de las Operaciones	**2,64**	**Bajo**
A14-Adquisición, desarrollo y mantenimiento	**2,30**	**Bajo**
A16-Gestión de Incidentes de Seguridad de la información y mejoras	**2,00**	**Bajo**
A17-Aspectos de seguridad de la información en la gestión de la continuidad del negocio	**2,00**	**Bajo**

Nota fuente: Autores del proyecto

De acuerdo con los planteamientos expuestos con anterioridad estas deben tomarse como oportunidades de mejora.

Capítulo 7. Oportunidades de Mejora

7.1 Organización de la seguridad de la información

Se debe establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.

Como resultado de la evaluación se encontró:

• No se observó un documento con los roles definidos y una matriz de incompatibilidades para facilitar una adecuada segregación de funciones. Ausencia de un procedimiento para autorizar la asignación de permisos y su retiro de los sistemas de información y demás accesos a la información.

• A pesar de la existencia de segregación de funciones, no se establece claramente la responsabilidad del funcionario con la información.

• No existe una política clara que regule el uso de dispositivos móviles.

• El acceso remoto a la empresa El Apostador, está prohibido, sin embargo, en situaciones extraordinarias se permite, pero no queda un rastro en el sistema que facilite detectar las acciones del usuario.

Recomendaciones

▪ Debido a que existe en la empresa una segregación de funciones bien definida, debe aprovecharse y asignarse la información de la cual ese funcionario debe hacerse responsable.

▪ En la empresa, por la naturaleza de su actividad, existe un personal técnico que utiliza equipos portátiles. Este personal permanece fuera de las instalaciones constantemente. Debe establecerse una política clara en el manejo de estos equipos, que contemplan los siguientes aspectos:

- Los equipos portátiles no se deben llevar para la casa del funcionario.
- La información de los equipos portátiles, debe estar encriptada, en caso de pérdida o robo.
- Los equipos portátiles deben ser revisados periódicamente por el personal técnico de la compañía.

- Debe establecerse una VPN que solicite usuario y clave para el acceso remoto, configurada de tal forma que permita hacer un seguimiento real de las actividades realizadas.

- No se debe permitir el acceso remoto por medio de programas abiertos como Team Viewer por ejemplo.

7.2 Políticas de Seguridad de la Información

De acuerdo a la norma, se debe proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.

Como resultado de la evaluación se encontró:

- No están documentadas e implementadas las políticas de seguridad de la información

- No se observan soportes de una revisión periódica de políticas de seguridad de la compañía

Al no tener definidas unas políticas claras y documentadas acerca de la seguridad de la información, aumenta la probabilidad de riesgo de fraude.

Recomendaciones

- Deben definirse de forma clara y concisa, unas políticas de seguridad de la información que se ajusten a los requerimientos del negocio.
- Una vez definidas, deben darse a conocer a todo el personal involucrado, con unas capacitaciones periódicas y permanentes.

7.3 Administración de Activos

Se deben identificar los activos de la organización y definir las responsabilidades de protección pertinentes.

Como resultado de la evaluación se encontró:

- No se observa un documento que defina las reglas para el uso de la información, ni para los activos relacionados con el manejo de la misma.

- No se observa un documento que defina la clasificación de la información.

- Al no existir una clasificación de la información, tampoco existe un documento que etiquete la información.

- Al no existir una clasificación de la información, tampoco existe un procedimiento para el manejo de activos de acuerdo a la clasificación de la misma.

Recomendaciones

La información tiene que clasificarse para indicar el grado de necesidad, de prioridad y de protección. Según la norma ISO27001 la información se puede clasificar según su valor, los requisitos legales, la sensibilidad y la criticidad de la empresa. En este caso, se recomienda realizar la clasificación de la información, basándose en criterios de confidencialidad.

La información se puede clasificar en 4 pasos que son (ISOTools Colombia, 2016):

- Realizar un inventario de activos de información
    - Debe conocerse qué activos de información tiene la empresa y quiénes son sus propietarios o responsables
- Clasificar los activos identificados

  Se pueden clasificar en 4 niveles de acuerdo a su nivel de confidencialidad:
    - Confidencial (Nivel alto de confidencialidad)
    - Restringida (Confidencialidad media)
    - De uso interno (Confidencialidad baja)
    - Público (De libre acceso)

  Además, pueden clasificarse de acuerdo al medio de comunicación utilizado, como por correo electrónico, en papel, en bases de datos, entre otros medios.

- Etiquetar los Activos

La forma de etiquetar los activos de información, es responsabilidad de la compañía. Como ejemplo se puede tomar la información en papel, con una marca que indique la confidencialidad en la esquina superior derecha del documento.

- Manejo de los Activos de la información de manera segura

Cada empresa es autónoma en detallar las reglas que considere para proteger la información, de acuerdo a su clasificación. Por ejemplo, un documento confidencial, debe permanecer en armarios con llave.

7.4 Requisitos del negocio para el control de acceso

Se debe restringir el acceso a la información y a las instalaciones de procesamiento de información.

Como resultado de la evaluación se encontró:

- No existe un procedimiento establecido que restrinja o controle los accesos privilegiados. Estos accesos se asignan de acuerdo a la consideración personal del director de sistemas de turno.
- No se observa un procedimiento establecido que controle la autenticación secreta de los usuarios.
- No existe un control de acceso al código fuente de los programas por parte de los desarrolladores.

Recomendaciones

- Debe establecerse un perfil de usuario que sea adecuado para asignarle la responsabilidad de los accesos privilegiados. Este puede ser de acuerdo al cargo desempeñado.

- Debe establecerse una herramienta de auditoría, que permita monitorear las actividades de la cuenta con acceso privilegiado.

- Para la autenticación secreta de los usuarios, deben establecerse políticas que hagan obligatorio el uso de buenas prácticas en el establecimiento de contraseñas.

- Debe implementarse un espacio único (servidor) para guardar el código fuente. Este espacio debe contar con una herramienta de control de versiones y debe tener restringida la copia de los archivos.

- Por otra parte, las máquinas utilizadas para el desarrollo, deben tener restringido (o eliminado) los puertos USB, unidades de CD-ROM, y correo electrónico.

7.5 Seguridad física y ambiental

Se debe evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.

Como resultado de la evaluación se encontró:

- Al ingresar a las instalaciones de la empresa el Apostador, sólo se da un carnet que debe portar el visitante.

- Las instalaciones cuentan únicamente con un sistema de detección de incendios, pero no tiene un sistema de apagado automático. Este debe hacerse de forma manual con extintores dispuestos para el caso.

Recomendaciones

- Deben implementarse seguros electrónicos en las puertas de acceso a las oficinas o debe asignarse un acompañante al visitante que garantice el lugar de visita correcto.

- Debe implementarse un sistema de apagado de incendios de forma automática y separar la parte eléctrica de la parte de datos.

7.6 Seguridad de las operaciones

Se debe asegurar la operación correcta y segura de las instalaciones de procesamiento de información.

Como resultado de la evaluación se encontró:

- No se encuentra documentación referente a los procedimientos de operación de los activos del Centro de Cómputo

- No existe un control sobre las actividades del administrador del sistema

- No existe un informe que determine las vulnerabilidades técnicas de los sistemas; por lo tanto, tampoco existe un plan de medidas para atacar el riesgo.

- No existe una actividad de auditoría que verifique los sistemas operacionales.

Recomendaciones

- Los activos del centro de cómputo, deben contar con una documentación clara y precisa de su puesta en funcionamiento y de su operatividad básica.
- Esta documentación debe estar únicamente al alcance del personal autorizado.

- Debe implementarse una herramienta que permita hacer auditoría a las actividades realizadas por la cuenta de acceso privilegiado.
- Debe desarrollarse un informe que determine de forma clara, las vulnerabilidades técnicas de los activos y un plan que permita minimizar los riesgos.
- Debe hacerse una revisión periódica de los sistemas operativos, con el fin de aplicarles parches, actualizaciones y mejoras que eviten los llamados Bugs.

7.7 Adquisición, desarrollo y mantenimiento de sistemas

Debe asegurarse que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de los sistemas de información.

Como resultado de la evaluación se encontró:

- En los nuevos desarrollos, o en las mejoras realizadas a los sistemas de información existentes, no se aplica ningún requisito relacionado con la seguridad de la información.
- No se encuentra un documento que defina las reglas para el desarrollo seguro y de forma estándar
- Una vez llevado a producción los cambios realizados, no se hacen pruebas de las aplicaciones críticas del negocio.
- No hay una política que desaliente el cambio a los paquetes de Software que se encuentran funcionando. Por el contrario, se tiende a hacer los cambios sobre ellos.
- No se realiza formalmente una prueba de seguridad. Sólo se realizan pruebas de funcionalidad.
- Los datos de prueba son tomados directamente de los datos reales de producción.

Recomendaciones

- Debe crearse un formato o un check list, que los desarrolladores cumplan para asegurar el cumplimiento en requisitos de seguridad.
- Debe crearse un documento con reglas estándares, basado en las buenas prácticas de desarrollo de aplicaciones, el cual deben respetar y seguir los desarrolladores.
- Debe existir un responsable de desarrollo, que dirija el equipo y verifique que los desarrollos cumplan con los estándares establecidos.
- Debe crearse un formato o check list, que garantice el correcto funcionamiento de las aplicaciones existentes.
- Debe evitarse al máximo realizar cambios en los paquetes, funciones y procedimientos que se encuentran funcionando correctamente. Lo mejor, es crear un nuevo paquete que haga las nuevas tareas.

7.8 Gestión de incidentes de seguridad de la información

Se debe asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Como resultado de la evaluación se encontró:

- No se encuentra establecido un procedimiento que asegure una respuesta rápida, eficaz y metódica a los incidentes de seguridad
- No hay establecido un proceso formal para informar los incidentes de seguridad que se puedan presentar

- Los empleados reportan las debilidades observadas, pero no existe una bitácora que permita hacer seguimiento al tratamiento de las mismas

- Al presentarse cualquier evento que afecte la seguridad de la información, este es atendido de forma inmediata, pero no existe una clasificación que permita calificar el evento.

- No existe un procedimiento claramente establecido, que indique la forma en que se debe actuar en un incidente de seguridad

- Al presentarse un incidente de seguridad, no existe un formato donde se registre un paso a paso de la forma en que se solucionó el incidente.

Recomendaciones

En caso de incidentes de seguridad, que son aquellas situaciones no previstas e indeseadas que ponen en tela de juicio la seguridad de la información depositada en la empresa, debe actuarse de la siguiente forma:

- Debe establecerse un claro mecanismo para informar un incidente. Este puede ser por vía telefónica, por correo electrónico o por alguna herramienta específica para incidentes. También debe ser claro a quién o quienes comunicar el incidente

- Deben establecerse unos criterios claros que permitan clasificar el incidente, de manera segura y sin equivocaciones. De acuerdo a su clasificación, se estima el tiempo que llevará solucionar el incidente.

- Una vez resuelto el incidente, debe documentarse el tratamiento dado, e informar nuevamente la solución del mismo.

- Debe crearse una base de conocimiento con los incidentes y el tratamiento dado, para saber cómo actuar, de forma rápida y segura, en incidentes futuros similares.

7.9 Continuidad de seguridad de la Información

La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas.

Como resultado de la evaluación se encontró:

- La empresa El Apostador tiene establecido un plan de continuidad de seguridad de la información, pero no ha creado un procedimiento formal para dicha situación
- No existe una documentación, ni una implementación de los procedimientos que aseguren la continuidad de la información.
- No existe un procedimiento establecido para evaluar la puesta en marcha de la continuidad del negocio

Recomendaciones

En caso de catástrofe, donde se deban activar los planes de continuidad del negocio, la empresa debe tener en cuenta lo siguiente:

- Definir e implementar un procedimiento que permita tener acceso a los recursos financieros necesarios para la atención de incidentes.
- Evaluar la posibilidad de contar con un fondo de reserva que permita la disposición de recursos financieros en momentos de crisis.
- Definir un responsable que se encargue de coordinar las distintas actividades en relación a la continuidad del negocio.

- Tener plenamente identificado el personal que ocupa puestos estratégicos o claves dentro de la compañía y definir el personal que pueda asumir dichos cargos en caso de emergencia.
- Definir planes de recuperación tecnológica, teniendo en cuenta tiempos de respuesta y equipos de recuperación.
- Debe tenerse al día, el plan de restauración de copias de seguridad y puesta en marcha de sistemas alternos.
- Definir uno o varios sitios alternos que permitan restablecer los servicios en el tiempo posible.

7.10 Plan de Capacitación

El éxito de cualquier política o procedimiento que se implemente en la empresa El Apostador (y en cualquier empresa) es un programa de capacitación adecuado a todo el personal involucrado.

De igual forma, se debe hacer un seguimiento constante y periódico para programar refuerzos en la capacitación al personal.

No se observó dentro del programa de capacitaciones temas relacionados a la seguridad de la información, así como formación a nuevos desarrollos.

Recomendaciones

El plan de capacitación, debería contener por lo menos:

- Detectar las necesidades
- Determinar los objetivos de la capacitación

- Elaborar el plan de capacitación
- Ejecutar el plan
- Evaluar los resultados
- Repetir todos los pasos, de acuerdo a los resultados

7.11 Visita a las Instalaciones del Centro de Cómputo

Mediante la técnica de la observación y utilizando el criterio del estándar ANSI/TIA/EIA-942, se encontró lo siguiente:

A pesar que las instalaciones del Centro de Cómputo cuentan con estándares básicos de seguridad física, se observaron las siguientes situaciones a mejorar:

- Presencia de Centro de cableado eléctrico en el Centro de Cómputo.
- Los aires acondicionados son convencionales y no de precisión, los cuales no cuentan con cronogramas de mantenimiento.
- No se identifica un aislante eléctrico o piso falso.
- Un rack abierto y con presencia de polución.
- Presencia de cajas en el Centro de Cómputo.
- No existe una bitácora que registre las fallas que se detectan a equipos

Las anteriores situaciones obedecen posiblemente a que el Centro de Cómputo no contó con un diagnóstico previo, ni tampoco con especificaciones técnicas para su diseño.

Recomendaciones:

- Estudiar la posibilidad de instalar las UPS y toda su infraestructura en otro cuarto o hacer una separación del actual.
- Debido a que la estructura física no permite la instalación de piso y techo falso, se recomienda adecuar las paredes con aislante eléctrico y pintura anti fuego. Así mismo, evitar conexiones que generen cargas electrostáticas sobre el suelo.
- Propender porque los racks se encuentren cerrados para evitar el ingreso de polvo u otros agentes contaminantes.
- Realizar mantenimientos periódicos a los elementos tecnológicos que hacen parte del Centro de Cómputo.
- Adquirir aires de precisión con manejo del aire caliente y recirculación del aire frio.
- Disponer de un espacio dentro de la Empresa para almacenar los empaques y cajas de los equipos adquiridos para dar mayor espacio y retirar objetos ajenos al Centro de Cómputo.
- Llevar una bitácora adecuada de los eventos presentados que debe ser diligenciada por personal idóneo.

A continuación, se presenta la evidencia fotográfica:

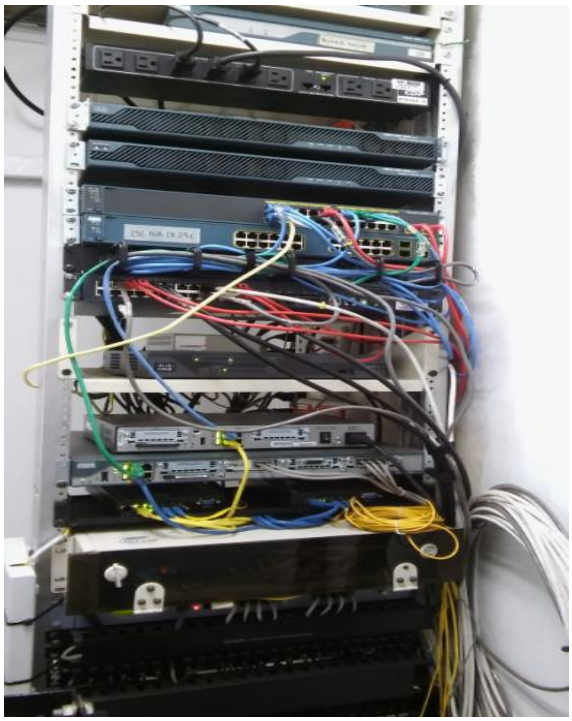

Ilustración 10. Rack abierto.

Ilustración 11. Instalación eléctrica dentro del Centro de Cómputo.

Ilustración 12. Presencia de objetos ajenos al Centro de Cómputo.

Ilustración 13. Ausencia de piso falso.

Conclusiones

Mediante el diseño y la aplicación de los instrumentos a la Empresa El Apostador, se logró un acercamiento al equipo de sistemas y un entendimiento global del estado actual de la seguridad de la información.

La evaluación realizada a la empresa El Apostador, permitió identificar los dominios de la norma ISO/IEC 27001 que presentan falencias o debilidades, que dejan expuesta la seguridad de la información, lo que hace necesario la implementación de acciones correctivas.

Tomando los resultados con calificación inexistente, bajo y muy bajo de los dominios evaluados, se identificaron las falencias y sobre las mismas, se establecieron recomendaciones que permitirán que la empresa pueda minimizar la materialización del riesgo mediante la formulación de controles correctivos.

Recomendación General

Las situaciones identificadas en la evaluación realizada al Centro de Cómputo de la empresa El Apostador, relacionadas con las debilidades de control de los dominios de la norma ISO/IEC 27001 y el estándar ANSI/TIA/EIA, deben ser revisadas mediante una metodología de análisis de causas propia, que asegure la identificación de acciones eficaces y efectivas para el adecuado funcionamiento del Sistema de Gestión de Seguridad de la Información, tanto a los activos de información del Centro de Cómputo, como a todos los procesos de la Empresa.

Se resalta que las recomendaciones dadas a conocer por cada dominio de la norma ISO/IEC 27001 y el estándar ANSI/TIA/EIA, le permitirán a la Empresa El Apostador, fortalecer los controles de seguridad de la información y minimizar el impacto del riesgo Afectación a la integridad, confidencialidad y disponibilidad de la información, asegurando así, la continuidad del negocio.

Referencias

Definicion Org. (s.f.). Definicion de Control. Obtenido de http://www.definicion.org/control

Congreso de la Republica . (2000). Código Penal Colombiano. Articulo 345. Financiación del terrorismo y de grupos de delincuencia organizada y administración de recursos relacionados con actividades terroristas y de la delincuencia organizada. Capítulo I. Título XII. Bogota : Leyer.

Congreso de la Republica. (2000). Código Penal Colombiano. Artículo 323. Lavado de Activos. Capítulo V. Titulo X. Bogota: Leyer.

ISO/ IEC 27004. (2009). Obtenido de Gestion de la Seguridad de la Informacion - Medicion : Obtenido de http://www.iso27001security.com/html/27004.html

ISO/ IEC 27005. (2001). Tecnologia de la Informacion. Tecnicas de seguridad- Gestion de riesgos de la seguridad de la informacion. Obtenido de Obtenido de http://www.iso27001security.com/html/27005.html

ISO/IEC 27002. (2013). Tecnologia de la Informacion- Tecnicas de Seguridad. En Código de prácticas para los controles de seguridad de la información .

ISO/IEC 27003. (2010). Obtenido de Obtenido de http://www.iso27001security.com/html/27003.html

ISOTools Colombia. (25 de Agosto de 2016). www.isotools.com.co. Obtenido de Obtenido de http://www.isotools.com.co/clasificar-la-informacion-segun-iso-27001/

Kosutic, D. (2015). ISO 27001 & ISO 22301. Obtenido de

http://www.iso27001standard.com/es/blog

Ministerior de las TIC. (2009). www.mintic.gov.co. Obtenido de Ley 1273: Obtenido de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Naranjo, A. (2009). Conceptos de la Auditoría de Sistemas. En N. A., Conceptos de la Auditoría de Sistemas (pág. 31). Bogotá: El Cid.

PWC. (2016). Resultados de la Encuesta Global de Seguridad de la Información.

Uptime Institute. (s.f.). Mapa de Certificaciones Tier. Obtenido de https://es.uptimeinstitute.com/TierCertification/certMaps.php

www.iso27000.es. (s.f.). Obtenido de ISO 27001: Obtenido de http://www.iso27000.es/iso27000.html

Apéndices

Apéndice A. Evaluación del Dominio A5

	**SGSI**						
	Herramienta para diagnosticar el nivel de madurez SGSI						Versión 01
A.5 Políticas de Seguridad de la Información							
A.5.1 Orientación de la dirección para la seguridad de la información							
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.5.1.1	Políticas para la seguridad de la información	La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información	NTC ISO-IEC 27001	3	3	3 - Medio	La Empresa el Apostador tiene definido políticas de seguridad de la Información, sin embargo, se observa que dentro de sus procesos no está documentado e implementado el de la seguridad de la información, lo que conlleva a tener controles no oficiales y ausencias de lineamientos y reglas de negocio claras.

A.5.1.2	Revisión de las políticas de seguridad de la información	**Control** Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continua.	NTC ISO-IEC 27001	1	1	1 - Muy bajo	No se observan soportes de una revisión periódica de políticas de seguridad. Tampoco hay evidencias de revisión de políticas debido a cambios significativos.

Apéndice B. Evaluación del Dominio A6

Auditores Externos	**SGSI**	
	Herramienta para diagnosticar el nivel de madurez SGSI	Versión 01

A.6 Organización de la Seguridad de la Información

A.6.1 Organización Interna

Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.

CÓDIGO	ASPECTO A EVALUAR	CONTROL	CRITERIO	CALIFICACIÓN			EVIDENCIA
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.	NTC ISO-IEC 27001	1	1	1 - Muy bajo	No se observó un documento con los roles definidos y una matriz de incompatibilidades para facilitar una adecuada segregación de funciones. Ausencia de un procedimiento para autorizar la asignación de permisos y su retiro de los sistemas de información y demás accesos a la información.
A.6.1.2	Segregación de funciones	Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificación no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.	NTC ISO-IEC 27001	2	2	2 - Bajo	Aunque existe una segregación de funciones dentro de la compañía, no se establece claramente la responsabilidad de la información al funcionario.

A.6.1.3	Contacto con autoridades	Se deben mantener los contactos apropiados con las autoridades pertinentes.	NTC ISO-IEC 27001			n - No aplica	
A.6.1.4	Contacto con grupos especiales de interés	Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.	NTC ISO-IEC 27001			n - No aplica	
A.6.1.5	Seguridad de Información en la gestión de proyecto	Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto	NTC ISO-IEC 27001			n - No aplica	
A.6.2 Dispositivo Móviles y trabajo remoto							
Objetivo: Garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.6.2.1	Política de dispositivos móviles	Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados el usar dispositivos móviles.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	No se observó un documento con las políticas y/o procedimientos que regulen el adecuado manejo de los diferentes dispositivos móviles. Se observa el manejo de portátiles por parte del personal técnico, sin control de salida y sin control de información
A.6.2.2	Trabajo remoto	Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.	NTC ISO-IEC 27001	1	1	1 – Muy Bajo	El acceso remoto en la empresa El Apostador, está prohibido. Sin embargo en situaciones extraordinarias se permite. Este acceso no tiene control, ni deja un rastro en el sistema, que facilite detectar las actividades realizadas.

Apéndice C. Evaluación del Dominio A7

	SGSI						
	Herramienta para diagnosticar el nivel de madurez SGSI					Versión 01	
A.7 Seguridad ligada a los recursos humanos							
A.7.1 Previo al empleo							
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.7.1.1	Selección	Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.	NTC ISO-IEC 27001	5	5	5 - Muy Alto	Existe una política de calidad en Recurso Humano, que obliga la revisión de antecedentes de cada aspirante. Adicionalmente, se hace nuevamente la revisión de antecedentes de forma periódica.
A.7.1.2	Términos y condiciones de la relación laboral	Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.	NTC ISO-IEC 27001	4	4	4 - Alto	Se observa un formato de confidencialidad, que todos los empleados y contratistas deben firmar, comprometiéndose a cumplir.
A.7.2 Durante el empleo							
Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**

A.7.2.1	Responsabilidades de la dirección	La dirección debe solicitar a todos los empleados y contratistas que aplique la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	NTC ISO-IEC 27001	4	4	4 - Alto	Se observa un formato de confidencialidad, que todos los empleados y contratistas deben firmar, comprometiéndose a cumplir.
A.7.2.2	Concientización, educación y formación en seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales pertinentes para su función laboral	NTC ISO-IEC 27001	3	3	3 - Medio	Aunque se realizan capacitaciones, no se evidencia una capacitación regular por parte de la compañía, en lo referente a seguridad de la información.
A.7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal sabido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información	NTC ISO-IEC 27001	3	3	3 - Medio	Los procesos disciplinarios son decididos por el Gerencia General, sin que exista un procedimiento establecido o estandarizado, que indique las acciones a tomar hacia los empleados por su falta.
A.7.3 Desvinculación y cambio de empleo							
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.7.3.1	Responsabilidades en la desvinculación o cambio del empleo	Se deben definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral.	NTC ISO-IEC 27001	3	3	3 - Medio	Al momento de contratación de un funcionario, se le hace firmar el formato de confidencialidad de información. Sin embargo, durante su estadía en el trabajo, muy pocas veces o nunca se les recuerda la confidencialidad y tampoco se menciona o se firma algún documento, sobre confidencialidad, al momento del retiro del empleado. La Empresa no ha contemplado establecer procedimientos disciplinarios por faltas recurrentes a la confidencialidad de la información a sus empleados.

Apéndice D. Evaluación del Dominio A8

	SGSI						
	Herramienta para diagnosticar el nivel de madurez SGSI					Versión 01	
A.8 Administración de activos							
A.8.1 Responsabilidad por los activos							
Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.8.1.1	Inventario de activos	Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos.	NTC ISO-IEC 27001	3	3	3 - Medio	Se observa un inventario de los activos de la empresa, pero de forma general. No existe un inventario separado que relacione sólo los activos que tienen que ver con el procesamiento de la información y que estén vinculados directamente con el Centro de Cómputo
A.8.1.2	Propiedad de los activos	Los activos que se mantienen inventario deben pertenecer a un dueño.	NTC ISO-IEC 27001	4	4	4 - Alto	De acuerdo al informe de Inventario observado, todos los activos tienen un responsable directo. En el caso del Centro de Cómputo, dicha responsabilidad recae sobre el Director de Sistemas.

A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	No se observa un documento que defina las reglas para el uso de la información, ni para los activos relacionados con el manejo de la misma.
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la información de su relación laboral contrato o acuerdo	NTC ISO-IEC 27001	5	5	4 -Muy Alto	Se observa un formato que relaciona la entrega formal del puesto y de los activos manejados por el empleado, en el momento de cesar su relación laboral con la empresa.
A.8.2 Clasificación de la información							
Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autorización.	NTC ISO-IEC 27001	0	0	0 - Inexistente	No se observa un documento que defina la clasificación de la información.
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización	NTC ISO-IEC 27001	0	0	0 - Inexistente	Al no existir una clasificación de la información, tampoco existe un documento que etiquete la información.

A.8.2.3	Manejo de activos	Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización	NTC ISO-IEC 27001	0	0	0 - Inexistente	Al no existir una clasificación de la información, tampoco existe un procedimiento para el manejo de activos de acuerdo a la clasificación de la misma.
A.8.3 Manejo de los medios							
Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.8.3.1	Gestión de los medios removibles	Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.	NTC ISO-IEC 27001	3	3	3 - Medio	Existe una política de control y manejo de medios removibles, sin embargo, en el área de Sistemas, estos controles son saltados por el personal.
A.8.3.2	Eliminación de los medios	Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe una política para el desecho de medios removibles, en la cual el departamento técnico, se asegura de eliminar toda la información existente en ellos.
A.8.3.3	Transferencia física de medios	Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.	NTC ISO-IEC 27001			n - No Aplica	

Apéndice E. Evaluación del Dominio A9

	SGSI						
	Herramienta para diagnosticar el nivel de madurez SGSI					Versión 01	
A.9 Control de Acceso							
A.9.1 Requisitos de negocios para el control de acceso							
Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe una política de Control de Acceso a la información y a las áreas de procesamiento de información
A.9.1.2	Accesos a las redes y a los servicios de la red	Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.	NTC ISO-IEC 27001	4	4	4 - alto	Existe un control de acceso a la red y a sus servicios.
A.9.2 Gestión de acceso del usuario							
Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**

A.9.2.1	Registro y cancelación de registro de usuario	Se debe implementar un proceso de registro y cancelación de registros de usuario para habilitar la asignación de derechos de acceso	NTC ISO-IEC 27001	4	4	4 - Alto	todo usuario del sistema, debe estar previamente registrado, para poder asignarle permisos de acceso al sistema
A.9.2.2	Asignación de acceso de usuario	Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o renovar los derechos de acceso para todos los tipos de usuario a todos los sistemas y servicios.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un procedimiento establecido para la asignación y remoción de permisos de acceso a los usuarios.
A.9.2.3	Gestión de derechos de acceso privilegios	Debe existir un procedimiento que restrinja y controle los derechos de acceso privilegiado	NTC ISO-IEC 27001	3	3	3 - Medio	Los accesos son asignados de acuerdo a la consideración personal del director de sistemas de turno. No existe un procedimiento establecido que restrinja o controle los accesos privilegiados.
A.9.2.4	Gestión de información secreta de autorización de usuarios	Debe existir un procedimiento de gestión formal que controle la asignación de autenticación secreta de usuarios	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	No se observa un procedimiento establecido que controle la autenticación secreta de los usuarios
A.9.2.5	Revisión de los derechos de acceso de usuario	Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares	NTC ISO-IEC 27001	3	3	3 - Medio	Se hace de forma irregular, una revisión de derechos de acceso a los usuarios del sistema.
A.9.2.6	Eliminación o ajuste de los derechos de acceso	Los derechos de acceso de los empleados y terceros, deben cancelarse al terminar su relación laboral o debe ajustarse cuando se hagan cambios	NTC ISO-IEC 27001	3	3	3 - Medio	Existe un procedimiento de cancelación de permisos y usuarios cuando cesa la relación laboral. Sin embargo, al hacerse cambios internos, no se revisan, ni ajustan los permisos de accesos existentes.
A.9.3 Responsabilidades del usuario							
Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**

A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.	NTC ISO-IEC 27001	3	3	3 - Medio	Existe una política de autenticación secreta, pero funciona sólo para los usuarios administrativos ya que los usuarios que son vendedores, utilizan una misma clave para ingresar al sistema.
A.9.4 Control de acceso al sistemas y aplicaciones							
Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.9.4.1	Restricciones de acceso a la información	Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.	NTC ISO-IEC 27001	4	4	4 - Alto	El acceso a la información se encuentra controlado por el aplicativo y por los permisos de acceso dados por la Base de Datos.
A.9.4.2	Procedimientos de inicio de sesión seguro	Cuando lo exige la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro	NTC ISO-IEC 27001			n - No Aplica	
A.9.4.3	Sistemas de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	NTC ISO-IEC 27001	3	3	3 - Medio	Se observó un control a la Base de Datos, que no permite la repetición de contraseñas y un cambio obligatorio cada 3 meses. No obstante, no existe una política de gestión de contraseñas, ni hay capacitación a los usuarios al respecto.
A.9.4.4	Uso de programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que puedan estar en capacidad de anular el sistema y los controles de aplicación.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe una política de control de programas ajenos o no autorizados por la compañía, que es controlada por medio de restricciones del sistema, administrada por el servidor de Acceso.
A.9.4.5	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	No existe un control de acceso al código fuente de los programas por parte de los desarrolladores.

Apéndice F. Evaluación del Dominio A10

	SGSI					
	Herramienta para diagnosticar el nivel de madurez SGSI					Versión 01
A.10 Criptografía						
A.10.1 Controles criptográficos						
Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad autenticidad o integridad de la información						
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**		**EVIDENCIA**
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NTC ISO-IEC 27001		n - No Aplica	

A.10.1.2	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.	NTC ISO-IEC 27001			n - No Aplica	

Apéndice G. Evaluación del Dominio A11

Auditores Externos	**SGSI**	
	Herramienta para diagnosticar el nivel de madurez SGSI	Versión 01

A.11 Seguridad física y del ambiente

A.11.1 Áreas seguras

Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información en la organización

CÓDIGO	ASPECTO A EVALUAR	CONTROL	CRITERIO	CALIFICACIÓN			EVIDENCIA
A.11.1.1	Perímetro de seguridad física	Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un perímetro bien definido y controlado que contiene el Centro de Cómputo de la empresa el Apostador.
A.11.1.2	Controles de acceso físico	Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que dolo se permite el acceso a personal autorizado.	NTC ISO-IEC 27001	4	4	4 - Alto	El Centro de Cómputo está dentro del departamento de Sistemas, al cual sólo se ingresa a través de una tarjeta magnética y una lectura de huella dactilar. Una vez dentro, para ingresar al Centro de Cómputo, debe desactivarse un seguro electrónico, por medio de un control remoto, que se encuentra guardado en un cajón bajo llave.

A.11.1.3	Seguridad de oficinas, salas e instalaciones	Se debe implementar un proceso de registro y cancelación de registros de usuario para habilitar la asignación de derechos de acceso	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	Al ingresar a las instalaciones de la empresa el Apostador, sólo se da un carnet que debe portar el visitante.
A.11.1.4	Protección contra amenazas externas y del ambiente	Se debe diseñar y aplicar la protección física contra daños por desastres naturales, ataque malicioso o accidental.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	Las instalaciones cuentan únicamente con un sistema de detección de incendios, pero no tiene un sistema de apagado automático. Este debe hacerse de forma manual con extintores dispuestos para el caso
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.	NTC ISO-IEC 27001			n - No Aplica	
A.11.1.6	Áreas de entrega y carga	Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas pueden acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.	NTC ISO-IEC 27001			n - No Aplica	
A.11.2 Equipamiento							
Objetivo: Prevenir pérdidas, daños, hurtos o el compromiso de los archivos así como la interrupción de las actividades de la organización.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.11.2.1	Ubicación y protección del equipamiento	El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionales por amenazas y peligros ambientales y oportunidades de acceso no autorizado.	NTC ISO-IEC 27001	4	4	4 - Alto	Los servidores y elementos activos, se encuentran dentro del Centro de Cómputo
A.11.2.2	Elementos de soporte	Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte	NTC ISO-IEC 27001	4	4	4 - Alto	La empresa cuenta con una Planta eléctrica Diesel, con capacidad y autonomía suficiente para mantener el funcionamiento básico de la compañía. Además, se cuenta con UPS que mantienen el funcionamiento de los equipos de los usuarios, mientras entra en funcionamiento la Planta eléctrica.

A.11.2.3	Seguridad en el cableado	Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de información contra interceptación, interferencia o daños.	NTC ISO-IEC 27001	3	3	3 - Medio	El cableado que se encuentra dentro de las instalaciones, se considera protegido. Sin embargo, la comunicación inalámbrica entre las antenas y los diferentes puntos de venta, puede ser blanco de interceptaciones.
A.11.2.4	Mantenimiento del equipamiento	El equipamiento debe recibir el mantenimiento correcto para asegurar su permanencia, disponibilidad e integridad.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un cronograma de mantenimiento de los equipos de cómputo de la compañía.
A.11.2.5	Retiro de activos	El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un procedimiento formal para el retiro de activos
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajo fuera de las instalaciones de la organización.	NTC ISO-IEC 27001	4	4	4 - Alto	Todos los activos de la compañía se encuentran asegurados.
A.11.2.7	Seguridad en la reutilización o descarte de equipos	Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado, se hayan removido o se haya sobre escrito con seguridad de su descarte o reutilización.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un procedimiento formal para el borrado de discos en caso de descarte de activos o de reutilización
A.11.2.8	Equipo de usuario desatendido	Los usuarios se deben asegurar de que los equipos desatendidos se les da protección apropiada.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe una política establecida por el sistema, que bloquea el equipo desatendido en 3 minutos.
A.11.2.9	Política de escritorio y pantalla limpios	Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe la política de las 5S, que todos los usuarios de la compañía deben aplicar.

Apéndice H. Evaluación del Dominio A12

Auditores Externos	**SGSI**	
	Herramienta para diagnosticar el nivel de madurez SGSI	Versión 01

A.12 Seguridad de las operaciones

A.12.1 Procedimientos, operaciones y responsabilidades

Objetivo: Asegurar la operación correcta y asegura de las instalaciones de procesamiento de información

CÓDIGO	ASPECTO A EVALUAR	CONTROL	CRITERIO	CALIFICACIÓN			EVIDENCIA
A.12.1.1	Procesamientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	NTC ISO-IEC 27001	2	2	2 - Bajo	No se encuentra documentación referente a los procedimientos de operación de los activos del Centro de Cómputo
A.12.1.2	Gestión de cambios	Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afectan la seguridad de la información.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un procedimiento formal para la gestión de Cambios en el sistema.
A.12.1.3	Gestión de la capacidad	Se debe supervisar y adaptar el uso de los recursos y se debe hacer proyecciones de los fututos requisitos de capacidad para asegurar el desempeño requerido del sistema.	NTC ISO-IEC 27001	4	4	4 - Alto	Aunque no se encuentra formalizado el procedimiento, si se hace un adecuado uso de recursos y se proyecta la capacidad de los mismos
A.12.1.4	Separación de los ambientes de desarrollo, prueba y operaciones	Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.	NTC ISO-IEC 27001	4	4	4 - Alto	Actualmente se encuentran separados los ambientes de Desarrollo y Producción.

A.12.2 Protección contra código malicioso							
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.12.2.1	Controles contra código malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse contra código malicioso junto con los procedimientos adecuados para concientizar a los usuarios.	NTC ISO-IEC 27001	4	4	4 – Alto	La compañía cuenta con un licenciamiento de un software especializado contra Malware.
A.12.3 Respaldo							
Objetivo: Proteger en contra de pérdida de datos							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.12.3.1	Respaldo de información	Se deben hacer copias de respaldo y pruebas de la información del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordada.	NTC ISO-IEC 27001	3	3	3 - Medio	Existe evidencia que se realizan copias de seguridad, pero no hay evidencia de pruebas de recuperación de las mismas.
A.12.4 Registro y monitoreo							
Objetivo: Registrar eventos y generar evidencia							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.12.4.1	Registro de evento	Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	NTC ISO-IEC 27001	3	3	3 - Medio	En la Base de Datos se guarda una trazabilidad de acciones de usuario. Pero no se encuentra activada la funcionalidad de Auditoría. Por otra parte, no existe un registro de eventos negativos o caídas del sistema.

A.12.4.2	Protección de la información de registros	Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	No existe una protección contra alteraciones o accesos no autorizados
A.12.4.3	Registro del administrador y el operador	Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.	NTC ISO-IEC 27001	0	0	0 - Inexistente	No existe un control sobre las actividades del administrador del sistema
A.12.4.4	Sincronización de mejora	Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente horaria de referencia.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un Servidor de relojes centralizado, del cual dependen todos los equipos de la red
A.12.5 Control de software de operación							
Objetivo: Asegurar la integridad de los sistemas operacionales							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.12.5.1	Instalación del software en sistemas operacionales	Se deben implementar los procedimientos para controlar la instalación de software en los sistemas operacionales	NTC ISO-IEC 27001	4	4	4 - Alto	Existe una política de control de instalación de software, controlado por restricciones del sistema
A.12.6 Gestión de la vulnerabilidad técnica							
Objetivo: Evitar la explotación de las vulnerabilidades técnicas							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**

A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.	NTC ISO-IEC 27001	0	0	0 - Inexistente	No existe un informe que determine las vulnerabilidades técnicas de los sistemas; por lo tanto, tampoco existe un plan de medidas para atacar el riesgo.
A.12.6.2	Restricciones sobre la instalación de software	Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios	NTC ISO-IEC 27001	4	4	4 - Alto	Existe una política de control de instalación de software, controlado por restricciones del sistema
A.12.7 Gestión de la vulnerabilidad técnica							
Objetivo: Evitar la explotación de las vulnerabilidades técnicas							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.12.7.1	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoría que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio.	NTC ISO-IEC 27001	0	0	0 - Inexistente	No existe una actividad de auditoría que verifique los sistemas operacionales.

Apéndice I, Evaluación del Dominio A13

	SGSI						
	Herramienta para diagnosticar el nivel de madurez SGSI						Versión 01
A.13 Seguridad de las comunicaciones							
A.13.1 Gestión de la seguridad de red							
Objetivo: Asegurar la operación correcta y asegura de las instalaciones de procesamiento de información							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.13.1.1	Controles de red	Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones	NTC ISO-IEC 27001	4	4	4 - Alto	Las redes se encuentran controladas y protegidas
A.13.1.2	Seguridad de los servicios de red	Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros	NTC ISO-IEC 27001	4	4	4 - Alto	Las redes se encuentran controladas y protegidas
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes	NTC ISO-IEC 27001	4	4	4 - Alto	La empresa cuenta con varias vlan que distribuyen los servicios y separan los diferentes usuarios
A.13.2 Transferencia de información							
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.							

CÓDIGO	ASPECTO A EVALUAR	CONTROL	CRITERIO	CALIFICACIÓN			EVIDENCIA
A.13.2.1	Políticas y procedimientos de transferencia de información	Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un procedimiento formal, para el intercambio de información con terceros
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben abarcar la transferencia segura de la información de negocio entre la organización y terceros.	NTC ISO-IEC 27002	4	4	4 - Alto	Existe un procedimiento formal, para el intercambio de información con terceros
A.13.2.3	Mensajería electrónica	La información involucrada en la mensajería electrónica debe ser debidamente protegida	NTC ISO-IEC 27003	4	4	4 - Alto	La mensajería electrónica es generada de forma automatizada, con la información necesaria.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Se deben identificar y revisar los requisitos de confidencialidad o acuerdos de no divulgación que refleja las necesidades de protección de la información de la organización.	NTC ISO-IEC 27004	4	4	4 - Alto	Existe un formato de confidencialidad entre las partes

Apéndice J. Evaluación del Dominio A14

Auditores Externos	**SGSI**	
	Herramienta para diagnosticar el nivel de madurez SGSI	Versión 01

A.14 Adquisición, desarrollo y mantenimiento del sistema

A.14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.

CÓDIGO	ASPECTO A EVALUAR	CONTROL	CRITERIO	CALIFICACIÓN			EVIDENCIA
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos y las mejoras para los de información existentes.	NTC ISO-IEC 27001	2	2	2 - Bajo	En los nuevos desarrollos, o en las mejoras realizadas a los sistemas de información existentes, no se aplica ningún requisito relacionado con la seguridad de la información
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, ys u divulgación y modificación no autorizada.	NTC ISO-IEC 27001			n - No Aplica	

A.14.1.3	Protección de las transacciones de servicios de aplicación	La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.	NTC ISO-IEC 27001			n - No Aplica	
A.14.2 Seguridad en procesos de desarrollo y soporte							
Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.14.2.1	Políticas de desarrollo seguro	Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.	NTC ISO-IEC 27001	2	2	2 - Bajo	No se encuentra un documento que defina las reglas para el desarrollo seguro y de forma estándar
A.14.2.2	Procedimientos de control de cambios del sistema	Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.	NTC ISO-IEC 27002	4	4	4 - Alto	Existe un procedimiento formal para la solicitud, desarrollo y puesta en producción de los cambios del sistema
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.	NTC ISO-IEC 27003	1	1	1 - Muy Bajo	Una vez llevado a producción los cambios realizados, no se hacen pruebas de las aplicaciones críticas del negocio.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación de sistema de información.	NTC ISO-IEC 27004	3	3	3 - Medio	A pesar de aplicar las buenas prácticas para el desarrollo, no se observa una documentación actualizada y completa del software

A.14.2.5	Principios de ingeniería de sistema seguro	Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta.	NTC ISO-IEC 27005	1	1	1 - Muy Bajo	No hay una política que desaliente el cambio a los paquetes de Software que se encuentran funcionando. Por el contrario, se tiende a hacer los cambios sobre ellos.
A.14.2.6	Entorno de desarrollo seguro	Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.	NTC ISO-IEC 27006	4	4	4 - Alto	Existe un ambiente de desarrollo adecuado, que permite el desarrollo de software de forma segura, con pruebas y cambios hasta la puesta en producción.
A.14.2.7	Desarrollo tercerizado	La organización debe supervisar y monitorear la actividad del desarrollo de sistemas tercerizado.	NTC ISO-IEC 27007			n - No Aplica	
A.14.2.8	Prueba de seguridad del sistema	Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad.	NTC ISO-IEC 27008	1	1	1 - Muy Bajo	No se realiza formalmente una prueba de seguridad. Sólo se realizan pruebas de funcionalidad
A.14.2.9	Prueba de aprobación del sistema	Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actuaciones y versiones nuevas.	NTC ISO-IEC 27009	4	4	4 - Alto	Existe un formato de aprobación del desarrollo de software, que es diligenciado junto con la persona que solicita el desarrollo
A.14.3 Datos de prueba							
Objetivo: Asegurar la protección de los datos usados para prueba.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.14.3.1	Protección de datos de prueba	Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	Los datos de prueba son tomados directamente de los datos reales de producción

Apéndice K. Evaluación del Dominio A15

	SGSI						
	Herramienta para diagnosticar el nivel de madurez SGSI						Versión 01
A.15 Relaciones con el proveedor							
A.15.1 Seguridad de la información en las relaciones con el proveedor							
Objetivo: Asegurar la protección de los activos de la organización a los que tiene acceso los proveedores							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de proveedor a los activos de la organización.	NTC ISO-IEC 27001			n - No Aplica	
A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	Todos los requisitos de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar y proporcionar componentes de infraestructura de TI para la información de la organización.	NTC ISO-IEC 27001			n - No Aplica	

A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones y la cadena de suministro de producto.	NTC ISO-IEC 27001			n - No Aplica	
A.15.2 Gestión de entrega del servicio del proveedor							
Objetivo: Mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos de proveedor.							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.15.2.1	Supervisión y revisión de los servicios del proveedor	Las organizaciones deben supervisar, revisar y auditar la entrega del servicio del proveedor.	NTC ISO-IEC 27001			n - No Aplica	
A.15.2.2	Gestión de cambios a los servicios del proveedor	Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluidos el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimiento y controles al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos.	NTC ISO-IEC 27002			n - No Aplica	

Apéndice L. Evaluación del Dominio A16

	SGSI	
	Herramienta para diagnosticar el nivel de madurez SGSI	Versión 01

A.16 Gestión de incidentes de seguridad de la información

A.16.1 Gestión de incidentes de seguridad de la información y mejoras

Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades

CÓDIGO	ASPECTO A EVALUAR	CONTROL	CRITERIO	CALIFICACIÓN			EVIDENCIA
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.	NTC ISO-IEC 27001	3	3	3 - Medio	Se encuentran responsables asignados a diferentes procedimientos, pero no hay establecidos procedimientos que aseguren una respuesta rápida y eficaz ante alguna eventualidad.
A.16.1.2	Informe de eventos de seguridad de la información	Se deben informar, lo antes posible los eventos de seguridad de la información mediante canales de gestión apropiados.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	No hay establecido un proceso formal para informar los eventos de seguridad que se puedan presentar
A.16.1.3	Informe de las debilidades de seguridad de la información	Se debe requerir que los empleados y contratistas que usan los sistemas y servicios de información de la organización, observen e informen cualquier debilidad en la seguridad de la información en los sistemas o servicios observada o que se sospeche.	NTC ISO-IEC 27001	2	2	2 - Bajo	los empleados reportan cualquier debilidad observada en el sistema, sin embargo no hay una bitácora formal, donde se pueda hacer seguimiento a estos hallazgos

A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	Al presentarse un evento que afecte la seguridad de la información, este es atendido, pero no existe una clasificación del evento.
A.16.1.5	Respuesta ante incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.	NTC ISO-IEC 27002	1	1	1 - Muy Bajo	Los incidentes de seguridad de la información, son atendidos, pero no existe ningún procedimiento establecido para ello.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.	NTC ISO-IEC 27003	3	3	3 - Medio	Al presentarse un evento que afecte la seguridad de la información, la manera en que se resuelve, queda en la mente del personal técnico. No queda un registro del tratamiento del problema.
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia.	NTC ISO-IEC 27004	3	3	3 - Medio	En un evento que afecte la seguridad de la información, la compañía hace la recolección de evidencias. Sin embargo no hay un repositorio de información que agrupe estos incidentes

Apéndice M. Evaluación del Dominio A17

Auditores Externos	**SGSI**	
	Herramienta para diagnosticar el nivel de madurez SGSI	Versión 01

A.17 Aspectos de seguridad de la información de la continuidad del negocio

A.17.1 Continuidad de la seguridad de la información

Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad de negocio de la organización.

CÓDIGO	***ASPECTO A EVALUAR***	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	NTC ISO-IEC 27001	3	3	3 - Medio	La compañía tiene establecido un plan de continuidad, para situaciones adversas. Sin embargo, aún no está definido del todo
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.	NTC ISO-IEC 27001	1	1	1 - Muy Bajo	No existe una documentación, ni una implementación de los procedimientos que aseguren la continuidad de la información
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debe verificar de manera periódica, los controles de continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas.	NTC ISO-IEC 27001	0	0	0 - Inexistente	No existe un procedimiento establecido para verificar y evaluar la continuidad de la información

A.17.2 Continuidad de la seguridad de la información

Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información

CÓDIGO	***ASPECTO A EVALUAR***	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**	**EVIDENCIA**

A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia para cumplir con los requisitos de disponibilidad.	NTC ISO-IEC 27001	4	4	4 - Alto	La compañía cuenta con redundancia en los elementos activos, para cumplir con la disponibilidad

Apéndice N. Evaluación del Dominio A18

	SGSI					
	Herramienta para diagnosticar el nivel de madurez SGSI					Versión 01
A.18 Cumplimiento						
A.18.1 Cumplimiento con los requisitos legales y contractuales						
Objetivo: Evitar incumplimiento de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.						
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**		**EVIDENCIA**
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	NTC ISO-IEC 27001	4	4	4 - Alto	La empresa cuenta con un departamento jurídico que cumple con los requisitos estatutarios y regulatorios que manda la ley
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados.	NTC ISO-IEC 27001	4	4	4 - Alto	La empresa cuenta con procedimientos que aseguran el respeto a los derechos de propiedad intelectual

A.18.1.3	Protección de los registros	Los registro se deben proteger contra pérdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	NTC ISO-IEC 27001	4	4	4 - Alto	La empresa cuenta con una política de conservación de datos de acuerdo a lo establecido por la ley
A.18.1.4	Privacidad y protección de la información de identificación personal	Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.	NTC ISO-IEC 27002	4	4	4 - Alto	La empresa asegura la privacidad de la información personal, de acuerdo a los requerimientos de ley.
A.18.1.5	Regulación de los controles criptográficos	Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes y regulaciones pertinentes.	NTC ISO-IEC 27003	0	0	0 - Inexistente	No existen controles criptográficos en la compañía
A.18.2 Revisiones de seguridad de la información							
Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información							
CÓDIGO	**ASPECTO A EVALUAR**	**CONTROL**	**CRITERIO**	**CALIFICACIÓN**			**EVIDENCIA**
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (Es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalo planificados, o cuando ocurran cambios significativos.	NTC ISO-IEC 27001	4	4	4 - Alto	Existe un proceso formal que permite revisar la gestión de seguridad de la información y se hace periódicamente

A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los gerentes deben revisar con regularidad el cumplimiento del procedimiento y los procedimientos de seguridad que están dentro de su área de responsabilidad de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.	NTC ISO-IEC 27001	4	4	4 - Alto	Los directores de cada departamento, se reúnen periódicamente para la revisión de los procedimientos de políticas de seguridad
A.18.2.3	Verificación del cumplimiento técnico	Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización.	NTC ISO-IEC 27001	4	4	4 - Alto	La empresa hace este tipo de verificaciones de forma periódica