AUDITORÍA A LOS PROTOCOLOS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICADOS EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO IBAL DE LA CIUDAD DE IBAGUÉ.

JOHN FREDDY LUGO LUNA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2017

AUDITORÍA A LOS PROTOCOLOS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICADOS EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO IBAL DE LA CIUDAD DE IBAGUÉ.

JOHN FREDDY LUGO LUNA

Proyecto de Grado para optar el título de Especialista en Seguridad Informática

Proyecto Aplicado

Director: Juan José Cruz Garzón

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2017

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Ibagué, 1 de Diciembre de 2017

DEDICATORIA

JOHN FREDDY LUGO LUNA

A dios que con su infinita misericordia me ha dado muchas bendiciones en la vida para poder lograr mis objetivos, a mis padres que con su apoyo incondicional no podría a ver llegado en el punto que estoy hoy en día y a mis hermanos que siempre son un gran apoyo para seguir.

AGRADECIMIENTOS

Los autores de este proyecto expresan sus más sinceros agradecimientos a:

Las directivas de la Universidad Nacional Abierta y a Distancia UNAD por brindar caminos y alternativas para poder prepararnos en esta disciplina tan importante como la seguridad informática.

Al Director del proyecto ingeniero Juan José Cruz Garzón, quien acompañó y dirigió el proceso de consolidación del proyecto.

TABLA DE CONTENIDO

Pag.

LISTA DE TABLAS

Pag.

LISTA DE ANEXOS

Pag.

RESUMEN

Con el fin de implementar una auditoría en forma práctica y efectiva, iniciando por la infraestructura misma hasta las políticas de manejo de datos y los protocolos de seguridad informática ejercidos actualmente en la empresa IBAL de la ciudad de Ibagué, siguiendo las normas técnicas, estándar internacionales de seguridad y calidad vigentes, sin olvidar los lineamientos éticos y legales vigentes a nivel nacional, tanto en la aplicación física como lógica de los recursos tecnológicos, además de considerar las características cualitativas adecuadas del recurso humano que asegurarán la efectividad de los protocolos; se establece el presente proyecto destinado a detectar, identificar, planear y rectificar los procesos actuales que implican la seguridad de la información durante la manipulación y almacenamiento de la misma. A través del desarrollo de la presente propuesta se catalogarán las vulnerabilidades detectadas y se determinarán pautas a seguir mediante la reingeniería de los protocolos actualmente en uso; para la planeación y ejecución definitiva de un óptimo plan de manejo de los recursos a disposición, que asegurará la integridad y seguridad de la información y sus procesos, así como de los estamentos que conforman la institución, garantizando la estabilidad, eficiencia, productividad y una proyección pública confiable de la empresa.

Palabras Clave: AUDITORÍA, PROTOCOLOS, POLÍTICAS, SEGURIDAD, VULNERABILIDAD.

INTRODUCCIÓN

Las políticas de seguridad informática aparecen como un conjunto de herramientas para concientizar a los funcionarios de las organizaciones sobre la significación y delicadeza de los sistemas informáticos, y los distintos servicios de carácter crítico que posibilitan la competitividad y crecimiento de la empresa.

Para ello las mismas empresas han generado nuevas políticas de seguridad informática, “debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual, lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información” [1].

La auditoría es un concepto muy amplio que se define como “la revisión y la evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes, del entorno informático de una entidad, abarcando todas sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, los controles existentes y el análisis de riesgos” [2].

Ante esta situación, las empresas deben implementar una auditoria en los protocolos de seguridad, estas prácticas requieren un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

El IBAL, empresa prestadora de servicio de agua y alcantarillado, posee políticas y algunos protocolos de seguridad informática que requieren ser constantemente evaluados; con el ánimo de detectar falencias y fortalezas, para tomar nuevas decisiones frente a los protocolos ejercidos.

Este trabajo está enfocado en evaluar los protocolos y sistemas de seguridad en los sistemas de información, con el fin de encontrar vulnerabilidades al momento tanto

[1] COLOMBIA. OFICINA DE PLANEACIÓN Y DIRECCIONAMIENTO ESTRATÉGICO SISTEMAS. Normas y políticas de seguridad informática (septiembre, 2013). Código de buenas prácticas para la gestión de la seguridad de la información. La oficina. Bogotá D.C., 2013 2 p.

[2] CRESPO GÓMEZ, Manuel y CAMACARO RIVAS, Mailen. Propuesta de una metodología de auditoría informática para la revisión de sistemas de información. [En línea]. Barquisimeto: Universidad Centroccidental “Lisandro Alvarado”. 2011., 57 p. Disponible en http://bibcyt.ucla.edu.ve/Edocs_Bciucla/Repositorio/TAQA76.9.A93C742011.pdf

de acceder como de administrar la información. Los aspectos que se tendrán en cuenta son:

Seguridad física, clasificación y análisis de la red: Esta fase de estudio de la red se realiza desde un nodo de conexión física a la red en análisis, y es considerada como intrusiva.

Detección de vulnerabilidades en protocolos, servicios, equipos y servidores: El objetivo de este paso, es realizar un listado de todas las posibles vulnerabilidades halladas para todos los equipos físicos y servicios lógicos detectados.

Seguridad de Usuario, accesos y almacenamiento de datos: En este paso se pretende obtener las contraseñas de acceso, otorgación de privilegios a usuarios, y el acceso a la totalidad de los datos incluyendo ubicaciones restringidas y la verificación del protocolo de copia de seguridad.

1. TÍTULO DEL PROYECTO

AUDITORÍA A LOS PROTOCOLOS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA APLICADOS EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO IBAL DE LA CIUDAD DE IBAGUÉ.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

La empresa de servicio de acueducto y Alcantarillado IBAL, prestadora de servicios públicos de almacenamiento, distribución, mantenimiento y protección del servicio de acueducto y alcantarillado, es una empresa pública altamente competitiva, consciente que se está en un ambiente de constante cambio, por ello la empresa IBAL ha implementado un sistema de seguridad y protocolos de información, que no ha sido evaluado, por ende se desconoce el nivel de vulnerabilidad y la eficacia de dichos protocolos de seguridad informática.

Respecto al seguimiento que se ha venido dando al problema de vulnerabilidad en seguridad informática y el establecimiento de políticas y protocolos para garantizar la misma, cabe citar el trabajo denominado: "Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor del Cauca"[3]. Sección del trabajo en la cual se relacionan los estándares y normas establecidas y utilizadas en el desarrollo del presente proyecto:

> Partiendo de la necesidad de determinar el estado de seguridad de la información mediante un diagnóstico en la institución Universitaria Colegio Mayor del Cauca, y en vista de que actualmente se tiene una estructura institucional con la dotación y tecnología necesarias para desarrollarlas, se plantea realizar el análisis de riesgos a partir de la revisión de algunos antecedentes en la materia.
> Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos (serie ISO/IEC 27000), y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información (por ejemplo, ISM3); sin embargo, en la especificación de los mismos no se afronta su aplicación a un grupo empresarial, lo cual requiere consideraciones adicionales. Existe una metodología en implantación de un SGSI para un grupo empresarial jerárquico[4], en donde se describe la importancia de implantar un SGSI que permita dotar de seguridad todos los procesos productivos de las empresas de cualquier tipo y tamaño, muestra una metodología clara para realizar análisis de riesgo en un ambiente empresarial.

[3] PERAFÁN RUIZ, John y CAICEDO CUCHIMBA, Mildred. Análisis de riesgos de la seguridad de la información para la Institución Univresitaria Colegio Mayor del Cauca. Trabajo de grado Especialista en Seguridad Informática. Popayán.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática, 2014.

[4] (Pallas Mega Gustavo, 2009) Metodología de Implantación de un SGSI [En línea]. Uruguay: Ing. Gustavo Pallas Mega 2009, Disponible en https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

Muchos de los planteamientos y problemas en seguridad informática se encaminan a protegerse contra accesos no autorizados, pero este es un problema sencillo de resolver, ya que durante años se han desarrollado y perfeccionado algoritmos matemáticos para el cifrado de datos, para el intercambio seguro de información, para garantizar el correcto funcionamiento del software, que se ha traducido en herramientas capaces de proporcionar soluciones rápidas y sencillas a problemas técnicos de seguridad. Desafortunadamente, no es suficiente simplemente arreglar los errores o eliminar las fallas técnicas de seguridad. El problema va mucho más allá. La Seguridad Informática es un problema cultural, en el que el usuario juega un rol protagónico. La metodología para el aseguramiento de entornos informatizados - MAEI[5], resalta la importancia de tener una metodología clara para realizar un análisis de riesgos e identificar claramente vulnerabilidades, riesgos y amenazas presentes en los activos de información, ser gestionados y que permita optimizar los procesos organizacionales.

De igual forma, también existen lineamientos establecidos en la norma internacional UNE/ISO 27001, que establece las especificaciones para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). Esta norma establece un enfoque por procesos basado en el ciclo Deming, que plantea la gestión de la seguridad como un proceso de mejora continua, a partir de la repetición cíclica de cuatro fases como lo son: planificar, hacer, verificar y actuar. Dentro de las especificaciones de la norma se establece un esquema documental del SGSI, que debe mantenerse actualizado, disponible y enmarcado en un índice, especialmente si la empresa desea superar un proceso de certificación, tal como lo describe un proceso de implantación de un SGSI, el cual expone claramente los lineamientos que deben seguirse para implantar un Sistema de Gestión de Seguridad de la Información en un entorno real, describiendo el proceso para realizar el análisis de riesgo y sus fases futuras[6].

[5] (INTECO) INTECO, Implantación de un SGSI en la empresa, Instituto Nacional de Tecnologías de la Comunicación [En línea], Disponible en https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

[6] PERAFÁN. Op. cit., p. 12-13.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles procesos de administración informática, protocolos y políticas de seguridad informática, deben ser sometidos a auditoría de seguridad, para ayudar a disminuir potencialmente las vulnerabilidades y amenazas en la empresa de acueducto y alcantarillado IBAL de Ibagué?

2.3 DESCRIPCIÓN DEL PROBLEMA

La empresa de Alcantarillado IBAL de Ibagué, ha presentado los siguientes síntomas perceptibles de debilidad que conllevan a la declaración de la necesidad de las Auditorías Externas: Síntomas de descoordinación y Desorganización (los objetivos del departamento de sistemas no coinciden con la misión de la empresa); síntomas de mala reputación e insatisfacción por parte de los usuarios; síntomas de inseguridad: Gestión de riesgos (seguridad lógica, seguridad física, confidencialidad; centro de procesamiento de datos con falencias de control). "Debido tanto a los problemas presentados y a las fallas de seguridad registradas, como al poco conocimiento que tienen las organizaciones del concepto de seguridad informática, se hace necesario descifrar este concepto, si se requiere de un documento adicional o de uno de más fácil aplicación por parte de las instituciones públicas, que facilite la comprensión de lo que es la seguridad informática, lo que esta implica y lo que conlleva el no tenerla implementada" [7].

Dentro de la observación realizada se descubrió:

- Ausencia considerable de inversión de presupuesto destinado para el desarrollo del departamento de sistemas. y la infraestructura informática de la empresa.

- Desconocimiento considerable en los niveles directivos de la empresa, sobre la grave situación informática de sus dependencias.

- Inexistencia parcial de seguridades lógicas y físicas, que permitan garantizar la integridad de los funcionarios, los equipos y la información.

- Hallazgo de fraudes informáticos efectuados en el pasado, y en ejecución de las mismas políticas y protocolos de seguridad.

- Falta de planeaciones informáticas fiables, y ausencia de documentación o documentación incompleta, referente a los sistemas que soportan el uso y mantenimiento de los sistemas en producción.

- La organización de la empresa no funciona como debería, ausencia de políticas fiables, objetivos a corto y largo plazo, seguimiento de normas, y

[7] GALEANO VILLA, Jorge y ALZATE CASTAÑEDA, Cristian. Protocolo de políticas de seguridad informática para las universidades de Risaralda. Trabajo de grado Profesional en Ingeniería de Sistemas y Telecomunicaciones. Pereira.: Universidad Católica de Pereira. Facultad de Ciencias Básicas e Ingeniería. Programa de Ingeniería de Sistemas y Telecomunicaciones, 2013. 13 p.

metodologías de trabajo, delegación de tareas y adecuada capacitación y administración del Recurso Humano.

- También se observó descontento general por parte de los usuarios. Debido al incumplimiento con las fechas asignadas, y la mala calidad de los servicios teleinformáticos.

3. JUSTIFICACIÓN

Las diferentes políticas de seguridad informática han aparecido como un conjunto de herramientas para concientizar a los funcionarios de las organizaciones sobre la significación y delicadeza de los sistemas informáticos, y de los servicios críticos de seguridad que posibilitan la competitividad y crecimiento de la empresa.

Por lo tanto, son las mismas empresas las encargadas de generar nuevas políticas de seguridad informática, políticas que a su vez han tomado un gran impulso al asegurar el establecimiento de protocolos confiables de seguridad.

Este proyecto es conveniente ya que permite disminuir las vulnerabilidades y amenazas mediante la aplicación de procesos de auditoría a los protocolos y políticas de seguridad informática en la empresa de acueducto y alcantarillado IBAL de Ibagué, la auditoria a los protocolos y políticas de seguridad informática aplicados en la empresa de acueducto y alcantarillado IBAL de la ciudad de Ibagué, permitirá la detección y corrección de falencias, asegurando la disminución de las posibilidades de pérdida de información, ataques cibernéticos y de terceros interesados en manipular la información que se maneja en el Instituto IBAL.

De igual forma, para administrar y garantizar el uso correcto de los sistemas de información, para dar una mayor certeza sobre la confiabilidad de estos y generando más y cada vez mejores resultados, reducción de inconvenientes a futuro y de costos a largo plazo.

Los beneficiarios directos del proyecto, son los treinta y siete (37) funcionarios del IBAL seccional Ibagué, éstos verán protegida la información de sus procesos asignados, y por ende se alejarán de la posibilidad de información fuera de contexto e irregular, de un escándalo resultante e investigaciones disciplinarias por fuga de información, ya que por ejemplo, si aparecen en los medios de comunicación datos reservados del proceso de un funcionario en particular, lo primero que se viene a la mente de todos, es que el funcionario lo hizo a propósito y se empezaría a especular sobre todo tipo de motivaciones, como corrupción o negligencia, que en resumen dañan la imagen del funcionario y de la Entidad en general.

De manera indirecta, los usuarios, que serán protegidos por la certeza de sus cuentas en los respectivos recibos de pago. Esto generará confianza en los usuarios sobre la seguridad y control de los servicios, aumentando la credibilidad de la ciudadanía al saber que sus instituciones están realizando auditorias de los procesos informáticos y sus bases de datos están protegidas.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Disminuir las vulnerabilidades y amenazas mediante la aplicación de procesos de auditoría a los protocolos y políticas de seguridad informática en la empresa de Acueducto y Alcantarillado IBAL de Ibagué.

4.2 OBJETIVOS ESPECÍFICOS

1. Establecer un diseño metodológico que permita la realización satisfactoria del proceso de auditoría a la seguridad informática de la empresa IBAL.

2. Determinar los activos computacionales y teleinformáticas utilizados en la empresa de acueducto y alcantarillado IBAL de Ibagué.

3. Identificar las vulnerabilidades, amenazas y riesgos de seguridad, y realizar el proceso de análisis y evaluación de los mismos para determinar los que tienen mayor impacto en la empresa.

4. Conocer los protocolos y políticas de seguridad informática de la empresa de acueducto y alcantarillado IBAL de Ibagué, y realizar una reingeniería del protocolo, para el diseño de una política confiable de seguridad informática.

5. Elaborar el informe de los hallazgos y recomendaciones para la aplicación de un sistema de control efectivo que posibilite la mitigación de los riesgos detectados, mediante la implementación de políticas y procedimientos aplicados a la seguridad de acuerdo a la norma ISO/IEC 27002.

5. PRODUCTO RESULTADO A ENTREGAR

Con base en el examen llevado a cabo en los activos físicos y lógicos de la empresa, se reconocerán las falencias de control y seguridad en todos los departamentos o dependencias de la misma, se realizará un informe preliminar, dicho informe será presentado al director de la Oficina de Sistemas y a la Gerencia General, para luego elaborar un informe final, el cual será entregado a la Gerencia General de la empresa de acueducto y alcantarillado IBAL.

Informe final de las observaciones y clasificaciones de los activos informáticos tanto físicos como lógicos en riesgo, para puntualizar y sugerir acciones, políticas o salvaguardas y protocolos de seguridad. Ayudando de esta forma a minimizar lo máximo posible, el eventual impacto en caso de materialización por alguna de las amenazas reveladas a través del proceso de gestión de seguridad.

Las recomendaciones consignadas en el informe final, con base en las falencias identificadas, y dependiendo de las posibilidades de realización de la empresa, se aconseja ser aplicadas en un plazo de máximo seis meses, y una vez que se hayan aplicado todas las sugerencias en cada uno de los departamentos de la empresa, estos deberán iniciar un proceso de evaluación.

6. MARCO REFERENCIAL

6.1 MARCO TEÓRICO

La seguridad de la Información, y el análisis de riesgos informáticos, se halla perfectamente definidos en el proyecto de gestión de seguridad informática de “John Perafán y Mildred Caicedo” [8], a continuación la transcripción de dicha sección:

> Se podría definir como seguridad de la información a un estado específico de la misma sin importar su formato, que nos indica un nivel o un determinado grado de seguridad de información, por ejemplo, que está libre de peligro, daño o riesgo, o por el contrario que es vulnerable y puede ser objeto de materialización de una amenaza. Las vulnerabilidades, el peligro o el daño de la misma es todo aquello que pueda afectar su funcionamiento directo y la esencia en sí de la información, o en su defecto los resultados que se obtienen de la consulta, administración o procesamiento de ella.
> Garantizar un nivel de protección total es virtualmente imposible[9], la seguridad de la información en la práctica a un nivel total o de completitud no es alcanzable porque no existe un sistema seguro al ciento por ciento. Existe un planteamiento denominado Desarrollo de una metodología para la auditoría de riesgos informáticos (físicos y lógicos) y su aplicación al departamento de informática de la dirección provincial de pichincha del consejo de la judicatura, donde se afirma que la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en cualquier tipo de idioma (ISO 2700) . Sistema de gestión de seguridad de la información. Términos de uso de información ISO 27000.es ©, 2012 conversación. “Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene”.
> La implementación de seguridad para los sistemas de información, protege a las organizaciones que la adoptan como parte de su visión y misión; brindándoles aseguramiento ante el amplio rango de amenazas existente actualmente, para respaldar efectivamente la continuidad y efectividad del negocio, minimizar los posibles daños y vulnerabilidades informáticas, y maximizar el retorno de las inversiones y las oportunidades para la organización. La información digital o en papel y los procesos que la apoyan, los sistemas y sus redes teleinformáticas, son importantes activos de la organización y por ello mismo deben ser resguardadas ante la posibilidad de cualquier tipo de amenaza.
> Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques intrusivos o

[8] PERAFÁN. Op. cit.
[9] (ISO 27000.es, 2005) El portal de ISO 27001 en Español [En línea]. ISO 27000.es. Disponible en http://www.iso27000.es/sgsi.html#home

de negación de servicios, se están volviendo cada vez más comunes, ambiciosas, sofisticadas y progresivamente peligrosas.
La seguridad de la información es importante en las instituciones tanto del sector público como del privado, para proteger sus infraestructuras teleinformáticas y los elementos críticos o delicados en el manejo de datos. En ambos sectores, la seguridad de la información, permitirá lograr la total seguridad de la manipulación electrónica de la información y, por ende, el mejoramiento o aumento del rendimiento del comercio electrónico, evitando y reduciendo los riesgos relevantes en estos medios. Es importante resaltar que el actual aumento en la interconexión de las redes públicas y privadas, y el compartir los recursos de información entre ellas, es un reto que aumenta así mismo, la dificultad de lograr el control total de los accesos y su respectiva seguridad.
Es necesario que exista seguridad en el activo más importante de la organización por las siguientes razones: gran variedad de Riesgos y Amenazas: fraudes, espionaje, sabotaje, vandalismo, incendio, inundación, hacking, virus, denegación de servicio, etc.; Provenientes de múltiples fuentes. Mayor vulnerabilidad a las amenazas por la dependencia de los sistemas y servicios de información interconectados. La mayoría de los sistemas de información no han sido diseñados para ser seguros.
Análisis de Riesgos Informáticos
Antes de definir lo que es el análisis de riesgos, tenemos que considerar lo que es un riesgo, a continuación, se expone la siguiente definición:
Según Fernando Izquierdo Duarte: “E R g, ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos” [10].

En cuanto al establecimiento de las normas y los estándares derivados de ellas, aplicables al presente trabajo debido a su efectividad y obligatoriedad legal, podemos continuar citando el trabajo aplicado a la “Institución Universitaria Colegio Mayor del Cauca” [11], debido a su similitud tanto práctica como contemporánea:

En la actualidad las empresas de carácter público y privado, son empresas que realmente invierten muy poco o nada en el aseguramiento tanto de sus recursos como de sus activos, incluyendo el más importante: La información. Al no implementar mecanismos de seguridad en las redes de computadores llevan no sólo a pérdidas sustanciales de dinero, sino a estar por fuera de las exigencias del mundo actual, la mayoría de las transacciones que involucran información se realizan a través de redes y el uso de internet.
Utilizar estándares como ISO27000[12], (específicamente un SGSI) contribuye a establecer procesos de reconocimiento y control en las áreas de una organización, dentro del área de sistemas se debe dar gran importancia a la creación y adaptación

[10] PERAFÁN. Op. cit. 14-16 p.
[11] Ibíd.
[12] (INTECO) Implantación de un SGSI en la empresa, Instituto Nacional de Tecnologías de la Comunicación [En línea], Disponible en https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

de mecanismos, políticas de procesos que permitan asegurar y mejorar la seguridad informática[13].

Respecto a las normativas y los métodos actuales para la realización de auditorías de seguridad informática, Verónica Quintuña expresa en su trabajo de "Auditoría Informática a la Superintendecia de Comunicaciónes"[14]:

> Normas, Técnicas, Estándares y Procedimientos de Auditoría: Actualmente el desarrollo de una auditoría informática se basa en la aplicación de normas, técnicas, estándares y procedimientos que garanticen el éxito del proceso. La gran mayoría de documentación existente coincide en que las normas de auditoría son requisitos mínimos de calidad, relativos a las cualidades del auditor, a los métodos y procedimientos aplicados en la auditoría, y a los resultados. (Aguirre, n. d. a). Las técnicas en cambio, son todos aquellos métodos que permiten al auditor evidenciar y fundamentar sus opiniones y conclusiones[15].

Igualmente, en dicho trabajo se encuentran relacionadas las normas que actualmente rigen los estándares de calidad para la realización de gestiones a la seguridad informática:

> Normas ISO ISO/IEC 27000. Las normas ISO/IEC 27000 constituyen una familia de estándares, desarrolladas por la International Organization for Standarization (ISO) y por la International Electrotechnical Commission (IEC). Esta familia de estándares se publicó ante la necesidad de contar con una base para la gestión de la seguridad de la información, especificando los requisitos para establecer, implementar, controlar, mantener e innovar un Sistema de Gestión de Seguridad de la Información (SGSI). La serie ISO 27000 está formada por varias normas. Son consideradas como normas base: ISO 27001 e ISO 27002, mientras que las normas complementarias son principalmente: ISO 27003, ISO 27004, e ISO 27005[5].
> ISO/IEC 20000. Proviene del estándar británico BS 15000. Es el primer estándar específico para la Gestión de Servicios de TI, y su objetivo es aportar los requisitos necesarios, dentro del marco de un sistema completo e integrado, que permita que una organización provea servicios TI gestionados, de calidad y que satisfagan los requisitos de la entidad. La norma ISO/IEC 20000 está estructurada en dos documentos:
> ISO/IEC 20000-1: Este documento de la norma incluye el conjunto de los "requisitos obligatorios" que debe cumplir el proveedor de servicios TI, para realizar una gestión eficaz de los servicios, que responda a las necesidades de las empresas y sus clientes.
> ISO/IEC 20000-2: Esta parte contiene un código de prácticas para la gestión de servicios que trata cada uno de los elementos contemplados en la parte 1, analizando y aclarando su contenido. En síntesis, este documento pretende ayudar a las

[13] PERAFÁN. Op. cit. 26 p.
[14] QUINTUÑA RODRÍGUEZ, Verónica. Auditoría Informática a la Superintendencia de Telecomunicaciones. Trabajo de grado Profesional en Ingeniería de Sistemas. Cuenca.: Universidad de Cuenca. Facultad de Ingeniería, 2012.
[15] Ibíd., 18 p.

organizaciones a establecer los procesos de forma que cumplan con los objetivos de la parte 1.
La norma ISO/IEC 20000 cubre las siguientes secciones: sistema de gestión de servicios TI, planificación e implementación de la gestión del servicio, planificación e implementación de servicios, nuevos o modificados, procesos de provisión de servicio, procesos de relaciones, procesos de resolución, procesos de control, y procesos de entrega[16].

6.2 MARCO CONCEPTUAL

"Amenaza. - Cualquier aspecto o escenario que pueda ocasionar que un riesgo se convierta en incidente, o sea, que llegue a realizarse"[17].

"Eficacia.- Capacidad de lograr el efecto que se desea o se espera"[18].

"Eficiencia.- Conjunto de atributos, que se refieren a las relaciones entre el nivel de rendimiento del software y, la cantidad de recursos utilizados bajo unas condiciones predefinidas"[19].

"Evidencia. - Es toda información que utiliza el AI, para determinar, si el ente o los datos auditados siguen los criterios u objetivos de la auditoría"[20].

"Integridad.- Consiste en que solo los usuarios autorizados pueden variar los datos"[21].

"Irregularidades. - Son las violaciones intencionales a una política gerencial establecida, declaraciones falsas deliberadas u omisión de información del área auditada o de la organización"[22].

---

[16] QUINTUÑA. Op. cit., p. 35-37.
[17] BARROS MARCILLO, Gabriela. Auditoría Informática de la Cooperativa de Ahorro y Crédito "Alianza del Valle" LTDA. Aplicando Cobit 4.0. Trabajo de grado Profesional en Ingeniería de Sistemas e Informática. Sangolquí.: Escuela Politécnica del Ejército. Dpto. de Ciencias de la Computación, 2012. 9 p.
[18] (Real Academia Española, 2017) Asociación de Academias de la Lengua Española, 2017 [En línea]. Disponible en http://dle.rae.es/?id=DgIqVCc
[19] (Real Academia Española, 2017) Asociación de Academias de la Lengua Española, 2017 [En línea]. Disponible en http://dle.rae.es/?id=DgIqVCc
[20] BARROS. Op. cit., p. 11.
[21] (Real Academia Española, 2017) Asociación de Academias de la Lengua Española, 2017 [En línea]. Disponible en http://dle.rae.es/?id=DgIqVCc
[22] (ERIKA, 2012) AUDITORÍA INFORMÁTICA DE LA COOPERATIVA DE AHORRO Y CRÉDITO "ALIANZA DEL VALLE" LTDA. APLICANDO COBIT 4.0, [En línea]. SANGOLQUÍ. Disponible en https://repositorio.espe.edu.ec/bitstream/21000/5197/1/T-ESPE-033091.pdf

“Pruebas de Cumplimiento. - Son aquellas evidencias que determinan (proporcionan evidencia de que) los controles claves existen y que son aplicables en forma efectiva y uniforme”[23].

“Pruebas Sustantivas. - Son aquellas que implican el estudio y evaluación de la información, por medio de comparaciones con otros datos relevantes”[24].

> Riesgo. - Posibilidad de que no puedan prevenirse o detectarse errores o irregularidades importantes.
> Riesgo inherente. - Existe un error que es significativo y se puede combinar con otros errores cuando no hay control.
> Riesgo de control. - Error que no puede ser evitado o detectado oportunamente por el sistema de control interno.
> Riesgo de detección. - Se realizan pruebas exitosas a partir de un procedimiento de prueba inadecuado[25].

6.3 MARCO LEGAL

Las normas que se encuentran relacionadas directamente con el presente proyecto de grado, serán relacionadas en su disposición he implementación en la jurisprudencia colombiana, cronológicamente a continuación:

- “La primera mención importante en la legislación colombiana, respecto a los medios y el manejo informático de la información, se hizo efectiva en la ley de protección de datos de 198826”[26].

- “Circular 052 de 25 de octubre de 2007, de la Superintendencia Financiera de Colombia. Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios”[27].

---

[23] BARROS. Op. cit., p. 14.
[24] Ibíd., p. 14.
[25] COLOMBIA. ALCALDÍA MUNICIPAL SIACHOQUE. Plan Anticorrupción y de Atención al Ciudadano. (2016). Administración Municipal 2016-2019. La Alcaldía. Siachoque., 2016. 35 p.
[26] (JURIDICA, 2015)Informática Jurídica, El derecho de autor con respecto al derecho a la libertad de la información [En línea]. Disponible en http://www.informatica-juridica.com/trabajos/el-derecho-de-autor-con-relacion-a-otros-derechos-especificos-de-la-sociedad-de-la-informacion/
[27] (JURIDICA, 2015)Informática Jurídica, Legislación informática de Colombia [En línea]. Disponible en http://www.informatica-juridica.com/legislacion/colombia/

- “Ley 1266 de 31 de diciembre de 2008, por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”. (Diario Oficial nº 47.219).

Específicamente relacionado con el presente proyecto, debido a la necesidad de dar el respectivo cumplimiento legislativo, a la protección de los bienes jurídicos tutelados por el estado, y la importancia que su naturaleza representa como lo es en este caso la información y sus tecnologías, tenemos la siguiente ley:

- “Ley 1273 de 5 de enero de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones” (Diario Oficial nº 47.223).

7. MARCO METODOLÓGICO

7.1 Tipo de investigación

El tipo de investigación específico, utilizado en el presente proyecto, es la investigación aplicada, la cual es un tipo de investigación enfocada en hallar los mecanismos o las estrategias que permitan alcanzar un objetivo específico, como lo es en este caso, auditar la seguridad informática de la empresa IBAL, para detectar las falencias de sus sistemas de seguridad, y brindar un diagnóstico encaminado a corregir dichos sistemas y mejorar las condiciones de seguridad de la empresa.

7.2 Metodología de investigación

Esta investigación se realiza desde el enfoque descriptivo y cuantitativo, ya que la información requerida para este caso se obtendrá por medio de listas de chequeos, entrevistas al talento humano y observación de los procesos de la empresa. Esto proporcionará el diagnóstico que permitirá identificar la situación de la empresa frente a los requisitos de la norma ISO/IEC 27001.

7.2.1 Metodología de Desarrollo

El desarrollo metodológico del presente proyecto, está basado fundamentalmente en el ciclo PHVA, “sus siglas significan en español (planificar, hacer, verificar, actuar) o en ingles según la ISO 27001 internacional (Plan, Do, Check, Act). Este ciclo es una metodología usada en la implementación de un sistema de gestión de la calidad, de tal manera que al aplicarla en la política y objetivos de calidad así como la red de procesos la probabilidad de éxito sea mayor” [28].

Para determinar los activos informáticos y de la información utilizados en la empresa de acueducto y alcantarillado IBAL de Ibagué, se contará con el instrumento de la observación y entrevista. El diseño metodológico que se plantea para el desarrollo de la presente gestión de seguridad, será casi idéntico al planteado en el trabajo realizado en la “Institución Universidad Colegio Mayor del Cauca” [29], debido a que en este caso, pese que se contará con la misma cantidad de etapas en el proceso, se realizará una menor cantidad de actividades para alcanzar las metas planteadas:

> …como parte del desarrollo de la investigación aplicada, se plantean a nivel general actividades que tratan de dimensionar y atacar el problema mencionado para brindar al final del proyecto las posibilidades que tiene la institución para adoptar un plan de mejora, de acuerdo a los resultados que se obtengan a partir del análisis de riesgos. Algunas de estas actividades se mencionan a continuación.
> Definición de los objetivos del proyecto y delimitación del alcance de acuerdo al problema planteado.
> Análisis de fuentes de datos y recopilación de información: Esta etapa busca recolectar la mayor cantidad de información posible con respecto al estado actual, estudios o proyectos que tengan relación con el análisis de riesgos y en general en materia de seguridad informática en la institución.
> Generación del plan de trabajo y establecimiento de plazos de tiempo: Esta actividad hace referencia a la generación de un cronograma de actividades a nivel general que establezca límites de tiempo y asignación de tareas para lograr el desarrollo del proyecto.
> Recolección de documentos organizacionales: Para realizar el análisis de riesgos es importante conocer el entorno y contexto en el que se basa la Institución objeto de estudio, conocer su estructura organizacional, forma de operación, lineamientos, normatividad y reglamentaciones en las que se ampara, entre otras.
> Reconocimiento del entorno y del ámbito de trabajo: Se requiere realizar una evaluación de activos, infraestructura y visita de los lugares físicos donde tendrá aplicación el proceso de análisis de riesgos.

[11] (SECURITY-JEIFER, 2010) SECURITY-JEIFER, ¿QUE ES EL CICLO PHVA? [En línea]. Disponible en https://securityjeifer.wordpress.com/2010/09/01/%C2%BFque-es-el-ciclo-phva/
[29] PERAFÁN. Op. cit., p. 34.

Desarrollo de análisis de riesgos: Gracias al plan de trabajo y la determinación de los componentes a evaluar, se recogen datos que permitan demostrar posibles deficiencias o fallas que puedan llegar a materializarse.

Identificación de vulnerabilidades: Se enfoca en el desarrollo de actividades y/o la aplicación de herramientas sobre sistemas de información, aplicaciones web, sistemas de comunicación o servicios de red y los activos de información críticos con el objetivo de determinar su estado actual desde el punto de vista de seguridad de la información.

Análisis de vulnerabilidades: Luego de obtener las evidencias se realiza un compendio y organización de todos estos datos, con información relevante que permita determinar focos de falla.

Análisis de los datos, hallazgos de debilidades y generación de recomendaciones: Con la información y datos obtenidos se genera una matriz con la valoración de los riesgos obtenidos, sugerencias y recomendaciones.

Discusión de resultados y obtención de la conclusión: paralelo a la generación del informe técnico, se realiza un resumen ejecutivo que muestre de una manera general y objetiva los resultados del proyecto.

Presentación del informe definitivo a las directivas de la Institución: Se prepara la sustentación del proyecto para socializar el trabajo realizado.

Etapa 1:

La primera etapa fue un reconocimiento de infraestructura física y tecnológica, así como la recolección de documentación e información relevante para el desarrollo del proyecto:

- ✓ Información contextual de la institución.
- ✓ Manuales de configuración por parte de fabricantes o elaborados por personal del área en cuanto a servicios, servidores y dispositivos de red.

Etapa 2:

En esta fase luego de comprender la estructura organizacional y su manera de operación, basada en el modelo de negocio (actividad principal) de la institución, se clasifican activos por criticidad, se definen planes para realizar y obtener datos sobre el estado de seguridad a nivel hardware y software de equipos, servicios, procesos y procedimientos; además de conseguir información con respecto a instalaciones físicas.

Visitas a los sitios físicos donde se encuentran los equipos de comunicación, seguridad perimetral, almacenamiento y procesamiento de datos para tomar evidencias de las condiciones actuales.

Clasificación de los activos de información más críticos que pueden detener el normal funcionamiento de la Sede en caso de falla.

Solicitud formal de cuentas de prueba y acceso en modo invitado a servidores y equipos de comunicación, tales como firewalls, switches y routers, con el fin de tomar evidencia del proceso y forma de configuración de cada dispositivo y/o sistema operativo.

Solicitud de acceso a la documentación de la red, se evidencia el diseño lógico (Definición de segmentos, diseño de direccionamiento, diagramas lógicos, VLANs), privilegios y características de cuentas de usuario, perfiles de cuentas de acceso, políticas definidas en los firewalls.

Etapa 3:

Con la información obtenida y el otorgamiento de acceso restringido sobre ciertos servicios, equipos o servidores y conociendo el direccionamiento e infraestructura tecnológica, se procede con el montaje de un escenario de pruebas, basado en herramientas de escaneo y análisis para detectar posibles vulnerabilidades a nivel de

servicios, protocolos o puertos; pruebas sobre conformación de contraseñas, modos de acceso y en general test que se encaminan a determinar el estado actual de seguridad en la infraestructura de red e información a nivel general.
Se realiza una selección de herramientas y entornos para realizar las diferentes pruebas que tienen aplicabilidad en el contexto del proyecto. La mayoría de herramientas utilizadas son herramientas de tipo Ethical hacking y versiones libres, aunque se hizo uso de herramientas en línea y versiones de prueba.
Se realiza un análisis y enumeración de puertos, protocolos y servicios para determinar el estado actual de puertos disponibles, abiertos y cerrados[30].

7.3 ALCANCE Y DELIMITACIÓN DEL PROYECTO

El alcance de esta propuesta, está orientado a auditar los protocolos y políticas de seguridad para que el director del IBAL tome las medidas necesarias que garantice la seguridad informática de la información, en la empresa de Acueducto y Alcantarillado IBAL de Ibagué.

Los procesos que incluyen esta auditoría están ligados solo a los sistemas de información, primero se planifica el procedimiento para identificar y comprender los procesos realizados por los funcionarios encargados del área de sistemas;

> …en segundo lugar se analiza y evalúa el control interno establecido, para determinar la probable efectividad y eficiencia del mismo; posteriormente, se aplican pruebas de auditoría para verificar la efectividad de los procedimientos de control (pruebas de cumplimiento), o de los productos de los procesos de trabajo (pruebas sustantivas).
> Después se informan los resultados de las auditorías, con el fin de reportar las sugerencias correspondientes a las oportunidades de mejora encontradas, y finalmente, se efectúa el seguimiento para evaluar el nivel del cumplimiento y el impacto de las recomendaciones hechas.[31]

El proyecto se llevará a cabo en la empresa de acueducto y alcantarillado IBAL ubicada en la calle 15 entre Carreras 6 y 7 de la ciudad de Ibagué, durante las 16 semanas correspondientes al periodo comprendido entre las fechas Agosto 24 a Diciembre 13 del año 2016.

[30] PERAFÁN. Op. cit., p. 34-37.
[31] FERNÁNDEZ GRAJALES, Nubia. Importancia de la auditoría informática en las organizaciones. [En línea]. México.: Universidad Nacional Autónoma de México. 2008. Disponible en http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.htm

7.4 Hipótesis

Para el planteamiento de las hipótesis, se utilizarán los tipos de hipótesis descriptivas; las siguientes variables: políticas y protocolos de seguridad de la información. Y la medición corresponderá con: óptima, regular y deficiente

Hi: Existen políticas regulares, que pretenden brindar eficiencia en la seguridad de los procesos llevados a cabo en la empresa IBAL.

Ho: Los protocolos existentes son deficientes, no brindan la seguridad suficiente a los procesos de las dependencias de la empresa IBAL.

7.5 Población

El proyecto se llevará a cabo en el edificio de la empresa de acueducto y alcantarillado IBAL, ubicado en la calle 15 entre Carreras 6 y 7 de la ciudad de Ibagué. Este edificio cuenta con 3 pisos entre los cuales se distribuyen las siguientes ocho áreas: Atención al cliente, Centro de comunicación, Contabilidad, Facturación, Financiera, Petición, quejas y recursos, Recuperación cartera y Sistemas.

7.6 Muestra

Se aplicó la auditoría a cada una de las áreas de la empresa IBAL, y se identificaron las políticas y los protocolos de seguridad de la información aplicados actualmente en cada una de sus dependencias. Para este efecto, se realizaron las entrevistas iniciales con sus respectivos test, a cada una de las personas encargadas o de mayor rango dentro de cada una de las mencionadas ocho dependencias de la empresa.

7.7 Instrumentos de recolección de datos

Como primera medida se consultaron las bases de datos correspondientes a los inventarios de hardware y software de la empresa IBAL, seguidamente se realizó la corroboración de campo para verificar el estado actual de la infraestructura tanto física como lógica de la empresa, seguidamente se realizaron entrevistas directas a los miembros del personal en cada una de las dependencias. Para el proceso de entrevistas al personal de la empresa, se diseñó una hoja de encuesta para ser diligenciada con la persona encargada o de mayor rango dentro de cada una de las ocho dependencias a auditar, estas hojas de encuestas serán parte del presente proyecto en la sección correspondiente a anexos.

8. RECURSOS NECESARIOS PARA EL DESARROLLO

8.1 Materiales

- Computador Portátil. Se requirió este elemento para realizar el análisis de los inventarios, diseño de encuestas y recopilación de información.
- Conexión a internet. Necesaria para la descarga de documentos, recopilación de información y realización de pruebas.
- Resma de papel. Para impresión de inventarios, documentos y hojas de encuestas.
- Impresora. Para la impresión rápida de los diversos documentos y formatos necesarios.
- Lápices.
- Lapiceros.
- Formatos para entrevista.
- Viajes. Viáticos para transporte dentro de la ciudad de Ibagué.
- Tablet. Para ingreso y consulta rápida de información.
- Fotocopias.

8.2 Institucionales

Se contó con el apoyo de la Empresa de Acueducto y Alcantarillado IBAL, de la ciudad de Ibagué, entidad donde se ejecutó el proceso de investigación y auditoria a su seguridad informática, para el desarrollo del presente proyecto. La Universidad Nacional Abierta y a Distancia UNAD, donde actualmente se lleva a cabo el seguimiento al planteamiento, desarrollo y aprobación de la presente auditoría de seguridad. Finalmente, la Biblioteca Darío Echandía de la ciudad de Ibagué, donde fue posible gran parte de la investigación bibliográfica y de referentes para el desarrollo del presente proyecto.

Tabla N° 1 “Recursos Necesarios”

RECURSOS NECESARIOS		
RECURSO	DESCRIPCIÓN	PRESUPUESTO ($)
1. Equipo Humano	(Investigadores en Formación) Estudiantes. Director trabajo: 20 horas Ingeniero Ibal 30	$ 900.000 $ 1.500.000 $ 600.000
2. Equipos y Software	Equipo de cómputo portátil, Tablet, conexión a internet.	$1.500.000
3. Viajes y Salidas de Campo	Entrevistas, visitas a la empresa.	$50.000 .
4. Materiales y suministros	Fotocopias, suministro de papelería.	$100.000
5. Bibliografía		
TOTAL		$4.650.000.00

Fuente: El Autor.

9. ESQUEMA TEMÁTICO

9.1 DETERMINACIÓN DE ACTIVOS COMPUTACIONALES Y TELEINFORMÁTICOS

Desarrollo:

Para la realización de este objetivo se recurrió a la Alcaldía de Ibagué, la cual exige el periódico diligenciamiento en formato digital, mediante formato de hojas de cálculo de Microsoft Excel, de la enumeración detallada de los recursos físicos e inventario de la empresa de acueducto y alcantarillado IBAL, este documento contiene el inventario de los bienes muebles de la empresa IBAL de Ibagué, por ende, en el mismo están detallados los activos computacionales y teleinformáticos existentes actualmente en la empresa, catalogados en el archivo oficialmente a diciembre de 2015, con los siguientes datos de cada uno de los equipos: Nombre, Dependencia y servidor público responsable, Número de identificación, fecha de adquisición, Precio de compra, descripción, Ubicación, Estado, póliza de seguro y mecanismo de control de inventarios. El documento en mención, será adjunto al documento del presente proyecto en un archivo comprimido mediante la aplicación WinRar, para efectos prácticos de las consultas futuras e implicadas en el presente proyecto, bajo el nombre oficial de archivo: “12885-DOC-20151202.xls”, pero también puede descargarse de la página oficial de la alcaldía de Ibagué mediante el siguiente link: www.alcaldiadeibague.gov.co/portal/admin/.../12885-DOC-20151202.xls

Es de resaltar que en dicho documento, además de encontrarse relacionada la actual existencia denominada como “bienes muebles” de la empresa de Acueducto y Alcantarillado IBAL de Ibagué, también se encuentra en este mismo documento de inventario, la relación detallada de todas y cada una de las licencias actuales de software, con su respetiva asignación de equipos y usuarios en cada una de las dependencias de la empresa.

9.2 IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS

Desarrollo:

Basado en la relación de equipos teleinformáticos de vital importancia en la implementación de la seguridad de la información en la empresa de acueducto y alcantarillado IBAL de la ciudad de Ibagué, ubicada en la Calle 15 N 6-70, los cuales se distribuyen en las siguientes 8 dependencias:

1. Atención al Cliente.
2. Centro de Comunicación.
3. Contabilidad.
4. Facturación.
5. Financiera.
6. Petición Quejas y Recursos.
7. Recuperación Cartera.
8. Sistemas.

Se llegó a las siguientes conclusiones tras analizar las características teleinformáticas y posibles vulnerabilidades en el manejo de la seguridad de la información por parte de la empresa, la relación se realiza mediante la diferenciación de las características por cada dependencia y de esta manera se concluye con el nivel de impacto en cada una de ellas:

1. Atención al Cliente:

El Hardware de esta dependencia consta de 3 equipos: 1 Servidor ML 110 65, 1 Computador DELL REF. 60SNLD1 y 1 Computador Portátil HP 43000S INTEL CORE 13 4R. El Software de esta dependencia consta de 3 licencias corporativas: Office (SMALL BUSINESS 20), Software “Control y Estadístico” y Office 2007. Es evidente la ausencia de hardware de protección eléctrica y de respaldo en casos de caída de tensión en la red de distribución eléctrica, también de equipos de soporte para la función de dicha dependencia, puesto que para una adecuada atención al cliente se debe prever la afluencia repentina de muchos visitantes que esperan ser atendidos oportunamente, por último es de notar que los equipos existentes no

disponen de defensa alguna contra software malintencionado y posibles ataques intrusivos, tampoco de algún protocolo de seguridad establecido para proteger la información de dichos ataques.

2. Centro de Comunicación:

Es preocupante descubrir que en una empresa en la que una comunicación oportuna es indispensable para su funcionamiento, no se cuente con equipo informático alguno como se halló en este caso, sólo disponen de un estabilizador eléctrico de 1000 W para efectos de equipos análogos de intercomunicación. Resulta obvia la recomendación de actualización de equipos y recurso humano, puesto que una empresa que espera brindar un servicio con garantías debe estar siempre en línea con sus demás dependencias para garantizar un servicio oportuno, así como la seguridad propia de todo proceso en el manejo de la información.

3. Contabilidad:

Esta dependencia cuenta con 6 Computadores de escritorio y tan sólo con 2 licencias corporativas de software: Office (SMALL BUSINESS 20) y Office 2007. En este caso es de notar la grave falencia de no tener software dedicado para la manipulación de contabilidad, haciendo notable el mal estado informático en que se encuentra la empresa, dificultando la manipulación de datos y cifras que podrían comprometer la estabilidad de la empresa al dejar estos procesos relegados al casi estricto manejo humano y confiabilidad que puede darse a la manipulación de hojas de cálculo convencionales y la vulnerabilidad que esto representa en la seguridad y confianza. Esto sin entrar en los detalles del peligro causado por la no existencia de software de seguridad al menos básico.

4. Facturación:

Esta dependencia cuenta tan sólo con 2 computadores de escritorio y 3 licencias corporativas de software: Windows XP Home, Office 2007 y licencia OLP Office MOL 2007. También se evidencia que partiendo de la inexistencia de licencias actualizadas de Sistema Operativo, equipos suficientes para la demanda de la función correspondiente a la facturación de una empresa de tal envergadura y software dedicado para la seguridad básica, tampoco se cuenta son software que facilite el proceso de manejo seguro de información en este caso, como lo es la administración de la misma y la generación de los documentos que ella implica, haciendo reiterativo el manejo de herramientas y hojas de cálculo que no aportan efectividad ni seguridad en los procesos.

5. Financiera:

Esta dependencia cuenta con 5 equipos de cómputo de escritorio, 1 equipo portátil Acer Core I3 y 4 licencias corporativas de software: Office 2013, Office 2007, Office

2003 ed. Beta y Windows XP Professional OEM. Nuevamente son notables las deprimentes características en cuanto a licenciamiento de software adecuado para las funciones de cada una de las dependencias, en este caso se vuelven a hacer evidentes las vulnerabilidades de seguridad y también de manejo adecuado de la información, dejando prácticamente a la deriva los procesos implicados en uno de los sectores más importantes de la empresa. Es de anotar que en este caso se trata de una total reestructuración de los procesos en su totalidad y de una aplicación prácticamente inicial de un sistema de seguridad y seguimiento de la información.

6. Petición Quejas y Recursos:

Este punto de atención y servicio está dotado con 24 equipos de cómputo de escritorio, 1 módem banda base pairgain, 2 router cisco 1600 y 2 UPS, cuenta con las siguientes licencias corporativas de software: Office 2007, Office 2003, Office 2013 y Windows XP Profesional. A pesar del respaldo que implica tener suficientes equipos de cómputo para dicha función empresarial y contando con el soporte de las UPS y los router para el aseguramiento del flujo de energía y la constante conectividad, se evidencia nuevamente, que como en los casos anteriores, no se cuenta con licencias actualizadas de software, programas específicos de la empresa o “empresariales” que aseguren la eficiencia de los procesos, así como de nuevo no se cuenta con software que garantice la seguridad de los mismos.

7. Recuperación Cartera:

Esta sección cuenta con el respaldo de 10 computadores de escritorio y una UPS Apc 650 Kva, también con las siguientes licencias corporativas de software: Office bassic edition 2003, Office MOL2007 y Windows XP Profesional.

8. Sistemas:

Esta importantísima área de la empresa cuenta con la siguiente dotación: 5 Servidores, 5 computadores de escritorio, 1 Router inalámbrico link doble antena, 1 Rack de comunicaciones, 2 swicht administrables de 48 puertos y una UPS American Power SU/3000 S#9, también cuenta con las siguientes licencias de software: RM/Cobol Development y Wow, Licencia Procesador 228-03182, Actualización OpenServer 5.0.5, Licencia Unix para 35 usuarios, Software Gestión Documental, Programa Visual FoxPro Versión 9.0, Software Creativity Designer, Office MOL 2007, Office 2013, Software Isolución, Software SIG, Firewall Fortinet, Licencia antivirus y Cal Open VLSC. Es importante anotar que pese al empeño por la manipulación de software dedicado en el área de sistemas, no todas las licencias son de carácter corporativo, haciendo sus funciones de carácter experimental, puesto que en la práctica hemos visto que las distintas dependencias de la empresa no cuentan con herramientas suficientes y confiables de software que garanticen los procesos de cada una de ellas, así, es evidente que las pruebas llevadas a cabo en el departamento de sistemas, más allá de la comprobación de las utilidades

lógicas, debe conllevar a la utilización práctica de aquellas utilidades por parte de cada uno de los funcionarios de la empresa y estar presentes en cada uno de los procesos de la misma.

Puede resumirse, de acuerdo al análisis elaborado, que no se puede determinar una o varias áreas de la empresa de acueducto y alcantarillado IBAL de Ibagué, como de mayor impacto en la vulnerabilidad de la seguridad dentro del conjunto de dependencias de la misma, puesto que cada una de ellas está ligada a cada uno de los procesos de vital importancia en el correcto funcionamiento de la misma. Es determinante concluir que, para lograr una aplicación efectiva de un Sistema de Seguridad en esta empresa, se debe declarar la misma como una institución que enteramente, con igual grado de impacto para cada una de sus dependencias, está en riesgo total, y deben tomarse medidas generales que abarcan desde el hardware, pasando por el software hasta llegar al recurso humano, para asegurar y dar garantías en el desempeño de cada uno de sus estamentos. Adjunto se anexa una hoja de cálculo de Microsoft Excel con la relación de equipos, programas y dependencias implicados en el desarrollo del plan de seguridad, el archivo se denomina “Relación Impacto Hardware y Software.xls”.

9.3 REINGENIERÍA DEL PROTOCÓLO, PARA UNA POLÍTICA DE SEGURIDAD CONFIABLE

Desarrollo:

Con base en los descubrimientos realizados en el desarrollo de los objetivos anteriores, la ausencia de políticas integrales de seguridad, que abarquen desde la infraestructura teleinformática, los soportes lógicos, protocolos confiables y la capacitación del recurso humano, para poder optar por la implementación de un protocolo de seguridad permanente y asegurar así la efectividad del mismo, se concluye que: en este caso no se trata de una reingeniería del protocolo; en este caso es necesario el diseño general del mismo, partiendo desde las políticas de la empresa, que deben ser ajustadas para que este nuevo protocolo sea atendido como una de las prioridades en el funcionamiento tanto interno como externo de la empresa de Acueducto y Alcantarillado IBAL de Ibagué.

Durante la investigación se halló que la empresa, aparte de su “Política de Tratamiento de Datos Personales”, la cual, obedece como cumplimiento a lo dispuesto en la ley 1581 de 2012 y el Decreto 1377 de 2013 en lo concerniente al tratamiento y protección de datos personales de los usuarios y que a su vez implica la garantía de seguridad teleinformática de la empresa, no cuenta con demás políticas así mismo ajustadas, ya en este caso, a normas de seguridad estrictamente tecnológicas, y no solamente al compromiso por parte de la empresa a cumplir estipulaciones éticas y legales. La política en mención será adjuntada al presente archivo mediante el archivo denominado “Política de tratamiento datos personales IBAL.pdf”

El diseño del protocolo de seguridad, constará de 3 fases en las que se replanteará el actual estado y funcionamiento general de la estructura informática en cada una de las dependencias (iniciando esta vez con en el área de Sistemas) de la empresa de Acueducto y Alcantarillado IBAL: Primera: Adecuación y actualización física. Segunda: Actualización y licenciamiento lógico corporativo. Tercera: Capacitación del recurso humano.

Primera Fase: Adecuación y actualización física.

- Sistemas:

Se detectó la necesidad de la instalación de un sistema de polo a tierra que abarque no solamente esta dependencia, sino que tenga la capacidad para la totalidad de equipos dentro de la sede de la empresa, la instalación de una UPS de respaldo de emergencia a la que actualmente soporta la carga de la empresa, el reemplazo de dos de los actuales servidores, los ML37064 2Ghz Procesador 3.0, debido a la baja velocidad de procesamiento (2Ghz), requerimiento vital para el manejo multiusuario de bases de datos, y la instalación de un sistema biométrico de identificación para el acceso de administradores y posibles usuarios autorizados.

- Atención al Cliente:

Aquí es necesaria la instalación de una UPS con capacidad de respaldo para el servidor y los equipos, el remplazo del equipo portátil HP 43000S por uno de escritorio y última generación, así mismo la adición de un equipo de escritorio más para esta sección, aumentando de esta manera el pobre rendimiento para la alta demanda de esta dependencia.

- Centro de Comunicación:

En vista de la total ausencia de equipos teleinformáticos digitales en esta importante dependencia, se hace necesaria la instalación de al menos dos equipos de escritorio y un portátil, todos de última generación. También, la instalación de una UPS regulada de respaldo para los equipos de esta sección, así como de un Acces Point de alto rango, para efectos de conectividad constante de equipos menores de comunicación como los Smartphone, a la red interna de la empresa.

- Contabilidad:

En esta sección hace falta una UPS de respaldo para los seis equipos. También de la instalación del sistema de identificación biométrico para cada uno de ellos; como en el caso de las áreas de sistemas y demás, esta será la primera barrera de seguridad, que en las siguientes fases será complementada por medio de software dedicado y corporativo (según las dependencias), además de las respectivas capacitaciones a que deberá someterse la totalidad del recurso humano de la empresa.

- Facturación:

En esta dependencia se debe tener en cuenta que la labor de facturación debe atender eficientemente dos procesos básicos: el ingreso de datos al sistema y la producción análoga de documentos, en vista de ello, es necesaria la instalación de

por lo menos un equipo de escritorio más de respaldo, para garantizar funcionalidad en caso que alguno de los dos equipos actuales llegue a presentar fallas, así mismo, la instalación de un sistema UPS de respaldo que soporte tanto los equipos de cómputo como las impresoras. Aquí también es evidente la necesidad de la implementación del sistema biométrico de identificación para los tres equipos.

- Financiera:

Aquí, como hemos visto en la totalidad de las dependencias de la empresa, existe la falencia de un sistema energético de respaldo para los equipos, como segunda alternativa de solución ante una posible falla eléctrica, así como de la necesidad de la puesta en marcha del sistema biométrico de identificación para cada equipo.

- Peticiones, Quejas y Reclamos (PQR):

En esta importantísima sección es urgente el cambio de una de las actuales UPS, la APC 650KVA, por una de 10k KVA de doble fase, para así poder soportar la carga de todos los computadores, los router y el módem, en caso de fallos eléctricos que sobrepases la primera barrera de protección. Por otra parte, también se requiere la instalación del sistema biométrico de identificación para los computadores, tanto para el acceso como para el registro eficiente de los usuarios.

- Recuperación Cartera:

Aquí es evidentemente necesario el reemplazo de la actual UPS de 650KVA por una de 10k KVA y doble fase, para poder soportar así la carga de los 10 computadores de esta dependencia. El reemplazo de uno de los computadores, el Pentium II 350 por uno de última generación y la adecuación biométrica de seguridad para cada uno de los computadores.

Segunda Fase:

Actualización y licenciamiento lógico corporativo.

Llegados a este punto, referente a la actualización y licenciamiento lógico corporativo del software de la empresa de Acueducto y Alcantarillado IBAL de la ciudad de Ibagué, es importante aclarar que para un óptimo funcionamiento tele informático, en el cual es de vital importancia la conectividad y transmisión eficiente de datos entre aplicativos y sus respectivas configuraciones entre servidores y clientes, es necesario adquirir licencias corporativas de software, tanto de Sistemas Operativos como de aplicaciones tanto generales como dedicadas, sin olvidar los respectivos controladores originales de hardware, obteniendo así fácil y de forma segura sus oportunas actualizaciones, para que la seguridad de la información que dichos programas manejan no se vea comprometida y a su vez sea administrada eficientemente.

Es de esta manera que se puede conjeturar que gracias a este tipo de licenciamiento, no es necesario hacer una programación inicial para acciones directas en cada una de las dependencias de la empresa, ya que por medio de licenciamientos corporativos para cantidades mínimas de equipos, se asegurará la cobertura inicial de todas las dependencias y también, de posibles expansiones futuras de las mismas. A su vez que permitirá gestionar administrativamente todo el software desde los servidores y el área de sistemas en general.

Según la proyección efectuada durante la primera fase, contamos con un total de 66 equipos de cómputo en la empresa, de los cuales seis son servidores; cinco ubicados en el departamento de sistemas y uno en el de atención al cliente. Teniendo en cuenta esta cantidad de equipos, podemos calcular de forma general la cantidad mínima de licencias tanto de equipos como de usuarios de aplicaciones, manteniendo estas cantidades mínimas para asegurar un buen campo de acción en caso de emergencias que hagan necesario el posible uso general de cualquier equipo de la empresa, como también del respaldo entre servidores sin sufrir mayores contratiempos.

De esta manera obtenemos las siguientes disposiciones:

Licenciamiento de Controladores de Hardware:

Se continuará manejando la actual vía legal de la empresa, tanto para equipos ya existentes como para las nuevas adquisiciones, esta metodología proporciona los controladores originales por unidades de hardware adquirido, así como el soporte en línea y las respectivas actualizaciones.

Licenciamiento de Sistemas Operativos:

Se adquirirán licencias corporativas para ocho servidores (dos de estas licencias serán para emergencias o expansiones), otorgadas para Windows Server 2016; evidentemente necesarias para implementar este Sistema Operativo en los servidores, en pro de la correcta y fácil configuración y funcionamiento de los aplicativos y sus divisiones entre servidores y clientes que conjuntamente correrán sobre plataformas Microsoft a través de la red tanto interna como externa de la empresa. También se adquirirán 70 licencias corporativas para equipos (10 de ellas para emergencias o expansiones), para Windows 10 Pro, versión más completa del último lanzamiento Windows de Microsoft.

Licenciamiento de Programas de uso general:

Se adquirirán licencias corporativas para 80 equipos (14 de ellas para emergencias o expansiones), para Microsoft Office 365 Personal (Office 2016 es la última versión, pero no incluye Outlook (correo corporativo), Publisher, Access, 1 Tb de almacenamiento en la nube, 60 min de Skype, ni se mantiene constantemente

actualizado). Y licencia corporativa para ocho servidores y 70 clientes (12 de ellas para emergencias y posibles expansiones, distribuidas dos para servidores y 10 para clientes), para McAfee; en este caso resulta recomendable adquirir End Point Protection Essential for SMB (de McAfee), el cual está diseñado para brindar soporte hasta a 250 dispositivos y bajo una misma licencia, el cuál será adquirido para uso local y configurado para actualizar por puertos específicos, dedicados y monitoreados por él mismo en los servidores.

Licenciamiento de Software Dedicado:

Se adquirirán nuevas y también se extenderán las licencias actuales a uso corporativo de 80 equipos (14 de ellas destinadas a emergencias o expansiones, dos para servidor y 12 para cliente) en las siguientes aplicaciones: RM/ Cobol Development y Wow, Software Gestión Documental, Visual FoxPro 9.0 SP2, en el importantísimo software Isolución (para el sistema de gestión de calidad ISO 9001, ISO 14001, OHSAS 18001, ISO 27001, ISO 31000, MECI y NTGCP 1000), también en el software SIG (Sistema de Información Geográfico), firewall Fortinet y Cal Open VLSC.

Es importante recordar que, así como las licencias legales deben otorgar el total soporte técnico al Sistema Operativo, controladores, aplicativos generales y dedicados, también debe asumirse por parte de la empresa, la correcta configuración y seguimiento de las actualizaciones automáticas de seguridad tanto en los servidores como en cada uno de los equipos y clientes de software, para garantizar la permanencia de la confiabilidad en la seguridad del sistema.

Tercera Fase:

Capacitación del Recurso Humano.

Llegados a esta última fase del proceso de reingeniería del protocolo de seguridad, se debe establecer un proceso de capacitación del personal de la empresa, éste proceso estará dividido en dos etapas para el manejo de los recursos de la empresa: Primero en el manejo de los recursos físicos y segundo en el manejo de los recursos lógicos.

- Primera etapa:

Manejo de Recursos Físicos.

En esta primera parte del proceso de capacitación, se dará entrenamiento para la adecuada manipulación de todos los recursos físicos implicados en el manejo de la información, esta capacitación estará enfocada a todo el personal, de todas las dependencias de la empresa, con el objetivo que cada uno de sus funcionarios esté en capacidad de dar el correcto y total seguimiento de los recursos físicos o de

hardware de que dispone en su puesto de trabajo, así como también que pueda brindar soporte de emergencia en el caso que éste sea necesario.

Esta capacitación estará comprendida por las siguientes secciones:

- Conocimiento y verificación de conexiones eléctricas y unidades de respaldo de energía.

- Conocimiento y verificación de conexión entre dispositivos de entrada y salida.

- Conocimiento, manipulación y verificación del correcto funcionamiento de dispositivos de identificación biométrica.

- Conocimiento y manipulación de unidades externas de almacenamiento.

- Segunda etapa:

Manejo de Recursos Lógicos.

Esta última parte del proceso de capacitación, se utilizará para dar instrucción sobre el correcto y seguro manejo de los recursos lógicos (software) de la empresa, esta capacitación estará diferenciada por grupos determinados según las dependencias de la empresa, excepto el área de sistemas, que aparte de la instrucción determinada para su grupo, también deberá cursar los temas de todas las demás dependencias, para así asegurar el soporte que ésta sección de la empresa debe brindar oportuna y eficientemente a todas las demás.

Las capacitaciones estarán conformadas desde el uso general de cada tipo de software, hasta sus características y procedimientos de seguridad, de esta manera, se dividirán y dictarán los cursos en el orden de las siguientes secciones:

Sistemas:

- Capacitación en Windows Server 2016.

- Capacitación en Windows 10 Pro.

- Capacitación en Office 365 Personal.

- Capacitación en End Point Protection Essential for SMB (de McAfee).

- Capacitación en RM/Cobol Development y Wow.

- Capacitación en Software Gestión Documental.
- Capacitación en Visual FoxPro 9.0 SP2.
- Capacitación en Isolución (Gestión de Calidad).
- Capacitación en SIG (Sistema de Información Geográfico).
- Capacitación en Firewall Fortinet (programación de control).

Demás dependencias:

- Capacitación en Windows 10 Pro.
- Capacitación en Office 365 Personal.
- Capacitación en End Point Protection Essential for SMB (Para Clientes).
- Capacitación en Software Gestión Documental.
- Capacitación en Isolución (Gestión de Calidad).
- Capacitación en SIG (Sistema de Información Geográfico).

10 PERSONAS QUE PARTICIPAN EN EL PROYECTO

10.1 PROPONENTE PRIMARIO:

JOHN FREDDY LUGO LUNA, Ingeniero de Sistemas egresado de la UT, actualmente estudiante en la UNAD en seguridad informática, trabaja como administrador en la alcaldía de Ibagué.

10.2 PROPONENTES SECUNDARIOS

SALAMON, Ingeniero de Sistemas, Orientar virtualmente a los estudiantes del curso de Ingeniería de Telecomunicaciones y Especialización en Seguridad Informática.

JUAN JOSE CRUZ GARZON, Ingeniero de Sistemas, Especialista en seguridad informática, Docente Ocasional de la Unad y es Director de trabajo de grado.

11 INFORME GENERAL DE HALLAZGOS, CONCLUSIONES Y RECOMENDACIONES

Con base en los hallazgos realizados en el desarrollo de los objetivos anteriores, se hace un llamado a la administración, sobre el grave estado tanto funcional como de seguridad de la empresa de Acueducto y Alcantarillado IBAL de la ciudad de Ibagué, las deficiencias pueden ser catalogadas en tres campos de la integridad informática de la empresa:

Infraestructura Física:

Se encontraron graves deficiencias, las cuales se describieron detalladamente en la sección de reingeniería del protocolo y entre las cuales se descubrieron problemas como la falta de polo a tierra para el circuito eléctrico interno de la empresa, falta de unidades de respaldo de energía en todas las dependencias, presencia y uso actual de servidores y equipos deficientes y descontinuados, falencia de equipos de soporte en algunas dependencias de alta demanda de la empresa, ausencia de métodos y dispositivos de identificación biométrica y falta total de unidades externas de respaldo de datos.

Infraestructura Lógica:

Se descubrió el grave estado actual de esta infraestructura y se detallaron anteriormente cada uno de los problemas hallados en cada dependencia de la empresa, para argumentar y rediseñar el protocolo; problemas como la falta de Sistemas Operativos debidamente licenciados y actualizados, tanto para servidores como para equipos, la falta de licenciamiento corporativo para programas de uso general, desde software para la gestión de documentos hasta software para la protección básica contra amenazas de seguridad, falta de licenciamiento empresarial para aplicativos de uso dedicado, tanto para servidores como para las configuraciones de clientes, y la ausencia total de un sistema lógico de soporte para la tecnología de identificación biométrica.

Recurso Humano:

En este importantísimo factor de la empresa, se hallaron problemas directamente ligados y dependientes de las condiciones actuales en la demás infraestructura de la empresa a través de todas sus dependencias, problemas como la falta de capacitación en procedimientos habituales básicos de verificación del soporte energético de emergencia, de comprobación de conectividad entre dispositivos de uso constante, de desconocimiento del uso y verificación de soportes tanto físicos como lógicos de identificación biométrica, la falta de capacitación para el uso de sistemas operativos, de programas de uso general, de aplicativos de uso dedicado tanto interno como externo y procedimientos de seguridad actualmente

desconocidos, naturalmente debido al desconocimiento implícito del software y la desactualización total de las herramientas lógicas actualmente en uso.

En estas condiciones actuales, se sugiere urgentemente adoptar las medidas descritas detalladamente en la reingeniería del protocolo actual de seguridad de la empresa, protocolo calificado en su momento por este estudio como totalmente inexistente, debido y a su vez argumentado por todos los problemas y falencias actuales descritas en el mismo. De esta manera, se sugieren las actualizaciones mencionadas y justificadas en el mismo, toda la adecuación de la infraestructura física, análoga, digital y de seguridad, la implementación lógica bajo el marco legal tanto para Sistemas Operativos como para programas básicos y dedicados, y la capacitación sugerida para la totalidad del recurso humano de la empresa. Todo esto como medida inicial para poder optar por la implementación de una gestión constante y confiable de la seguridad de la empresa de Acueducto y Alcantarillado IBAL de la ciudad de Ibagué, con la continuación y evolución del presente protocolo que según la norma ISO/IEC 27002 asegura su efectividad, aumentando y garantizando de esta manera la seguridad, el rendimiento general y por ende la confiabilidad de la empresa.

Se pudo evidenciar que las políticas que cuenta la empresa en su sede principal no se están aplicando en la sede de la calle 15 No. 6-48 es importante que el personal encargado haga saber de estas y se cumplan así como también retroalimentar políticas que en su momento funcionaban pero que a lo largo del tiempo han perdido su finalidad las cuales se deben retroalimentar y en otras ocasiones crear porque no existe política alguna que reglamente el uso de determinados procesos.

Se deben modificar los permisos de todos los contratistas que pasan por la empresa para evitar fraudes, donde contratistas de años pasados que no pertenecen podrían entrar a aplicativos o correos institucionales.

Se recomienda la instalación de un sistema de detección de intrusos donde se pueda tomar medidas de los ataques que se reciban, ya que se tiene instalado un firewall pero que esta administrado por un tercero donde la empresa no cuanta con ese control dejando todo en manos del isp.

Se debe coordinar con el administrador de la red tanto local como interna que se cierren los puertos que no se están utilizando como la actualización de los parches de seguridad en el servidor que enlaza con la sede principal ubicada en la pola.

Se pudo verificar que las bases de datos funcionan perfectamente y están en procesos de actualizar el a un nuevo sistema, se recomienda que tengan en cuenta la complejidad en las cuentas y el cifrado de la información de ellas.

IDENTIFICACIÓN DE ACTIVOS

En esta fase se revisa todos los activos que posee la empresa IBAL con el fin de conocer su estado actual[32].

TABLA No.1 Identificación de activos

[S]DATOS / INFORMACIÓN	• [files]Ficheros • [conf]Datos de configuración • [int]Datos de gestión interna • [pasword]Credenciales • [auth]Datos de validación de credenciales • [acl]Datos de control de acceso • [log]Registro de actividad
[SW]SOFTWARE	• [os]Sistema operativo Microsoft Windows 7Professional licenciado (estaciones de trabajo para desarrolladores e integradores). • [wu]Windows Update • [prp]Desarrollo propio • [hypervisor]Gestor de máquinas virtuales • [app]Aplicaciones de reporte de horas, plataforma de E-Learning, bases de datos de conocimiento y otros. • [app]Servidor de directorio LDAP
[HW]HARDWARE	• [dbms]Servidor de base de datos contiene: BBDD corporativas y las empleadas por el desarrollo y pruebas. • [app]Servidor de aplicaciones: entorno de desarrollo y pruebas • [app]Mainframe: No existe, se está utilizando los entornos de pruebas para este fin. • [print]Servidor de ficheros e impresión • []Workstations de desarrollo • [app]Servidor proxy + firewall nivel de aplicación • [app]Servidor DNS interno + Host IDS

[32] (Rocio, 2013)APLICACION DE LA METODOLOGIA MAGERIT, 2013 [En línea] UNIVERSIDAD POLITECNICA SALESIANA SEDE CUENCA, Disponible en https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

	• [app]Servidor DNS externo + Host IDS • [app]Servidor web interno + host IDS • [app]Servidor web externo + host IDS • [pabx]Servidor de acceso remoto telefónico • [email server]Servidor de correo electrónico + host IDS • [network]Network IDS (2) • [firewall]Firewall interno (2) • [firewall]Firewall externo • [firewall]Firewall Zona Wifi
[COM]COMUNICACIONES	• [internet]Acceso internet ISP • [pstn]Red Telefónica básica o RDSI • [wifi]Red WIFI • [lan]Red LAN • [internet]Internet • [vpn]Red VPN
[AUX]EQUIPOS AUXILIARES	• [power]Fuentes de alimentación • [ups]Sistemas de alimentación interrumpida • [gen]Generadores eléctricos Diesel • [wire]Cable eléctrico • [fiber]Fibra óptica • [sei]Sistema de extinción de incendios • [ac]Equipos de climatización
[S]SERVICIOS	• [email]Correo electrónico • [file]Almacenamiento de ficheros • [edi]Intercambio electrónico de datos • [ftp]Transferencia de ficheros • [internet]Internet
[L]INSTALACIONES	• [buildong]Oficinas o delegaciones • [cpd]CPD
[P]PERSONAL	• [ur]Usuarios remotos • [des]Desarrolladores • [adm]Funcionarios para la gestión de infraestructura
[SI]SOPORTES DE INFORMACIÓN	• [san]Almacenamiento en red • [seg]Tarjeta de identificación • [electronic]Electrónicos

VALORACIÓN DE LOS ACTIVOS

La valoración de los activos va de acuerdo a lo que puede repercutir para la empresa estimar su costo de valor inicial, costo de reposición, costo de configuración, costo de uso del activo y valor de perdida de oportunidad.

La empresa debe conocer cuánto le vale adquirirlo o desarrollarlo y contemplar el costo por la función que ella desempeña y el costo que genera ponerlo nuevamente en marcha en caso de que éste llegase a dañarse o deteriorarse.
Es por ello que se hace necesario tener en cuenta diferentes variables a la hora de darle valor a un activo. Según la situación actual de la empresa IBAL Los activos más relevantes y que pueden afectar el correr del negocio son los siguientes:

Servidores de Bases de Datos: No específica cuantos posee la empresa, se sabe que guardan todo los datos de la empresa e incluyendo el sistema de gestión de proyectos que es un repositorio de documentos y que también guarda el código fuente. Se observa que en este servidor es esencialmente útil para la empresa y su pérdida intencional o involuntariamente puede afectar altamente todas las propiedades de la seguridad: Autenticidad (A), Confiabilidad (C), Integridad (I), Disponibilidad (D), Trazabilidad del servicio (T). Igualmente, no conoce un sistema de backup o si se tiene replica de los datos en otros servidores; no se conoce el nivel de seguridad en cuanto a los datos y al acceso de este servidor que guarda y registra el activo más importante de la empresa. “La Información y el código fuente de los desarrollos”.

Servidores de aplicaciones: No se recomienda tener en el mismo servidor de aplicaciones un entorno de desarrollo y pruebas, debido al recurso que esto puede requerir y puede afectar la disponibilidad del servicio, además por seguridad la empresa debe tener su propio entorno para estos procesos.

IDENTIFICACIÓN DE LAS AMENAZAS

Para esta actividad se tomó la caracterización usada por la herramienta Pilar estandarizada por Magerit. Como la herramienta Pilar, es licenciada no se puede utilizar para este caso, sin embargo, utilizo la clasificación de las amenazas según la misma[33].

TABLA No.2 Clasificación de amenazas

[N] Desastres Naturales
[I] De origen industrial
[E] Errores y fallos no intencionados
[A] Ataques intencionados

TABLA 3. Clasificación de Amenazas herramienta PILAR

[N] Desastres naturales
[N.1] Fuego
[N.2] Daños por agua
[N.*] Desastres naturales
[I] De origen industrial
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios y suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados
[E.1] Errores de los usuarios

[33] (Rocio, 2013)APLICACION E LA METODOLOGIA MAGERIT, 2013 [En línea] UNIVERSIDAD POLITECNICA SALESIANA SEDE CUENCA, Disponible en https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.7] Deficiencias en la organización
[E.8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Escapes de información
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A] Ataques intencionados
[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.13] Repudio
[A.14] Interceptación de información (escucha)
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[A.22] Manipulación de programas
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo

[A.27] Ocupación enemiga
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

TABLA No. 4 Identificación de las amenazas de la empresa IBAL

Activos
DATOS / INFORMACIÓN
Ficheros, Datos de configuración, Datos de gestión interna, Credenciales, Datos de control de acceso, Copia de respaldo y Registro de actividad
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.3] Errores de monitorización (log)
[E.4] Errores de configuración
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caída del sistema por agotamiento de recursos
[A.3] Manipulación de los registros de actividad (log)
[A.4] Manipulación de la configuración
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.18] Destrucción de información
[A.19] Divulgación de información
[I.8] Fallo de servicios de comunicaciones
SERVICIOS
Internet, Intercambio electrónico de datos, Transferencia de ficheros, Almacenamiento de ficheros y Correo electrónico
[E. 1] Errores de los usuarios
[E.2] Errores del administrador

[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.19] Divulgación de información
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
[I.8] Fallo de servicios de comunicaciones
SOFTWARE
Sistema operativo Microsoft Windows 7Professional licenciado (estaciones de trabajo para desarrolladores e integradores), Windows Update, Gestor de máquinas virtuales, Desarrollo propio (aplicaciones bancarias) y Aplicaciones corporativas
[I. 5] Avería de origen físico y lógico
[E. 1] Errores de los usuarios
[E.2] Errores del administrador
[E. 8] Difusión de software dañino
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E. 20] Vulnerabilidades de los programas (software)
[E. 21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso

[A. 7] Uso no previsto
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.19] Divulgación de información
[A.22] Manipulación de programas
HARDWARE
Servidor de base de datos, Servidor de aplicaciones, **Servidores Web, Mainframe, Work stations de desarrollo y Firewalls**
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I. 5] Avería de origen físico y lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[I.*] Desastres industriales
[E.2] Errores del administrador
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
E.24] Caída del sistema por agotamiento de recursos
[E.25] Pérdida de equipos
[A.6] Abuso de privilegios de acceso
[A. 7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.24] Denegación de servicio
[A.25] Robo
[A.26] Ataque destructivo
REDES Y COMUNICACIONES
Red LAN , Red de área local 802.1X, Red VPN, Acceso internet ISP y Red Telefónica básica o RDSI
[E.2] Errores del administrador
[E.9] Errores de [re-]encaminamiento

[E.10] Errores de secuencia
E.19] Fugas de información
E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad del usuario
[A.6] Abuso de privilegios de acceso
[A. 7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.10] Alteración de secuencia
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
EQUIPAMIENTO AUXILIAR
Sistemas de alimentación interrumpida, Generadores eléctricos Diésel, Cableado, Fibra óptica, Equipos de climatización, Sistema de extinción de incendios
[A. 7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación de los equipos
[A.25] Robo
[A.26] Ataque destructivo
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I. 5] Avería de origen físico y lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.9] Interrupción de otros servicios y suministros esenciales
[I.11] Emanaciones electromagnéticas
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.25] Pérdida de equipos
SOPORTES DE INFORMACIÓN

Tarjeta de proximidad y código PIN, Electrónicos
[A. 7] Uso no previsto
[A.11] Acceso no autorizado
[A.15] Modificación deliberada de la información
[A.19] Divulgación de información
[A.23] Manipulación de los equipos
[A.25] Robo
[A.26] Ataque destructivo
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[I. 5] Avería de origen físico y lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.10] Degradación de los soportes de almacenamiento de la información
[E. 1] Errores de los usuarios
[E.2] Errores del administrador
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.25] Pérdida de equipos
INSTALACIONES
Oficinas o delegaciones, CPD
[N.1] Fuego
[N. 3] Desastres naturales
[I.1] Fuego
[I. 2] Daños por agua
[I.3] Contaminación mecánica
[I.4] Contaminación electromagnética
[A.11] Acceso no autorizado
[A. 7] Uso no previsto
[A.15] Modificación deliberada de la información

[A.19] Divulgación de información
[A.26] Ataque destructivo
[A.27] Ocupación enemiga
[N.*] Desastres naturales
[E.18] Destrucción de información
[E.19] Fugas de información
PERSONAL
Usuarios remotos, desarrolladores, funcionarios para la gestión infraestructura y demás usuarios
[E.7] Deficiencias en la organización
[E.19] Fugas de información
[A.5] Suplantación de la identidad del usuario
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)

VALORACIÓN DE LAS AMENAZAS

El fin de esta fase es:

- Evaluar la probabilidad de ocurrencia de cada amenaza correspondiente a cada activo.
- Estimar el grado del impacto que causaría esta amenaza al llegar a materializarse.

Partiendo de la información anterior se procede a realizar la valoración de las amenazas para cada activo para determinar la frecuencia y la dimensión de seguridad que puede afectar.

Para esto se realiza una escala de valores para determinar el rango de frecuencia de la amenaza

TABLA No. 5 Probabilidad de ocurrencia

Alto (A)
Medio (M)
Bajo (B)

TABLA No. 6 Dimensiones de seguridad

Autenticidad (A)
Confiabilidad (C)
Integridad (I)
Disponibilidad (D)
Trazabilidad del servicio (T)

TABLA No. 7 Escala de rango porcentual Dimensión de Seguridad

Alto (A)
Medio (M)
Bajo (B)

La probabilidad de ocurrencia de una amenaza que puede materializarse, según el análisis que realice para la empresa IBAL se realiza de manera general para cada activo en cada amenaza, la dimensión de seguridad va de acuerdo a lo que pueda afectar en las propiedades de la seguridad de acuerdo a la amenaza. Si se contara la ayuda de la herramienta Pilar, esta identificación sería más precisa y detallada[34].

TABLA No. 8 Identificación de riesgo

Activo/Amenazas	**Probabilidad de Ocurrencia**	**[A]**	**[C]**	**[I]**	**[D]**	**[T]**
Activos						
DATOS / INFORMACIÓN						
Ficheros, Datos de configuración, Datos de gestión interna, Credenciales, Datos de control de acceso, Copia de respaldo y Registro de actividad						
[E.1] Errores de los usuarios	A		M	A	B	
[E.2] Errores del administrador	B		B	M	A	
[E.3] Errores de monitorización (log)	B			A		M
[E.4] Errores de configuración	M			A		

[34] (Rocio, 2013)APLICACION E LA METODOLOGIA MAGERIT, 2013 [En línea] UNIVERSIDAD POLITECNICA SALESIANA SEDE CUENCA, Disponible en https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

[E.15] Alteración accidental de la información	M			A		
[E.18] Destrucción de información	B				A	
[E.19] Fugas de información	M		A			
[E.24] Caída del sistema por agotamiento de recursos	M				A	
[A.3] Manipulación de los registros de actividad (log)	B			A		A
[A.4] Manipulación de la configuración	B		A	A	A	
[A.5] Suplantación de la identidad del usuario	B	M	A	B		
[A.6] Abuso de privilegios de acceso	B		A	M	B	
[A.11] Acceso no autorizado	B		A	M		
[A.15] Modificación deliberada de la información	M			A		
[A.18] Destrucción de información	B				A	
[A.19] Divulgación de información	M		A			
[I.8] Fallo de servicios de comunicaciones	M				A	
SERVICIOS						
Internet, Intercambio electrónico de datos, Transferencia de ficheros, Almacenamiento de ficheros, Correo electrónico						
[E. 1] Errores de los usuarios	A		M	A	B	
[E.2] Errores del administrador	B		B	M	A	
[E.15] Alteración accidental de la información	A			A		
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
E.24] Caída del sistema por agotamiento de recursos	A				A	
[A.5] Suplantación de la identidad del usuario	M	A	A	A		
[A.6] Abuso de privilegios de acceso	M		A	M	B	
[A.11] Acceso no autorizado	B		A	A		
[A.12] Análisis de tráfico	A				A	
[A.14] Interceptación de información (escucha)	A		A			
[A.19] Divulgación de información	M		A			
[A.24] Denegación de servicio	A				A	
[A.25] Robo	M		A		A	
[A.26] Ataque destructivo	B				A	
[I.8] Fallo de servicios de comunicaciones	M				A	

SOFTWARE						
Sistema operativo Microsoft Windows 7Professional licenciado (estaciones de trabajo para desarrolladores e integradores), Windows Update, Gestor de máquinas virtuales, Desarrollo propio (aplicaciones bancarias), Aplicaciones corporativas						
[I. 5] Avería de origen físico y lógico	B				A	
[E. 1] Errores de los usuarios	M		M	A	M	
[E.2] Errores del administrador	B		B	M	A	
[E. 8] Difusión de software dañino	A		B	M	A	
[E.9] Errores de [re-]encaminamiento	B		A			
[E.10] Errores de secuencia	B			A		
[E.15] Alteración accidental de la información	M			A		
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
[E. 20] Vulnerabilidades de los programas (software)	B		B	A	M	
[E. 21] Errores de mantenimiento / actualización de programas (software)	B			A	M	
[A.5] Suplantación de la identidad del usuario	M	A	M	B		
[A.6] Abuso de privilegios de acceso	M		A	M	M	
[A. 7] Uso no previsto	B		A	B	M	
[A.10] Alteración de secuencia	B		A			
[A.11] Acceso no autorizado	B		A	M		
[A.15] Modificación deliberada de la información	M			A		
[A.19] Divulgación de información	M		A			
[A.22] Manipulación de programas	M		A	M	B	
HARDWARE						
Servidor de base de datos, Servidor de aplicaciones, **Mainframe, Work stations de desarrollo, Firewalls**						
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
[I.4] Contaminación electromagnética	B				A	

[I. 5] Avería de origen físico y lógico	B				A	
[I.6] Corte del suministro eléctrico	B				A	
[I.7] Condiciones inadecuadas de temperatura o humedad	B				A	
[I.11] Emanaciones electromagnéticas	B		A			
[I.*] Desastres industriales	B					
[E.2] Errores del administrador	B		B	M	A	
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				A	
E.24] Caída del sistema por agotamiento de recursos	M				A	
[E.25] Pérdida de equipos	B		M		A	
[A.6] Abuso de privilegios de acceso	B		A	M	B	
[A. 7] Uso no previsto	B		A	B	M	
[A.11] Acceso no autorizado	B		A	M		
[A.23] Manipulación de los equipos	B		A		M	
[A.24] Denegación de servicio	M				A	
[A.25] Robo	B		M		A	
[A.26] Ataque destructivo	B				A	
REDES Y COMUNICACIONES						
Red LAN , Red de área local 802.1X, Red VPN, Acceso internet ISP y Red Telefónica básica o RDSI						
[E.2] Errores del administrador	B		M	M	A	
[E.9] Errores de [re-]encaminamiento	B		A			
[E.10] Errores de secuencia	B			A		
E.19] Fugas de información	M		A			
E.24] Caída del sistema por agotamiento de recursos	A				A	
[A.5] Suplantación de la identidad del usuario	M	M	A	B		
[A.6] Abuso de privilegios de acceso	B		A	M	B	
[A. 7] Uso no previsto	M		A	M	A	
[A.9] [Re-]encaminamiento de mensajes	B		A			
[A.10] Alteración de secuencia	B		A			
[A.11] Acceso no autorizado	M		A	M		
[A.12] Análisis de tráfico	A				A	
[A.14] Interceptación de información (escucha)	A		A			
[A.24] Denegación de servicio	A				A	
EQUIPAMIENTO AUXILIAR						
Sistemas de alimentación interrumpida, Generadores eléctricos Diésel,						

Cableado, Fibra óptica, Equipos de climatización, Sistema de extinción de incendios						
[A. 7] Uso no previsto	M		A	B	M	
[A.11] Acceso no autorizado	M		A	M		
[A.23] Manipulación de los equipos	M		A		M	
[A.25] Robo	B		M		A	
[A.26] Ataque destructivo	B				A	
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
[I.4] Contaminación electromagnética	B				A	
[I. 5] Avería de origen físico y lógico	B				A	
[I.6] Corte del suministro eléctrico	B				A	
[I.7] Condiciones inadecuadas de temperatura o humedad	B				A	
[I.9] Interrupción de otros servicios y suministros esenciales	M				A	
[I.11] Emanaciones electromagnéticas	B		A			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				A	
[E.25] Pérdida de equipos	B		M		A	
SOPORTES DE INFORMACIÓN						
Tarjeta de proximidad y código PIN, Electrónicos y no electrónicos						
[A. 7] Uso no previsto	B		A	B	M	
[A.11] Acceso no autorizado	M		A	M		
[A.15] Modificación deliberada de la información	M			A		
[A.19] Divulgación de información	M		A			
[A.23] Manipulación de los equipos	M		A		M	
[A.25] Robo	B		M		A	
[A.26] Ataque destructivo	B				A	
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
[I.4] Contaminación electromagnética	B				A	
[I. 5] Avería de origen físico y lógico	B				A	
[I.6] Corte del suministro eléctrico	B				A	

[I.7] Condiciones inadecuadas de temperatura o humedad	B				A	
[I.10] Degradación de los soportes de almacenamiento de la información	B				A	
[E. 1] Errores de los usuarios	M		M	A	B	
[E.2] Errores del administrador	B		B	M	M A	
[E.15] Alteración accidental de la información	M			A		
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B				A	
[E.25] Pérdida de equipos	B		M		A	
INSTALACIONES						
Oficinas o delegaciones, CPD						
[N.1] Fuego	B				A	
[N. 3] Desastres naturales	B				A	
[I.1] Fuego	B				A	
[I. 2] Daños por agua	B				A	
[I.3] Contaminación mecánica	B				A	
[I.4] Contaminación electromagnética	B				A	
[A.11] Acceso no autorizado	B		A	M		
[A. 7] Uso no previsto	B		A	M	M	
[A.15] Modificación deliberada de la información	M			A		
[A.19] Divulgación de información	M		A			
[A.26] Ataque destructivo	B				A	
[A.27] Ocupación enemiga	B		M		A	
[N.*] Desastres naturales	B					
[E.18] Destrucción de información	M				A	
[E.19] Fugas de información	M		A			
PERSONAL						
Usuarios remotos, desarrolladores, funcionarios para la gestión infraestructura y otros						
[E.7] Deficiencias en la organización	M				A	
[E.19] Fugas de información	M		A			
[A.5] Suplantación de la identidad del usuario	M	M	A	M		
[A.28] Indisponibilidad del personal	M				A	
[A.29] Extorsión	M		A	M	B	
[A.30] Ingeniería social (picaresca)	M		A	M	B	

RIESGOS POTENCIALES Y RESIDUALES

Una vez identificado la probabilidad de ocurrencia de una amenaza sobre un activo de la empresa, se puede determinar el impacto potencial en caso que se materialice, teniendo en cuenta que los activos esenciales son los que requieren mayor atención ya que es donde se centra la información que se maneja y los servicios prestados (datos y servicios). La empresa debe garantizar la continuidad del negocio bajo cualquier circunstancia y brindar total confianza a los usuarios en cuento a la confidencialidad, integridad y disponibilidad del servicio.

La empresa actualmente posee seguridad sobre sus activos, contemplada sobre la protección de las localidades físicas donde se encuentran físicamente sus activos de información y alguna protección lógica a nivel de antivirus o firewall pero no contempla específicamente medidas o salvaguardas para cada activo.

El proceso de tratamiento de riesgos consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños que perjudique las propiedades de la seguridad y afectando de esta manera los activos de la empresa. Debe garantizar como mínimo:

- ✓ Un funcionamiento efectivo y eficiente de la organización.
- ✓ Controles internos efectivos.
- ✓ Conformidad con las leyes y reglamentos vigentes.

Para que el tratamiento de los riesgos sea efectivo, es necesario que la empresa adopte determinadas medidas y acciones encaminadas a modificar, reducir o eliminar el riesgo, que tienen un costo y debes ser asumido por la misma. Igualmente, si no se toma medidas contra el riesgo la empresa debe enfrentarse a pérdidas importantes que pueden afectar el correr del negocio y su credibilidad con los usuarios.

Se debe realizar un análisis teniendo en cuenta, el coste para la empresa de cada una de las diferentes medidas que podríamos adoptar de forma efectiva; frente al

de evaluar y cuantificar las posibles pérdidas que derivarían de la no adopción de medidas contra el riesgo. Al comparar los resultados; podremos saber si debemos actuar o no ante el riesgo, y en caso de decidir actuar, buscar la medida más adecuada para el tratamiento del riesgo que debe ser el más apropiado de acuerdo a su importancia y relevancia en la actividad de la empresa.

ANÁLISIS Y EVALUACIÓN DE RIESGOS, LA MATRIZ DE RIESGOS

Medición Riesgo[35]

Medición del Riesgo		
Potencial	**Probabilidad de Ocurrencia**	**Nivel**
S (Pequeño)	B (Bajo) (0-25)	L (leve) (0-40)
M (Medio)	M (Medio) (26-75)	M (Moderado)(41-80)
L (Grande)	A (Alto) (76-100)	C (Catastrófico) (81-100)

Clasificación Riesgo

Activo: SERVIDORES				
Factor de Riesgo	**Probabilidad de Ocurrencia**	**Nivel de Impacto**	**Vulnerabilidad**	**Amenaza**
Acceso no autorizado	B	C	Falta de protección, puertas del Data Center Ausencia de control de Ingreso al Data Center	Robo, modificación de información

[35] (Erb, s.f.)Gestión de Riesgo en la Seguridad Informática [En línea]. Disponible en https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

Corte de fluido eléctrico, UPS en descarga o con variación de voltaje	B	C	Falta de mantenimiento de la UPS, reguladores, planta eléctrica. Falta de control de nivel de combustible para la planta eléctrica	Falla eléctrica
Destrucción de un componente	B	C	Falta de mantenimiento periódico de los servidores Corto circuito	Polución, humedad, corrosión
Error de configuración	B	M	Falta de personal capacitado en el área Políticas de Seguridad inadecuadas Inestabilidad del Sistema Falta de controles periódicos a la configuración Falta de capacitación continua al personal	Operaciones incorrectas, personal descontento negligencia
Límite de vida útil - Máquinas obsoletas	B	M	Deterioro del funcionamiento. Sistemas desactualizados	Servicios y seguridad desactualizados
Activo: BASES DE DATOS				

Copia no autorizada en medios de datos	M	C	Falta de control de acceso a los sistemas	Robo de información, fraude Daño a la integridad de los datos Daño a los sistemas motores bd
Errores de software	B	M	Falta de Actualizaciones y parches Falta de controles periódicos de verificación de la configuración. Falta de mantenimiento	Caída del servicio Bugs del sistema Huecos de seguridad
Falta de espacio de almacenamiento	M	M	Falta de planeación del crecimiento del sistema Almacenamiento compartido Falta de Mantenimiento	Problemas con nuevos registros
Mala configuración de backups	B	M	Falta de políticas adecuadas Falta de procedimientos documentados Falta de Control periódico	Perdida de información, perdida de integridad de la información, restauraciones fallidas.

			Backups realizados no concurrentes Backups parciales	
Mala integridad de los datos	B	M	Falta de Mantenimiento	Datos corruptos
Medios de datos no están disponibles cuando son necesarios	M	M	Falta de monitoreo adecuado Falta de Tuning de las base de datos y aplicaciones	Fallas de software, hardware y o red de datos, ataques de DDOS
Pérdida de backups	B	C	Falta de control adecuado de rotación de backups Falta de políticas adecuadas Backups Expuestos Backups almacenados en equipos sin protección Falta de redundancia en los backups	Robo de información, barrado de información, divulgación de la información, virus
Perdida de confidencialidad en datos privados y de sistema	B	C	Backups almacenados en equipos sin protección Backups expuestos	Robo de información, alteración de información, virus

Sabotaje	B	C	Falta de controles de acceso físicos Falta de controles accesos lógicos Falta de controles de seguridad (antivirus, firewall)	Vandalismo, perdida de datos, divulgación de información, virus
Activo: SOFTWARE DE APLICACIÓN, PROGRAMAS FUENTE				
Acceso no autorizado a datos (borrado, Modificación, etc.)	B	C	Falta de controles de accesos. Falta de mecanismos de monitorización Falta de Control de usuarios cesados Existencia de puntos de la red sin ningún control de seguridad Políticas de seguridad inadecuadas Falta de capacitación sobre valores y ética profesional	Robo, Perdida divulgación, alteración de la información. Sabotaje, vandalismo. Personal interno (descontento, negligencia, deshonestidad, cesados, etc)
Aplicaciones sin licencia	B	B	Políticas de Seguridad inadecuadas.	Multas, Demandas.

			Falta de control y monitoreo. Equipos con usuario administrador sin protección o restricción	
Error de configuración	B	B	Políticas inadecuadas. Personal no capacitado. Falta de mecanismos de monitorización.	Daño del sistema. Perdida de confidencialidad
Errores en las funciones de encriptación	M	M	Software obsoleto. Falta de nieles de administración.	Perdida de la confidencialidad . Robo de información
Falta de compatibilidad	B	B	Falta de control de versiones. Software desactualizado.	Falla de la prestación del servicio.
Falta de confidencialidad	M	C	Usencia de control de los sistemas. Ausencias de sistemas de seguridad. Políticas inadecuadas.	Robo, alteración y divulgación de la información
Mala administración de control de acceso	B	M	Ausencia de administración. Personal o capacitado.	Suplantación de identidad. Autorización elevada de privilegios. Robo, alteración y divulgación de la información
Poca adaptación a cambios del sistema	B	B	Ausencia de capacitación. Proyectos inmaduros.	Fallas en el sistema. Rechazo al sistema.

			Mal diseño de sistemas	Corrupción de datos.
Prueba de software deficiente	B	M	Ausencia de control de versiones. Necesidades inmediatas. Falta de personal de pruebas. Ausencia de ambiente de pruebas	Fallas en el sistema, Corrupción de datos. Información privilegiada expuesta.
Falla del sistema	M	C	Ausencia de mecanismos de control y monitoreo. Falta de mayor cantidad de persona especializado	Corte en la prestación del servicio.
Software desactualizado	B	B	Ausencia de mecanismos de monitoreo. Ausencia de mecanismos para despliegue de actualizaciones y parches. Softwares sin soporte.	Virus
Activo: ALMACENAMIENTO				
Copia no autorizada a un medio de datos	B	C	Falta o imprecisión de políticas sobre uso de medios de almacenamiento externo	Información privilegiada conocida por terceros
Errores de software	B	B	Copias de volúmenes información grandes	Perdida de integridad en los datos

			Fallas en los procesos lógicos de transferencia de datos	
Falla en medios externos	B	B	Daños físicos en medios externos Perdida de medios externos	Perdida o inaccesibilidad de información
Falta de espacio de almacenamiento	B	M	Almacenamiento compartido Falta de políticas sobre tipos de archivos a almacenar	
Mala configuración de backups	B	M	Copia de información innecesaria Periodicidad de copias indebidas	Espacio de almacenamiento mal utilizado Respaldo de datos desfasados
Mala integridad de los datos resguardados.	B	M	Procesos de copias de datos fallidos	Información no acta para su lectura
Medios de datos no están disponibles cuando son necesarios	B	M	Falta de rotulación en las copias de seguridad realizadas	Información no actualizada en el momento indicado
Pérdida de backups	B	C	Sistemas no integrales	
Robo	B	C	Información privilegiada expuesta	Información privilegiada conocida por terceros
Sabotaje	B	M	Falta de control sobre el nivel de acceso a la información	Falta de disponibilidad, integridad y accesibilidad en la información

Spoofing y Sniffing	B	M	Información privilegiada expuesta	Perdida de integridad en los datos
Activo: CABLEADO Y EQUIPOS ACTIVOS				
Conexión de cables inadmisible	M	M	Uso de medios de conexión no certificados	Perdida de comunicación entre nodos de red. Loops en la red
Daño o destrucción de cables o equipamiento inadvertido	A	C	Falta de control o inspección a los centros de cableado Hojas de vida de equipos activos desactualizadas	Nodos de red desconectados Comunicaciones fallidas
Factores ambientales	M	C	Exceso de calor en los centros de cableado	Deterioro de los componentes electrónicos de los equipos de comunicaciones
Interferencias	M	M	Espectro electromagnético compartido en redes WiFi Equipos de potencia cercanos a los de comunicaciones	Bloqueos e intermitencias del servicio
Límite de vida útil de equipos.	A	C	Falta de equipos de soporte en inventario	Perdida o caída del servicio
Longitud de los cables de red excedida	B	M	Certificaciones de cableado adulteradas	Transmisión de datos deficiente
Reducción de velocidad de transmisión	M	M	Medios desprotegidos Equipos activos obsoletos	Desgaste del medio o tiempos de vida útil excedidos

Riesgo por el personal de limpieza o personal externo	A	M	Inexperiencia en estática eléctrica Falta de control en ingreso a los centros de cableado	Daño físico a los equipos activos Puntos de conexión a la red

Lista Riesgo

Factor de Riesgo	**Probabilidad de Ocurrencia**	**Nivel de Impacto**
Acceso no autorizado	B	C
Corte de luz, UPS descargado o variaciones de Voltaje.	B	C
Destrucción de un componente	B	C
Error de configuración	B	M
Límite de vida útil - Máquinas obsoletas	B	M
Copia no autorizada de un medio de datos	M	C
Errores de software	B	M
Falta de espacio de almacenamiento	M	M
Mala configuración de backups	B	M
Mala integridad de los datos	B	M
Medios de datos no están disponibles cuando son necesarios	M	M
Pérdida de backups	B	C
Perdida de confidencialidad en datos privados y de sistema	B	C
Sabotaje	B	C
Acceso no autorizado a datos (borrado, Modificación, etc.)	B	C
Aplicaciones sin licencia	B	B
Error de configuración	B	B
Errores en las funciones de encriptación	M	M
Falta de compatibilidad	B	B
Falta de confidencialidad	M	C
Mala administración de control de acceso.	B	M

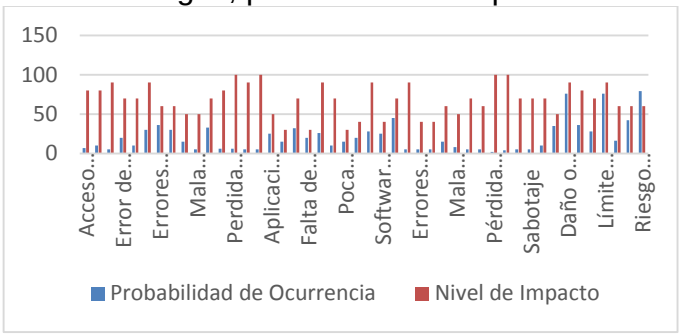
Poca adaptación a cambios del sistema	B	B
Prueba de software deficiente	B	M
Falla del sistema	M	C
Software desactualizado	B	B
Virus	M	M
Copia no autorizada a un medio de datos	B	C
Errores de software	B	B
Falla en medios externos	B	B
Falta de espacio de almacenamiento	B	M
Mala configuración de backups	B	M
Mala integridad de los datos resguardados.	B	M
Medios de datos no están disponibles cuando son necesarios	B	M
Pérdida de backups	B	C
Robo	B	C
Rótulos inadecuado en los medios de datos	B	M
Sabotaje	B	M
Spoofing y sniffing	B	M
Conexión de cables inadmisible	M	M
Daño o destrucción de cables o equipamiento inadvertido	A	C
Factores ambientales	M	C
Interferencias	M	M
Límite de vida útil de equipos.	A	C
Longitud de los cables de red excedida	B	M
Reducción de velocidad de transmisión	M	M
Riesgo por el personal de limpieza o personal externo	A	M

Matriz Riesgo

Riesgo		Probabilidad		
		B	M	A
Impacto	S	L	L	M
	M	M	M	C
	L	C	C	C

1.

Riesgos, probabilidad e Impacto



DECLARACIÓN DE APLICABILIDAD

LR: Requisitos Legales, CO: Obligaciones Contractuales, BR/BP: Requerimientos del Negocio/Mejores Prácticas Adoptadas, RRA: Resultados de la Evaluación de Riesgos[36]

Dominio de Seguridad	Control	Nombre Control	Descripción del Control	Selección del control y las razones de su selección				Aplicabilidad	Justificación
				LR	CO	BR/ BP	RRA		
A.5 **Políticas de seguridad** **de la información**	A.5.1	Orientación de la dirección para la gestión de la seguridad de la Información	Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.						

[36] (ISO 27000.es, 2005)ISO 27000.es, El portal de ISO 27001 en Español [En línea]. ISO 27000.es. Disponible en http://www.iso27000.es/sgsi.html#home

	A.5.1.1	Políticas para la seguridad de la información	Redacción del documento sobre la política de seguridad de información para la empresa IBAL				X	SI	La empresa ya cuenta con un documento de declaración de aplicabilidad versión 1.0
	A.5.1.2	Revisión de las políticas para la seguridad de la información	Revisión periódica al documento de las políticas de seguridad de información por parte del Comité de Seguridad en asocio con la Alta Dirección			X		SI	En base al ciclo de Deming y con la intención de identificar la efectividad de la política.
A.6 **Organización de la seguridad de la información**	A.6.1	Organización interna	La dirección debería aprobar la política de seguridad de la información, asignar las funciones de seguridad, coordinar y revisar la implementación de la seguridad en toda la empresa IBAL						

	A.6.1.1	Roles y responsabilidades para la seguridad de la información. Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización.	En el documento de la política de seguridad de la información se plasma el compromiso manifiesto de las máximas autoridades de la empresa y de los jefes de área para la difusión, consolidación y cumplimiento de los principios de seguridad que rigen a la empresa IBAL			X		SI	La empresa IBALmediante su política de seguridad de la información debe establecer el compromiso, organización y asignación de responsabilidades para su cumplimiento de la misma.

	A.6.1.2	Separación de deberes Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones y de los distintos sectores que forman la Organización	En el documento de la política de seguridad de la información se establece la conformación de un comité de seguridad de la información, integrado por miembros de distintos sectores de la organización.			X		SI	La información es un activo transversal para toda organización, por ende la seguridad de la misma es compromiso de diversas áreas de la empresa.
	A.6.1.3	Contacto con las autoridades	En el documento de la política de seguridad de la información, se establecen las responsabilidades frente a la seguridad de la información.	X				SI	La empresa debe cumplir con las leyes, por lo tanto debe mantener contacto permanente con las autoridades especialmente

			Todos los empleados deben cumplir las leyes y regulaciones nacionales e internacionales respecto a derechos de autor y propiedad intelectual, comercio electrónico e intercambio electrónico de datos						con la finalidad de verificar el uso adecuado de los activos de información.
		A.6.1.4	Contactos con grupos de interés especial	En el documento de la política de seguridad de la información, se establecen las responsabilidades frente a la seguridad de la información.			X		SI	Se debe garantizar el contacto permanente con empresas dedicadas al desarrollo de Software, en aras de mantener actualizado al personal y con

			La Organización por medio de contratos comerciales o civiles, alianzas o convenios que tenga con el personal externo y que posea acceso a la información del proyecto deberá acatar el modelo normativo de seguridad de la información.						entidades que se especialicen en la seguridad de la Información.
	A.6.1.5	Seguridad de la información en la gestión de proyectos	El acceso a los activos de información está sujeto a validación por parte del personal encargado de la seguridad de la información en la Organización, para que no se otorgue acceso a la información confidencial sin la existencia de una autorización y compromiso	X	X	X	X	SI	El comité de seguridad establece unos parámetros base para ser tenidos en cuenta en los proyectos que aborda la empresa

			explícitos, los cuales deben estar respaldados por un acuerdo escrito de confidencialidad y/o de no-revelación, total ni parcial de información.						
	A.6.2	Dispositivos móviles y teletrabajo	Controles enfocados a la movilidad						
	A.6.2.1	Política para dispositivos móviles Políticas para gestionar los riesgos introducidos por el uso de dispositivos móviles	En la Gestión integral de la Seguridad de la Información, las actividades relacionadas con dispositivos móviles deben ser contempladas			X	X	NO	No ha sido definido en el Sistema de Gestión de la Seguridad de la Información.

	A.6.2.2	Teletrabajo	E es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo	X				NO	Existe la ley 1221 de 2008 la cual regula el teletrabajo en Colombia. La empresa IBAL no cuenta con empleados bajo la modalidad de Teletrabajo

A.7 Seguridad de los recursos humanos	A.7.1	Antes de asumir el empleo	Asegurar que los empleados, contratistas y usuarios de terceras partes entienden sus responsabilidades y sean aptos para las funciones para las cuales están considerados, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones						
	A.7.1.1	Selección	Se establece el procedimiento adecuado para la selección y contratación de personal,	X		X		SI	La empresa IBAL debe contar con procedimientos para la selección de personal que incluye investigación de antecedentes, realizar revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con

		Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para trabajos sensibles							las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
	A.7.1.2	Términos y condiciones del empleo	Inclusión a manera de anexos en los contratos de los empleados, una póliza o cláusula de confidencialidad de la información de la empresa.	X		X		SI	El área jurídica establece los mecanismos legales que garanticen la seguridad de la información corporativa.

	Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de información deberían firmar un acuerdo sobre sus funciones y responsabilidades de seguridad							
A.7.2	Durante la ejecución del empleo.	Es conveniente definir las responsabilidades de la dirección para garantizar que se aplica la seguridad durante todo el contrato laboral de una persona dentro de la organización						Establecer condiciones contractuales para la seguridad de la información
A.7.2.1	Gestión de Responsabilidades	La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los			X		SI	Identificar las funciones de cada usuario permite establecer las responsabilidades específicas que deben asumir.

		procedimientos establecidos de la organización.						
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la Información	Realizar campañas y actividades que sensibilicen a sus colaboradores sobre la seguridad de la Información mediante: Inducción y reinducción., charlas al personal, difusión a través de la página web y en todos los medios de comunicación que posee la empresa.			X		SI	La empresa IBAL Brinda un nivel adecuado de concientización, educación y formación en los procedimientos de seguridad, y el uso correcto de los servicios de procesamiento de información a todos los empleados, contratistas y usuarios de terceras partes para minimizar los posibles riesgos de seguridad.

		Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo							
	A.7.2.3	Proceso disciplinario	Establecer un proceso disciplinario formal para el manejo de las violaciones de seguridad., contemplado en el	X		X		SI	Puesta en servicio de la Oficina de Control Interno

			documento de la política de seguridad de la información, se establecen sanciones por incumplimiento.						
		En caso de no cumplir con los criterios de Seguridad de la información, la empresa Ibal debe contar con procesos disciplinarios conforme al marco legal.							
	A.7.3	Terminación y cambio de empleo	Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.			**x**			Definir terminos de contrato legales
	A.7.3.1	Terminación o cambio	Al finalizar un contrato con la empresa, el área de recursos humanos y administrativa es responsable de verificar que todos				X	SI	Se deben establecer un proceso que permita identificar aquellos usuarios que han sido desvinculados de

			los activos de la organización que estén en posesión de empleados, contratistas y terceros sean devueltos.							la empresa para suspender sus credenciales de acceso a los diversos sistemas informáticos al interior.
		de responsabilidades de empleo	Deshabilitación de usuarios, se establecen los procedimientos de retiro de permisos para los usuarios en los sistemas de información. Cuando se presenta un cambio o retiro del cargo se debe diligenciar el formato para este fin.							

		Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas							
A.8 Gestión de activos	*A.8.1*	Responsabilidad por los activos Lograr mantener la protección adecuada de los activos de la organización.							
A.8 Gestión de activos	A.8.1.1	Inventario de activos Identificar todos los activos propios de la organización.	Establecer un procedimiento inventario y clasificación de activos de información			X		SI	Actividad requerida para conocer y clasificar los activos de Información.

	A.8.1.2	Propiedad de los activos Se deben identificar los dueños para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados	Establecer un procedimiento inventario y clasificación de activos de información			X		SI	Documentar responsabilidades sobre la asignación de activos
	A.8.1.3	Uso aceptable de los activos	Políticas contenidas en el manual de seguridad de la información sobre de uso de los recursos tecnológicos			X		SI	Contar con políticas para el manejo y uso de recursos tecnológicos
	A.8.1.4	Devolución de activos	Procedimiento de entrega de cargos			X	X	SI	Asegurar la integridad, confidencialidad y disponibilidad de los activos de información durante el proceso de retiro,

									renuncia y traslados de personal
	A.8.2	Clasificación de la información							
	A.8.2.1	Clasificación de la información	Busca la caracterización de los activos relacionados con la información			X	X	SI	Actividad realizada previamente donde se identifica cada activo relacionado con la información de la empresa
	A.8.2.2	Etiquetado de la información	Procedimiento definido para facilitar la identificación de la información			X		SI	Actividad realizada previamente donde se identifica cada activo relacionado con la información de la empresa
	A.8.2.3	Manejo de activos	Procedimientos claros para definir la manera de actuar u operar los activos			X	X	SI	Actividad realizada previamente: Manual de procedimientos

			identificados en la empresa.						relacionados con los activos
	A.8.3	Manejo de medios	Procedimientos de control claros que permiten definir la manera de actuar u operar los medios de información de la empresa.						
	A.8.3.1	Gestión de medios removibles	Especificación de la manera de administrar los medios extraíbles de información			X	X	SI	De acuerdo al análisis de Riesgos realizado previamente en la empresa.
	A.8.3.2	Disposición de los medios	Identificación de acciones específicas que permitan establecer el destino final de un medio de información			X	X	SI	Procedimiento requerido para el tratamiento de los medios
	A.8.3.3	Transferencia de medios físicos	Procedimiento para determinar las acciones requeridas para resguardar la información contenida en los medios físicos			X	X	SI	Procedimiento requerido para el tratamiento de los medios

A.9	*A.9.1*	Requisitos del negocio para control de acceso	Procedimientos para establecer un correcto control de acceso						
	A.9.1.1	Política de control de acceso	Debe contemplar todos los requerimientos de seguridad de cada una de las aplicaciones y definir perfiles o privilegios para cada tipo de usuario.			X		SI	Definido previamente en Sistema de Gestión
Control de acceso	A.9.1.2	Acceso a redes y a servicios en red	El proceso de Gestión de Tecnologías liderado por la Oficina de Sistemas debe establecer bloqueos o excepciones de acceso según la necesidad o funciones de los usuarios			X		SI	Definido previamente en Sistema de Gestión
	A.9.2	Gestión de acceso de usuarios	Proceso de administración de perfiles y derechos de usuarios						

	A.9.2.1	Registro y cancelación del registro de usuarios	Proceso liderado por la Oficina de Talento Humano, que determina quién es vinculado o retirado de la empresa			X		SI	Identificar el personal permite gestionar correctamente el acceso a los diferentes Sistemas de la empresa.
	A.9.2.2	Suministro de acceso de usuarios	De acuerdo al filtro establecido en el registro de usuarios, se procede a asignar el acceso al personal que debe contar con el mismo.			X		SI	Se gestiona correctamente el acceso a los usuarios
	A.9.2.3	Gestión de derechos de acceso privilegiado	Se identifica el nivel de privilegio con que debe contar cada usuario según sus funciones			X		SI	Se gestiona correctamente el acceso a los usuarios
	A.9.2.4	Gestión de información de autenticación secreta de usuarios	Se establecen los datos de acceso a los Sistemas de Información, los cuales deberán estar conformados como mínimo por nombre			X		SI	Se gestiona correctamente el acceso a los usuarios

		de usuario o ID y contraseña.						
A.9.2.5	Revisión de los derechos de acceso de los usuarios	Se deberán realizar revisiones periódicas a los privilegios de acceso concedidos en los diferentes sistemas de información a los empleados.			X		SI	Se gestiona correctamente el acceso a los usuarios
A.9.2.6	Retiro o ajuste de los derechos de acceso	Validación frente a la calidad del empleado (activo, desvinculado) de los derechos asignados			X		SI	Se gestiona correctamente el acceso a los usuarios
A.9.3	Responsabilidades de los usuarios	Proceso para identificar los deberes del usuario frente a la Seguridad Informática de la empresa						
A.9.3.1	Uso de información secreta de autenticación	Establecimiento y verificación de buenas prácticas en manejo de datos de acceso para los empleados.			X		SI	Se debe garantizar que los datos de acceso a los diferentes Sistemas de la empresa sean

								manejados de la mejor manera.
A.9.4	Control de acceso a sistemas y aplicaciones	Se enfoca en determinar los procedimientos para conceder acceso a los diversos sistemas informáticos						
A.9.4.1	Restricción de acceso a la información	Se debe evitar que usuarios no autorizados tengan acceso a la información			X	X	SI	La empresa IBAL mediante su política de seguridad de la información establece las restricciones de acceso
A.9.4.2	Procedimiento de ingreso seguro	Se debe garantizar la confidencialidad de los datos y la trazabilidad de las actividades realizadas por cada usuario.	X		X		SI	La política de seguridad de la empresa debe generar confianza al usuario
A.9.4.3	Sistema de gestión de contraseñas	Establecimiento de longitud, nivel de complejidad y calidad de las contraseñas permitidas en los			X		SI	Se requiere validación en el ingreso a los sistemas e implementación de niveles

			diversos sistemas de informáticos de la empresa.						aceptables de seguridad.
	A.9.4.4	Uso de programas utilitarios privilegiados	Solo el personal del área de soporte debe hacer uso de este tipo de software			X	X	SI	Es vital para empresa gestionar correctamente el software instalado en sus equipos de cómputo.
	A.9.4.5	Control de acceso a códigos fuente de programas	Teniendo en cuenta que es el activo principal de la empresa, se debe restringir el acceso al código fuente generado y al de los programas adquiridos.	X		X		SI	La política de seguridad debe establecer que solo el personal autoriza acceda al código fuente
A.10 Criptografía	*A.10.1*	*Controles criptográficos*	Procedimiento pensado para la protección de la confidencialidad, integridad y disponibilidad de la información						

	A.10.1.1	Política sobre el uso de controles criptográficos	Se debe identificar qué nivel de protección adicional (certificados, llaves, etc.) requieren los sistemas informáticos para determinar su implementación	X		X	X	SI	La empresa puede hacer uso de herramientas de open source o adquirir una comercial dependiendo del nivel de control requerido.
	A.10.1.2	Gestión de llaves	Se debe generar el sistema de gestión de llaves criptográficas según la necesidad detectada.	X		X	X	SI	La empresa puede hacer uso de herramientas de open source o adquirir una comercial dependiendo del nivel de control requerido.
A.11	*A.11.1*	*Áreas seguras*	Procedimiento para determinar aquellas zonas que deben ser aseguradas o requieran de control específico en la empresa						
	A.11.1.1	Perímetro de seguridad física	Establecer áreas específicas que deban ser aseguradas perimetralmente de acuerdo al tipo de			X	X	SI	Los activos informáticos deben ser resguardados con especial protección, se

			activos o de información que maneja. Ejm: DataCenter principal.						debe contemplar un nivel de seguridad superior
Seguridad física y del entorno	A.11.1.2	Controles de acceso físico	Establecer sistemas de control de acceso como sensores, cámaras, carné de identificación para cada empleado, etc.			X	X	SI	Se debe identificar quien está en la empresa y cuando lo hace, para garantizar un nivel de seguridad óptimo.
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe evitar el acceso a personal no autorizado a la empresa.			X		SI	La empresa cuenta con una recepción principal que funciona las 24 Horas y que tiene definida políticas de acceso al personal en horas no convencionales.
	A.11.1.4	Protección contra amenazas externas y ambientales	Se debe contar con equipos de control ambiental en el centro de datos y alimentación redundante para contribuir a la			X		SI	La empresa cuenta con equipos para el control de la temperatura y humedad en el DataCenter,

			continuidad del servicio.						sistemas de extinción de incendios y UPS de respaldo
	A.11.1.5	Trabajo en áreas seguras	Identificación y protección de zonas de trabajo seguro.			X		SI	Se debe evitar el acceso no autorizado, daños o alteraciones de la infraestructura de la empresa. No solo centrar los esfuerzos en el CPD o Data Center
	A.11.1.6	Áreas de despacho y carga	Se debe evitar que las áreas de carga o entrega de mercancía sean cercanas a los activos de información.			X		SI	Se debe incluir el en documento de políticas de seguridad con el ánimo de que personal externo no acceda fácilmente a los activos de Información.
	A.11.2	*Equipos*	Procedimientos determinados para resguardar la seguridad de los						

		equipos de cómputo de la empresa						
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar dispuestos en puntos estratégicos que dificulten el uso o acceso no autorizado a los mismos			X	X	SI	De acuerdo al análisis de riesgos se puede plantear una ubicación adecuada para los equipos informáticos de la empresa.
A.11.2.2	Servicios de suministro	Se debe proteger los equipos contra fallas en el fluido eléctrico	X		X	X	SI	El Data Center cuenta con UPS con soporte de 15 minutos y sistema de planta eléctrica alimentada por combustible diesel que entra en funcionamiento al detectar falla en fluido eléctrico comercial.

	A.11.2.3	Seguridad del cableado	Se debe procurar que los centros de cableados y equipos de comunicaciones no cuenten con facilidad de acceso para evitar que terceros ingresen y se conecten a la red o realicen daños en la infraestructura.			X	X	SI	La empresa debe establecer en su política de seguridad el cumplimiento de estándares y normas de cableado estructurado.
	A.11.2.4	Mantenimiento de equipos	Se debe establecer hoja de vida a los equipos informáticos y establecer plan de mantenimiento preventivo, correctivo y predictivo a los mismos.			X		SI	La empresa cuenta con plan de mantenimiento a equipos garantizando la disponibilidad e integridad de los mismos.
	A.11.2.5	Retiro de activos	No deben ser retirados equipos o datos de los mismos, de las instalaciones de la empresa			X	X	SI	La política de seguridad de la empresa debe contener explícitamente esta información.

	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se debe contemplar la implementación de un tipo de seguridad para los equipos que se encuentran fuera de la empresa teniendo en cuenta los riesgos a que pueden estar la información contenida en los mismos.			X	X	SI	La política de seguridad de la empresa debe contener explícitamente esta información.
	A.11.2.7	Disposición segura o reutilización de equipos	Todos los equipos deben ser verificados con la finalidad de eliminar datos sensibles o licenciamiento que puedan contener antes de ser reutilizados o eliminados			X		SI	La empresa debe establecer por medio del área de soporte los mecanismos idóneos para desechar o reutilizar equipos.
	A.11.2.8	Equipos de usuarios desatendidos	Establecer mecanismos de protección a los equipos no supervisados como portátiles del personal administrativo.			X		SI	La política de seguridad de la empresa debe ser clara en el sentido de especificar los procedimientos de protección a dispositivos que

									constantemente salen de la red LAN
	A.11.2.9	Política de escritorio limpio y pantalla limpia	La empresa debe establecer una política concreta frente al uso de medios extraíbles y acumulación de documentación física en los puestos de trabajo de los empleados.			X		SI	El documento con las políticas debe indicar las practicas recomendadas frente a esta situación
A.12 Seguridad de las operaciones	*A.12.1*	Procedimientos operacionales y responsabilidades	Se deberían establecer las responsabilidades y procedimientos para la gestión de los medios procesamiento de la información						
	A.12.1.1	Procedimientos de operación documentados	Los manuales de funciones u operación deben estar disponibles			X		SI	El sistema de Gestión establece la disponibilidad de la documentación de

			siempre que sean requeridos.						los procedimientos
	A.12.1.2	Gestión de cambios	Los cambios que afectan la seguridad de la Información deben ser controlados por el departamento de Seguridad Informática			X		SI	Procedimiento Gestión de cambios
	A.12.1.3	Gestión de capacidad	La empresa debe monitorear y gestionar el uso de los recursos disponibles para garantizar su rendimiento			X		SI	Los sistemas requieren capacidad de procesamiento por lo tanto el sistemas de Gestión debe contemplarlo
	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Con el ánimo de reducir riesgos de acceso o modificación en el ambiente de operación, se deben separar tanto los de desarrollo y pruebas del ambiente de operación			X		SI	La empresa cuenta con la política de seguridad previamente establecida, los desarrolladores solo pueden ingresar a los entornos de

									desarrollo y para esto cuentan con un entorno simulado y uno similar al de los clientes
	A.12.2	Protección contra códigos maliciosos	Procedimientos dedicados a la protección lógica del software						
	A.12.2.1	Controles contra códigos maliciosos	Se deben implementar mecanismos de protección tecnológicos como software Antivirus y capacitaciones periódicas sobre buenas prácticas de navegación en Internet			X	X	SI	La empresa establece en su política de seguridad el control sobre software malicioso. Cuenta con IDS y Firewall instalados en la sede
	A.12.3	Copias de respaldo	Su principal finalidad es mantener la integridad y la disponibilidad de los servicios relacionados con la información.						

	A.12.3.1	Respaldo de la información	Se deberán programar copias de seguridad periódica y mecanismos de restauración de la misma para garantizar la funcionalidad de los procesos realizados.			X		SI	No ha sido puesto en funcionamiento aún en la empresa
	A.12.4	*Registro y seguimiento*	Se deben monitorear constantemente los sistemas informáticos de la empresa y registrar los eventos de seguridad que sean detectados.						
	A.12.4.1	Registro de eventos	Se deben mantener los registros de las actividades realizadas por cada usuario			X		SI	Implementación de un sistema de centralización de logs con la finalidad de generar correlación de eventos.
	A.12.4.2	Protección de la información de registro	La información de los log registrada debe ser protegida para evitar su alteración o consulta no autorizada.			X		SI	El departamento de seguridad informática es quien debe tener acceso directo a esta información.

	A.12.4.3	Registros del administrador y del operador	Al igual que las actividades de un usuario estándar, las de un usuario administrador u operador de los diversos sistemas, también deben ser registradas.			X		SI	Implementación de un sistema de centralización de logs con la finalidad de generar correlación de eventos.
	A.12.4.4	Sincronización de relojes	Todos los relojes internos de los Sistemas de Información deben ser sincronizados, para conservar una sola referencia horaria en los sistemas de log.			X		SI	La correlación de eventos es precisa cuando los relojes de los sistemas de información involucrados están sincronizados
	A.12.5	Control de software operacional	Se debe efectuar un análisis de riesgos previo a la modificación de un software que se encuentre en producción.						
	A.12.5.1	Instalación de software en sistemas operativos	Se deben poner en marcha mecanismos que permitan condicionar la instalación de software en			X		SI	Se debe establecer políticas de implantación de actualizaciones o modificaciones a

			Sistemas en estado de producción.						todo el software de la empresa.
	A.12.6	Gestión de la vulnerabilidad técnica	Se debe evitar al máximo la explotación de vulnerabilidades técnicas sobre los sistemas de la empresa.						
	A.12.6.1	Gestión de las vulnerabilidades técnicas	Indagar constantemente sobre las vulnerabilidades detectadas en los sistemas de información para emprender actividades de mitigación de riesgos.			X		SI	Examinación del documento elaborado previamente de identificación de vulnerabilidades
	A.12.6.2	Restricciones sobre la instalación de software	Establecimiento e implementación de reglas que rijan instalación de software por parte de los usuarios.			X	X	SI	Política establecida previamente por el departamento de seguridad informática

	A.12.7	Consideraciones sobre auditorias de sistemas de información	Se debe minimizar el impacto de las actividades de auditoria en los sistemas de producción						
	A.12.7.1	Controles de auditoria de sistemas de información	Se deben minimizar las interrupciones en los software misionales planificando y organizando las tareas de auditoria sobre los mismos.			X		SI	Identificar previamente los requisitos y actividades de auditoria a realizar
A.13 Seguridad de las comunicaciones	*A.13.1*	Gestión de la seguridad de las redes	Se debe evitar el acceso físico no autorizado, los daños e interferencias a la información de la organización.						
	A.13.1.1	Controles de redes	Se deben administrar y controlar las redes para proteger la información trasmitida en las primeras.			X		SI	El departamento de Seguridad Informática de la empresa realiza periódicamente revisión a las políticas relacionadas con la red de datos

	A.13.1.2	Seguridad de los servicios de red	Todos los servicios de red, deben contar con su respectivo acuerdo de servicio			X	X	SI	Los servicios de red deben estar debidamente caracterizados para determinar adecuadamente sus mecanismos de seguridad
	A.13.1.3	Separación en las redes	Implementación de VLANS según las dependencias, grupos de usuarios, o manejo de información			X		SI	La empresa cuenta con una segmentación ya definida; los desarrolladores se encuentran en un segmento diferente al resto de usuarios.
	A.13.2	Transferencia de información	Se debe mantener la seguridad de la información que se transfiere internamente en la empresa y con entidades externas.						
	A.13.2.1	Políticas y procedimientos de transferencia de información	Se deben establecer procedimientos formales y documentados de transferencia de información a través las redes de datos			X		SI	Se debe implementar la política de transferencia de información.

	A.13.2.2	Acuerdos sobre transferencia de información	Deben tratar principalmente la transferencia segura de información entre la misma empresa y esta con terceros.			X		SI	Se debe implementar la política de transferencia de información.
	A.13.2.3	Mensajería electrónica	Se debe proteger la información transmitida en medios electrónicos			X		SI	Se debe implementar la política de transferencia de información.
	A.13.2.4	Acuerdos de confidencialidad o de no divulgación	La empresa deberá identificar, revisar y documentar constantemente los requisitos relacionados con la divulgación de la información			X		SI	Se debe implementar la política de transferencia de información.
A.14 Adquisición, desarrollo y mantenimiento de sistemas	*A.14.1*	*Requisitos de seguridad de los sistemas de información*	Se debe garantizar que la seguridad sea requisito esencial de los sistemas de información						
	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos de seguridad deben contemplados siempre en la compra de nuevo software y en la			X		SI	Plan de compras y procedimiento de desarrollo de software deben ser tenidos en cuenta.

			actualización de los existentes.						
	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	La información transmitida por medio de redes públicas deben ser protegidas contra actividades irregulares			X		SI	Las aplicaciones web desarrolladas y comercializadas por la empresa IBAL, cuentan con mecanismos de autenticación y manejo de sesiones, pensando en mejorar la seguridad de la información se podría implementar conexiones VPN.
	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Las transacciones realizadas por medio de redes públicas deben ser protegidas contra actividades irregulares			X		SI	Las transacciones vía web pueden ser controladas mediante certificados criptográficos

	A.14.2	*Seguridad en los procesos de desarrollo y soporte*	La seguridad de la información debe ser diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.						
	A.14.2.1	Política de desarrollo seguro	Se deben actualizar o establecer políticas de desarrollo de software y sistemas al interior de la empresa.			X		SI	El procedimiento de desarrollo de software debe ser tenido en cuenta.
	A.14.2.2	Procedimientos de control de cambios en sistemas	Se deben establecer procedimientos específicos para el control de cambios en el ciclo de desarrollo			X		SI	El procedimiento de desarrollo de software y el de gestión del cambio deben ser tenidos en cuenta.
	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Se deben establecer mecanismos de prueba a los sistemas de producción críticos, luego de cualquier cambio sobre el sistema base			X		SI	El procedimiento de desarrollo de software y el de gestión del cambio deben ser tenidos en cuenta.

	A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deben evitar modificaciones a los paquetes de software suministrados por terceros y de ser necesario aplicar solo los necesarios.			X			El procedimiento de desarrollo de software y el de gestión del cambio deben ser tenidos en cuenta.
	A.14.2.5	Principios de construcción de los sistemas seguros	Se deben aplicar principios de ingeniería de sistemas en búsqueda de una correcta implementación en los sistemas de información			X		SI	El procedimiento de desarrollo de software y el de gestión del cambio deben ser tenidos en cuenta.
	A.14.2.6	Ambiente de desarrollo seguro	Se debe disponer de un adecuado entorno de desarrollo e integración de sistemas			X		SI	Ya se cuenta con un entorno de desarrollo en la empresa, aunque por ahora es simulado directamente en los puestos de trabajo de los desarrolladores.

	A.14.2.7	Desarrollo contratado externamente	Se debe contemplar la posibilidad de tercerizar algunos servicios, dependiendo del grado de usabilidad de cada uno.			X		NO	La empresa no aplica este control, teniendo en cuenta que las actividades pueden ser realizadas por personal contratado
	A.14.2.8	Pruebas de seguridad de sistemas	Se deben realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.			X		SI	El procedimiento de desarrollo de software y el de gestión del cambio deben ser tenidos en cuenta.
	A.14.2.9	Prueba de aceptación de sistemas	Se deben establecer criterios de pruebas y aceptación de software			X		SI	El procedimiento de desarrollo de software y el de gestión del cambio deben ser tenidos en cuenta.
	A.14.3	*Datos de prueba*	Se debe garantizar la protección de los datos utilizados para escenarios de pruebas.						

	A.14.3.1	Protección de datos de prueba	Se deben seleccionar estratégicamente los datos a utilizar en escenarios de prueba para evitar la exposición de datos sensibles			X		SI	La política de seguridad debe impedir la revelación de datos sensibles en entornos de prueba
A.15 Relaciones con los proveedores	*A.15.1*	Seguridad de la información en las relaciones con los proveedores	Se debe garantizar la protección de los activos que son accesibles por proveedores o personal externos						
	A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Se deben acordar y establecer los controles o requisitos de seguridad necesarios para la protección los activos de información dispuestos a proveedores o terceras personas			X		SI	Aunque el software que se desarrolla es propio pueden existir relaciones con terceros que generan riesgos que deben ser mitigados.

	A.15.1.2	Tratamiento de seguridad dentro de los acuerdos con proveedores	Para cada proveedor se debe determinar las acciones específicas requeridas para mitigar los riesgos generados con su acceso a la información de la empresa.			X		SI	Aunque el software que se desarrolla es propio pueden existir relaciones con terceros que generan riesgos que deben ser mitigados.
	A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Se deben indicar en los acuerdos con los proveedores los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones de cada uno.			X		SI	Aunque el software que se desarrolla es propio pueden existir relaciones con terceros que generan riesgos que deben ser mitigados.
	A.15.2	Gestión de la prestación de servicios de proveedores	Se deben mantener los niveles de prestación de servicios establecidos según los acuerdos de						

			seguridad con los proveedores						
	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	La empresa debe monitorear y auditar constantemente su prestación de servicios con los proveedores.			X		SI	Aunque el software que se desarrolla es propio pueden existir relaciones con terceros que generan riesgos que deben ser mitigados.
	A.15.2.2	Gestión de cambios en los servicios de los proveedores	Se debe establecer un control a los cambios en los servicios prestados a proveedores y terceros, con la finalidad de mantener y mejorar el servicio.			X		SI	Aunque el software que se desarrolla es propio pueden existir relaciones con terceros que generan riesgos que deben ser mitigados.
A.16	*A.16.1*	Gestión de incidentes y mejoras en la seguridad de la información	Se debe garantizar la administración de incidentes relacionados con la seguridad de la información evidenciando						

			eventos y debilidades de seguridad detectados						
Gestión de incidentes de seguridad de la información	A.16.1.1	Responsabilidades y procedimientos	Se deben establecer las responsabilidades y procedimientos de gestión para garantizar una adecuada respuesta a incidentes			X		SI	Se debe establecer una política clara de gestión de incidentes en la empresa
	A.16.1.2	Reporte	Los eventos de seguridad de la información deben ser notificados mediante los canales apropiados de manera ágil.			X		SI	Se debe establecer una política clara de gestión de incidentes en la empresa

	A.16.1.3	Reporte de debilidades de seguridad de la información	Se deben reportar todas las debilidades o eventos sospechosos sobre los sistemas o servicios provistos por la empresa.			X		SI	Se debe establecer una política clara de gestión de incidentes en la empresa
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad deben ser evaluados y clasificados según el tipo de incidencia presentada			X		SI	Se debe establecer una política clara de gestión de incidentes en la empresa
	A.16.1.5	Respuesta a incidentes de seguridad de la información	La empresa debe tener claramente documentados los procedimientos para responder de manera adecuada y oportuna a los incidentes presentados			X		SI	La documentación es requerida para una correcta gestión sobre los incidentes de seguridad
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	De acuerdo a los incidentes generados se debe utilizar la experiencia para evitar o reducir la probabilidad de ocurrencia futura			X		SI	La política debe contemplar el mejoramiento continuo de los servicios y debe ser adaptativa

	A.16.1.7	Recolección de evidencia	La empresa debe velar por la identificación, recopilación y preservación de información que pueda servir de evidencia por lo tanto debe definir procedimientos claros al respecto.			X		SI	La empresa debe documentar el procedimiento re recolección de evidencias
A.17	*A.17.1*	Continuidad de seguridad de la información	La Seguridad de la Información debe ser tenida siempre en cuenta en los planes de continuidad del negocio						
	A.17.1.1	Planificación de la continuidad de la seguridad de la información	La empresa debe establecer los requisitos de seguridad de la información y su respectiva gestión frente a situaciones adversas			X		SI	Se requiere un documento claro y conciso de recuperación ante desastres

Aspectos de seguridad de la información de la gestión de continuidad del negocio	A.17.1.2	Implementación de la continuidad de la seguridad de la información	La empresa debe implantar los requisitos de seguridad de la información y su respectiva gestión frente a situaciones adversas			X		SI	Se requiere un documento claro y conciso de recuperación ante desastres
	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La empresa debe verificar periódicamente los requisitos de seguridad de la información y su respectiva gestión frente a situaciones adversas			X		SI	La empresa debe garantizar la continuidad del servicio ante situaciones adversas
	A.17.2	Redundancias	Se debe garantizar la disponibilidad de las instalaciones de procesamiento de datos.						

	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Se deben implementar mecanismos que garanticen la redundancia en los centros de datos y con los requisitos de disponibilidad			X		SI	La empresa cuenta con un solo CPD, se debe contemplar este punto para garantizar la continuidad del servicio
A.18 **Cumplimiento**	*A.18.1*	Cumplimiento de requisitos legales y contractuales	Se debe evitar incumplimientos a requisitos relacionados con la seguridad de la información de cualquier tipo especialmente a las obligaciones legales, estatutarias, normativas o contractuales.						
A.18	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Se deben identificar, documentar y mantener en operatividad explícita los sistemas de información y los requisitos estatutarios, normativos y			X		SI	La política de seguridad debe contemplar el marco legal respectivo

			contractuales legislativos para que la empresa pueda cumplir con estos.						
Cumplimiento	A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos para garantizar el cumplimiento de la normatividad de propiedad intelectual y hacer uso de software legal.	X		X		SI	La política de seguridad debe contemplar el marco legal respectivo, especialmente contemplar en la misma los derechos de autor
	A.18.1.3	Protección de registros	Los registros deben ser protegidos contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos de ley.			X		SI	Se deben caracterizar y establecer los controles a los registros de la empresa

	A.18.1.4	Privacidad y protección de información de datos personales	La empresa debe garantizar la privacidad y la protección de los datos personales según la normativa vigente	X		X		SI	La empresa cumple con la ley Estatutaria 1581 conocida popularmente como de “Habeas data”
	A.18.1.5	Reglamentación de controles criptográficos	La empresa debe hacer uso de controles de cifrado de información en cumplimiento con la normatividad vigente.	X		X		SI	La empresa debe adoptar la ley 527 de 1999 relacionada firmas digitales y certificados criptográficos en los sistemas informáticos
	A.18.2	Revisiones de seguridad de la información	Se debe garantizar la implementación y operación de la seguridad de la Información según las políticas y procedimientos de la empresa			X		SI	

	A.18.2.1	Revisión independiente de seguridad de la información	Se debe verificar el enfoque de la empresa para implementar y gestionar la seguridad de la información según revisiones independientes y cuando existan cambios significativos en la misma.			X		SI	Caracterización de procesos de Auditoria interna
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	La alta dirección de la empresa debe revisar regularmente el cumplimiento de las políticas, normas y cualquier otro requisito de seguridad correspondiente.	X		X		SI	Caracterización de procesos de Auditoria interna
	A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas			X		SI	Caracterización de procesos de Auditoria interna

			por la información de la organización.						

BIBLIOGRAFÍA

BARROS MARCILLO, Gabriela. Auditoría Informática de la Cooperativa de Ahorro y Crédito "Alianza del Valle" LTDA. Aplicando Cobit 4.0. Trabajo de grado Profesional en Ingeniería de Sistemas e Informática. Sangolquí.: Escuela Politécnica del Ejército. Dpto. de Ciencias de la Computación, 2012.

COLOMBIA. ALCALDÍA MUNICIPAL SIACHOQUE. Plan Anticorrupción y de Atención al Ciudadano. (2016). Administración Municipal 2016-2019. La Alcaldía. Siachoque., 2016.

COLOMBIA. OFICINA DE PLANEACIÓN Y DIRECCIONAMIENTO ESTRATÉGICO SISTEMAS. Normas y políticas de seguridad informática (septiembre, 2013). Código de buenas prácticas para la gestión de la seguridad de la información. La oficina. Bogotá D.C. 2013.

CRESPO GÓMEZ, Manuel y CAMACARO RIVAS, Mailen. Propuesta de una metodología de auditoría informática para la revisión de sistemas de información. [En línea]. Barquisimeto: Universidad Centroccidental "Lisandro Alvarado". 2011., 57 p. Disponible en http://bibcyt.ucla.edu.ve/Edocs_Bciucla/Repositorio/TAQA76.9.A93C742011.pdf

Erb, M. (s.f.). Gestión de Riesgo en la Seguridad Informática. Obtenido de https://protejete.wordpress.com/gdr_principal/matriz_riesgo/

ERIKA, B. M. (10 de 02 de 2012). https://repositorio.espe.edu.ec. Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/5197/1/T-ESPE-033091.pdf

FERNÁNDEZ GRAJALES, Nubia. Importancia de la auditoría informática en las organizaciones. [En línea]. México.: Universidad Nacional Autónoma de México. 2008. Disponible en http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.htm

GALEANO VILLA, Jorge y ALZATE CASTAÑEDA, Cristian. Protocolo de políticas de seguridad informática para las universidades de Risaralda. Trabajo de grado Profesional en Ingeniería de Sistemas y Telecomunicaciones. Pereira.: Universidad Católica de Pereira. Facultad de Ciencias Básicas e Ingeniería. Programa de Ingeniería de Sistemas y Telecomunicaciones, 2013.

Informática, G. d. (s.f.). Gestión de Riesgo en la Seguridad Informática. Obtenido de https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

INTECO, I. d. (s.f.). https://www.incibe.es/. Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

ISO 27000.es, E. p. (2005). ISO 27000.ES. Obtenido de http://www.iso27000.es/sgsi.html

Izquierdo Duarte Fernando, A. d. (2016). http://slideplayer.es/slide/4743467/. Obtenido de http://slideplayer.es/slide/4743467/

JURIDICA, I. (01 de 01 de 2015). InformaticaJuridica.com. Obtenido de http://www.informatica-juridica.com/trabajos/el-derecho-de-autor-con-relacion-a-otros-derechos-especificos-de-la-sociedad-de-la-informacion/

Pallas Mega Gustavo, M. d.-p. (12 de 2009). https://www.fing.edu.uy. Obtenido de https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

PERAFÁN RUIZ, John y CAICEDO CUCHIMBA, Mildred. Análisis de riesgos de la seguridad de la información para la Institución Univresitaria Colegio Mayor del Cauca. Trabajo de grado Especialista en Seguridad Informática. Popayán.: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática, 2014.

QUINTUÑA RODRÍGUEZ, Verónica. Auditoría Informática a la Superintendencia de Telecomunicaciones. Trabajo de grado Profesional en Ingeniería de Sistemas. Cuenca.: Universidad de Cuenca. Facultad de Ingeniería, 2012.

Real Academia Española, A. d. (2017). Real Academia Española. Obtenido de http://dle.rae.es/?id=DgIqVCc

Rocio, G. V. (10 de 2013). https://dspace.ups.edu.ec. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

SECURITY-JEIFER. (01 de 09 de 2010). SECURITY-JEIFER. Obtenido de https://securityjeifer.wordpress.com/2010/09/01/%C2%BFque-es-el-ciclo-phva/

Sosa, J. (27 de 01 de 2012). http://pegasus.javeriana.edu.co. Obtenido de http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf

ANEXOS

Anexo A. – Relación Impacto Hardware y Software

RELACIÓN DE EQUIPOS, LICENCIAS Y DEPENDENCIAS		
No. de identificación del bien	Descripción	Ubicación
0212-0000103-A	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000103-B	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000103-C	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000103-D	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000103-E	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000103-F	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000103-G	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000103-H	LICENCIA OFFICE (SMALL BUSINESS 20	ATENCION AL CLIENTE
0212-0000126A-A	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000126A-B	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000126A-C	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000126A-D	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000126A-E	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000126A-F	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000126A-G	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000126A-H	LICENCIA OFFICE	ATENCION AL CLIENTE
0212-0000237A	SOFTWARE DE CONTROL Y ESTADISTICO	ATENCION AL CLIENTE
0212-000528	SERVIDOR ML 110 65	ATENCION AL CLIENTE
0212-0000243	LICENCIA OFFICE 2007	ATENCION AL CLIENTE
0212-000517	COMPUTADOR DELL REF. 60SNLD1	ATENCION AL CLIENTE
0212-000601	PORTATIL HP 43000S INTEL CORE 13 4R	ATENCION AL CLIENTE
0218-000077	ESTABILIZADOR DE 1000 W	CENTRO DE COMUNICACIÓN
0212-0000103-A	LICENCIAS OFFICE (SMALL BUSINESS20	CONTABILIDAD
0212-0000103-B	LICENCIAS OFFICE (SMALL BUSINESS20	CONTABILIDAD
0212-0000105	COMPUTADOR DE ESCRTIRIO HP PRO 300	CONTABILIDAD
0212-000056A	COMPUTADORE PRESARIO SG3313LA	CONTABILIDAD
0212-000118A	LICENACIA OFFICE	CONTABILIDAD
0212-000126C	LICENCIA WINDOWS XP PROFESSIONAL OE	CONTABILIDAD
0212-000243-A	LICENCIA OFFICE 2007	CONTABILIDAD
0212-000243-B	LICENCIA OFFICE 2007	CONTABILIDAD

0212-000243-C	LICENCIA OFFICE 2007	CONTABILIDAD
0212-000493	COMPUTADOR DESTOKTOP HP COMPAQ DX20	CONTABILIDAD
0212-000525	COMPUTADOR COMPAQ PRESARIO 19 PUL	CONTABILIDAD
0212-000600-A	COMPUTADOR HP PRO 350 MT INTEL COR	CONTABILIDAD
0212-000600-B	COMPUTADOR HP PRO 350 MT INTEL COR	CONTABILIDAD
0212-0000105	COMPUTADOR DE ESCRITORIO HP PRO 300	FACTURACION
0212-0000135A	MICROSOFT DE WINDOWS XP HOME CD Y L	FACTURACION
0212-000243	LICENCIA OFFICE 2007	FACTURACION
0212-000509	COMPUTADOR DELL REF. 20SNLD1	FACTURACION
0212-000522	LICENCIA OLP OFFICE MOL 2007	FACTURACION
0212-0000105	COMPUTADOR DE ESCRITORIO HP PRO 300	FINANCIERA
0212-000035C	COMPUTADOR PROC. INTEL P4	FINANCIERA
0212-0000493	COMPUTADOR DESTOKTOP HP COMPAQ DX20	FINANCIERA
0212-000118A	LICENCIA OFFICE	FINANCIERA
0212-000118B	LICENCIA OFFICE	FINANCIERA
0212-000126C	LICENCIA WINDOWS XP PROFESSIONAL OE	FINANCIERA
0212-000243	LICENCIA OFFICE 2007	FINANCIERA
0212-000495	LICENCIA MICROSOFT OFICCE- 03 EDIC. B	FINANCIERA
0212-000525	COMPUTADOR COMPAQ PRESARIO 19 PUL	FINANCIERA
0212-000111A	COMPUTADOR PORTATIL ACER CORE 13	FINANCIERA
0212-0000105-A	computador de escritorio hp pro 300	PETICION QUEJAS Y RECURSOS
0212-0000105-B	computador de escritorio hp pro 300	PETICION QUEJAS Y RECURSOS
0212-0000105-C	computador de escritorio hp pro 300	PETICION QUEJAS Y RECURSOS
0212-0000105-D	computador de escritorio hp pro 300	PETICION QUEJAS Y RECURSOS
0212-0000105-E	computador de escritorio hp pro 300	PETICION QUEJAS Y RECURSOS
0212-0000130-A	computador hp 3400 core 13	PETICION QUEJAS Y RECURSOS
0212-0000130-B	computador hp 3400 core 13	PETICION QUEJAS Y RECURSOS
0212-000035A-A	computador	PETICION QUEJAS Y RECURSOS
0212-000035A-B	computador	PETICION QUEJAS Y RECURSOS
0212-000038	computador clon pentium	PETICION QUEJAS Y RECURSOS
0212-000118A-1	licencia office	PETICION QUEJAS Y RECURSOS

0212-000118A-2	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-3	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-4	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-5	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-6	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-7	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-8	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-9	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-10	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-11	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118A-12	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118B-A	licencia office	PETICION QUEJAS Y RECURSOS
0212-000118B-B	licencia office	PETICION QUEJAS Y RECURSOS
0212-000126C-A	licencia windows xp profesional	PETICION QUEJAS Y RECURSOS
0212-000126C-B	licencia windows xp profesional	PETICION QUEJAS Y RECURSOS
0212-000126C-C	licencia windows xp profesional	PETICION QUEJAS Y RECURSOS
0212-000126C-D	licencia windows xp profesional	PETICION QUEJAS Y RECURSOS
0212-000139	moden banda base pairgain	PETICION QUEJAS Y RECURSOS
0212-000168-A	router cisco 1600	PETICION QUEJAS Y RECURSOS
0212-000168-B	router cisco 1600	PETICION QUEJAS Y RECURSOS
0212-000209	ups APC 650 KVA	PETICION QUEJAS Y RECURSOS
0212-000493-A	computador destoktop hp compaq	PETICION QUEJAS Y RECURSOS
0212-000493-B	computador destoktop hp compaq	PETICION QUEJAS Y RECURSOS
0212-000495-A	licencia microsoft office-03 edicion	PETICION QUEJAS Y RECURSOS
0212-000495-B	licencia microsoft office-03 edicion	PETICION QUEJAS Y RECURSOS
0212-000495-C	licencia microsoft office-03 edicion	PETICION QUEJAS Y RECURSOS
0212-000495-D	licencia microsoft office-03 edicion	PETICION QUEJAS Y RECURSOS
0212-000507	computador del ref GZRNLD1	PETICION QUEJAS Y RECURSOS
0212-000512	computador dell ref 80NSNLD1	PETICION QUEJAS Y RECURSOS

0212-000515	computador dell ref B0NSNLD1	PETICION QUEJAS Y RECURSOS
0212-000522-A	licencia olp office 2007	PETICION QUEJAS Y RECURSOS
0212-000522-B	licencia olp office 2007	PETICION QUEJAS Y RECURSOS
0212-000522-C	licencia olp office 2007	PETICION QUEJAS Y RECURSOS
0212-000522-D	licencia olp office 2007	PETICION QUEJAS Y RECURSOS
0212-000525	coputador compaq presario 19"	PETICION QUEJAS Y RECURSOS
0212-000600-1	computador hp pro 3500 MT	PETICION QUEJAS Y RECURSOS
0212-000600-2	computador hp pro 3500 MT	PETICION QUEJAS Y RECURSOS
0212-000600-3	computador hp pro 3500 MT	PETICION QUEJAS Y RECURSOS
0212-000600-4	computador hp pro 3500 MT	PETICION QUEJAS Y RECURSOS
0212-000600-5	computador hp pro 3500 MT	PETICION QUEJAS Y RECURSOS
0212-000600-6	computador hp pro 3500 MT	PETICION QUEJAS Y RECURSOS
0212-0000105	computador de escritorio hp	RECUPERACION CARTERA
0212-000038-A	computador clon penium	RECUPERACION CARTERA
0212-000038-B	computador clon penium	RECUPERACION CARTERA
0212-000052	computador penium II 350	RECUPERACION CARTERA
0212-000118A	licencia office	RECUPERACION CARTERA
0212-000120A	licencia office bassic edition 2003	RECUPERACION CARTERA
0212-000126C	licencia windows xp profesional	RECUPERACION CARTERA
0212-000243-A	licencia office 2007	RECUPERACION CARTERA
0212-000243-B	licencia office 2007	RECUPERACION CARTERA
0212-000493	computador destoktop hp	RECUPERACION CARTERA
0212-000513	computador dell ref IZRNLDI	RECUPERACION CARTERA
0212-000522	licencia office MOL 2007	RECUPERACION CARTERA
0212-000525	computador compaq presario 19	RECUPERACION CARTERA
0212-000209	ups apc 650 va	RECUPERACION CARTERA
0212-000600-A	computador hp pro 3500 mt intel cor	RECUPERACION CARTERA
0212-000600-B	computador hp pro 3500 mt intel cor	RECUPERACION CARTERA
0212-000600-C	computador hp pro 3500 mt intel cor	RECUPERACION CARTERA
0212-000600-D	computador hp pro 3500 mt intel cor	RECUPERACION CARTERA
0207-000603	ROUTER INHALAMBRICO LINK DOBLE ANTE	SISTEMAS
0212-00018345	RACK	SISTEMAS
0212-000236	SOFTWARE RM/COBOL DEVELOMENT	SISTEMAS
0212-000126E	LICENCIA PROCESADOR 228-03182	SISTEMAS

0212-000183	SERVIDOR COMPAQ PROLIANT ML 370	SISTEMAS
0212-000001	ACTUALIZA. OPENSERVER INTERRI 5.05	SISTEMAS
0212-000237	SOFTWARE RM/COBOL WOW	SISTEMAS
0212-000261	LICENCIA UNIX PARA 35 USUARIOS	SISTEMAS
0212-000056A	COMPUTADOR PRESARIO SG3313LA	SISTEMAS
0212-000188B	SOFWARE GESTION DOCUMENTAL	SISTEMAS
0212-000183A-A	SERVIDOR ML 370G4. 2GHZ PROC 3.0	SISTEMAS
0212-000183A-B	SERVIDOR ML 370G4. 2GHZ PROC 3.0	SISTEMAS
0212-0001340-A	SWICHT ADMINITRALE 48 PUERTOS	SISTEMAS
0212-0001340-B	SWICHT ADMINITRALE 48 PUERTOS	SISTEMAS
0212-000162A	PROGRAMA VISUAL FOX PRO VERSION 9.0	SISTEMAS
0212-000238	SOFTWARE REATIVITY DESIGNER	SISTEMAS
0212-000243-A	LICENCIA OFFICE. MOL 2007	SISTEMAS
0212-000243-B	LICENCIA OFFICE. MOL 2007	SISTEMAS
0212-0000105	COMPUTADOR DE ESCRITORIO HP PRO 300	SISTEMAS
0212-0001834	SERVIDOR TIPO RACK HP DI380 2 PROC	SISTEMAS
0212-000249-1	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-2	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-3	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-4	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-5	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-6	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-7	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-8	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-9	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-10	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-11	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-12	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-13	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-14	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-15	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-16	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-17	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-18	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-19	SOFTWARE ISOLUCION	SISTEMAS
0212-000249-20	SOFTWARE ISOLUCION	SISTEMAS
0212-000235	SOFTWARE M/COBOL RUNTIME	SISTEMAS

0212-000210	UPS 1 AMERICAN POWER SU /3000 S#9	SISTEMAS
0212-000491	SOTFWARE S.I.G.(SISTEMA INFORMAC. GE	SISTEMAS
0212-000522	LICENCIA OLD OFICE. MOL 2007	SISTEMAS
0212-000528	SERVIDOR ML 110 G5	SISTEMAS
0212-000600	COMPUTADOR HP PRO 3500 MT INTEL COR	SISTEMAS
21200002	EQUIPO COMPUTO - MONITOR 19"	FINANCIERA
21200002	EQUIPO COMPUTO - MONITOR 19"	SISTEMAS
21200002	EQUIPO COMPUTO - MONITOR 19"	SISTEMAS
21200002	EQUIPO COMPUTO - MONITOR 19"	PETICIONES QUEJAS Y RECURSOS
21200002	EQUIPO COMPUTO - MONITOR 19"	PETICIONES QUEJAS Y RECURSOS
21200017	UPS 10 KVA BIFASICA	PETICIONES QUEJAS Y RECURSOS
21200020	FIREWALL FORTINET	SISTEMAS
225000001	LICENCIA ANTIVIRUS

225000001	LICENCIA ANTIVIRUS	SISTEMAS

225000001	LICENCIA ANTIVIRUS	SISTEMAS

225000001	LICENCIA ANTIVIRUS	SISTEMAS

225000001	LICENCIA ANTIVIRUS	SISTEMAS
225000001	LICENCIA ANTIVIRUS	SISTEMAS
225000001	LICENCIA ANTIVIRUS	SISTEMAS
22500002	LICENCIA OFFICE 2013	FINANCIERA
22500002	LICENCIA OFFICE 2013	SISTEMAS
22500002	LICENCIA OFFICE 2013	SISTEMAS
22500002	LICENCIA OFFICE 2013	PETICIONES QUEJAS Y RECURSOS
22500002	LICENCIA OFFICE 2013	PETICIONES QUEJAS Y RECURSOS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS
22500003	LICENCIA CAL OPEN VLSC	SISTEMAS

Anexo B. – Hojas de Encuestas

ENTIDAD : Ibal.			
DEPENDENCIA : Contabilidad.			
NOMBRE ENCUESTADO : Luz Mery Casaq.			
ROL QUE DESEMPEÑA : Contratista.			
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**N/A**
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?			X
¿Existen políticas para la seguridad del Sistema Informático?		X	
¿Se retroalimentan periódicamente las políticas?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?		X	
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?		X	
¿Se efectúan respaldos de la información?		X	
¿Las copias de seguridad son encriptadas?		X	
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?			X
¿Se ejerce control del Sistema Informático?	X		
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?			X

¿El cableado se encuentra correctamente instalado?	X		
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?			
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?		X	
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?			
¿El sistema Informático cuenta con licencia?	X		
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?			X
¿Existe un instructivo para el uso del Software Informático?			X
¿Existe un organigrama con la estructura del área de Informática?	X		
¿Los equipos cuentan con protección de sobre voltaje?	X		
¿Los puertos y servicios innecesarios están desactivados?			X
¿Se cargan los parches de seguridad liberados por Microsoft?		X	
¿Los dispositivos de entrada al sistema están deshabilitados?			X

ENTIDAD : Ibal			
DEPENDENCIA : Atención al usuario			
NOMBRE ENCUESTADO : Luisa Martínez			
ROL QUE DESEMPEÑA :			
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**N/A**
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?			X
¿Existen políticas para la seguridad del Sistema Informático?	X		
¿Se retroalimentan periódicamente las políticas?			X
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?		X	
¿Se efectúan respaldos de la información?	X		
¿Las copias de seguridad son encriptadas?		X	
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?		X	
¿Se ejerce control del Sistema Informático?	X		
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?			X

¿El cableado se encuentra correctamente instalado?			X
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?			X
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?			X
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿El sistema Informático cuenta con licencia?			X
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?			X
¿Existe un instructivo para el uso del Software Informático?			X
¿Existe un organigrama con la estructura del área de Informática?	X		
¿Los equipos cuentan con protección de sobre voltaje?	X		
¿Los puertos y servicios innecesarios están desactivados?			X
¿Se cargan los parches de seguridad liberados por Microsoft?			X
¿Los dispositivos de entrada al sistema están deshabilitados?			X

ENTIDAD : IBAL			
DEPENDENCIA : CENTRO DE COMUNICACIÓN			
NOMBRE ENCUESTADO : DANIEL M. QUINTANA			
ROL QUE DESEMPEÑA : COORDINADOR			
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**N/A**
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?	X		
¿Existen políticas para la seguridad del Sistema Informático?	X		
¿Se retroalimentan periódicamente las políticas?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?		X	
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?		X	
¿Se efectúan respaldos de la información?	X		
¿Las copias de seguridad son encriptadas?		X	
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?		X	
¿Se ejerce control del Sistema Informático?	X		
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?	X		

¿El cableado se encuentra correctamente instalado?	X		
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?	X		
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?		X	
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?		X	
¿El sistema Informático cuenta con licencia?		X	
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?	X		
¿Existe un instructivo para el uso del Software Informático?		X	
¿Existe un organigrama con la estructura del área de Informática?		X	
¿Los equipos cuentan con protección de sobre voltaje?	X		
¿Los puertos y servicios innecesarios están desactivados?		X	
¿Se cargan los parches de seguridad liberados por Microsoft?		X	
¿Los dispositivos de entrada al sistema están deshabilitados?			X

ENTIDAD : ISAL			
DEPENDENCIA : Financiera.			
NOMBRE ENCUESTADO : Felipe Ortiz mazuera.			
ROL QUE DESEMPEÑA : auxiliar.			
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**N/A**
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?			X
¿Existen políticas para la seguridad del Sistema Informático?			X
¿Se retroalimentan periódicamente las políticas?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?			X
¿Se efectúan respaldos de la información?		X	
¿Las copias de seguridad son encriptadas?			X
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?		X	
¿Se ejerce control del Sistema Informático?			X
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?			X

¿El cableado se encuentra correctamente instalado?	X		
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?			X
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?		X	
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿El sistema Informático cuenta con licencia?	X		
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?			X
¿Existe un instructivo para el uso del Software Informático?			X
¿Existe un organigrama con la estructura del área de Informática?			X
¿Los equipos cuentan con protección de sobre voltaje?		X	
¿Los puertos y servicios innecesarios están desactivados?		X	
¿Se cargan los parches de seguridad liberados por Microsoft?			X
¿Los dispositivos de entrada al sistema están deshabilitados?		X	

ENTIDAD : IBAL			
DEPENDENCIA : POT			
NOMBRE ENCUESTADO : ALEJANDRO PARRA			
ROL QUE DESEMPEÑA : CONTRATISTA			
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**N/A**
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?	X		
¿Existen políticas para la seguridad del Sistema Informático?			X
¿Se retroalimentan periódicamente las políticas?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?		X	
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?	X		
¿Se efectúan respaldos de la información?		X	
¿Las copias de seguridad son encriptadas?			X
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?		X	
¿Se ejerce control del Sistema Informático?		X	
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?		X	

¿El cableado se encuentra correctamente instalado?		X	
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?	X		
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?	X		
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?		X	
¿El sistema Informático cuenta con licencia?	X		
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?		X	
¿Existe un instructivo para el uso del Software Informático?	X		
¿Existe un organigrama con la estructura del área de Informática?		X	
¿Los equipos cuentan con protección de sobre voltaje?	X		
¿Los puertos y servicios innecesarios están desactivados?	X		
¿Se cargan los parches de seguridad liberados por Microsoft?	X		
¿Los dispositivos de entrada al sistema están deshabilitados?		X	

ENTIDAD : IBAL			
DEPENDENCIA :			
NOMBRE ENCUESTADO : JOSE VICENTE URREGO.			
ROL QUE DESEMPEÑA :			
CUESTIONARIO			
PREGUNTA	SI	NO	N/A
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?	X		
¿Existen políticas para la seguridad del Sistema Informático?			X.
¿Se retroalimentan periódicamente las políticas?			X.
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?			X.
¿Se efectúan respaldos de la información?	X		
¿Las copias de seguridad son encriptadas?			X
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?		X	
¿Se ejerce control del Sistema Informático?	X		
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?	X		

¿El cableado se encuentra correctamente instalado?	X		
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?	X		
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?			X.
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X.	
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿El sistema Informático cuenta con licencia?	X		
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?	X		
¿Existe un instructivo para el uso del Software Informático?			X
¿Existe un organigrama con la estructura del área de Informática?			X
¿Los equipos cuentan con protección de sobre voltaje?	X		
¿Los puertos y servicios innecesarios están desactivados?			X
¿Se cargan los parches de seguridad liberados por Microsoft?	X		
¿Los dispositivos de entrada al sistema están deshabilitados?		X	

ENTIDAD : IBAL			
DEPENDENCIA : FACTURACION			
NOMBRE ENCUESTADO : CESAR AUGUSTO CARVAJAL B.			
ROL QUE DESEMPEÑA :			
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**N/A**
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?	X		
¿Existen políticas para la seguridad del Sistema Informático?	X		
¿Se retroalimentan periódicamente las políticas?	X		
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?	X		
¿Se efectúan respaldos de la información?	X		
¿Las copias de seguridad son encriptadas?		X	
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?		X	
¿Se ejerce control del Sistema Informático?	X		
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?	X		

¿El cableado se encuentra correctamente instalado?	X		
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?			X
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?		X	
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?	X		
¿El sistema Informático cuenta con licencia?	X		
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?	X		
¿Existe un instructivo para el uso del Software Informático?			X
¿Existe un organigrama con la estructura del área de Informática?	X		
¿Los equipos cuentan con protección de sobre voltaje?	X		
¿Los puertos y servicios innecesarios están desactivados?		X	
¿Se cargan los parches de seguridad liberados por Microsoft?	X		
¿Los dispositivos de entrada al sistema están deshabilitados?			X

ENTIDAD : IBAL			
DEPENDENCIA : Sistemas			
NOMBRE ENCUESTADO : Giovanni Ruiz			
ROL QUE DESEMPEÑA :			
CUESTIONARIO			
PREGUNTA	**SI**	**NO**	**N/A**
¿La empresa cuenta con un Departamento de Informática?	X		
¿El acceso al centro de Cómputo se encuentra restringido?	X		
¿Existen políticas para la seguridad del Sistema Informático?	X		
¿Se retroalimentan periódicamente las políticas?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?		X	
¿Las contraseñas de los usuarios se cambian dependiendo de la situación?		X	
¿Se efectúan respaldos de la información?	X		
¿Las copias de seguridad son encriptadas?		X	
¿El sistema cuenta con personal técnico que ayude cuando se produzcan inconvenientes?	X		
¿En caso de que un equipo principal falle, existen equipos auxiliares?		X	
¿Se ejerce control del Sistema Informático?	X		
¿Se administrará y restringirá el acceso a la red utilizando direcciones, protocolos de seguridad y contraseñas para la red inalámbrica?	X		

¿El cableado se encuentra correctamente instalado?	X		
¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?	X		
¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?	X		
¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?		X	
¿Se realiza un adecuado mantenimiento al Sistema Informático?		X	
¿El sistema Informático cuenta con licencia?	X		
¿Existe control de acceso a los aplicativos que son utilizados en las diferentes áreas de la empresa?	X		
¿Existe un instructivo para el uso del Software Informático?		X	
¿Existe un organigrama con la estructura del área de Informática?	X		
¿Los equipos cuentan con protección de sobre voltaje?	X		
¿Los puertos y servicios innecesarios están desactivados?		X	
¿Se cargan los parches de seguridad liberados por Microsoft?	X		
¿Los dispositivos de entrada al sistema están deshabilitados?	X		