DIAGNÓSTICO PARA LA MITIGACIÓN DE RIESGOS INFORMÁTICOS DE LA EMPRESA LYD COLOMBIA S.A.S.

WILLIAM DANILO DONCEL ORTEGON

MIGUEL ANGEL PEROZO LEÓN

MARIO ALBERTO PINTO BARRETO

UNIVERSIDAD PILOTO DE COLOMBIA

SECCIONAL DEL ALTO MAGDALENA

PROGRAMA DE INGENIERÍA DE SISTEMAS

GIRARDOT

2019

DIAGNÓSTICO PARA LA MITIGACIÓN DE RIESGOS INFORMÁTICOS DE LA EMPRESA LYD COLOMBIA S.A.S.

WILLIAM DANILO DONCEL ORTEGON

MIGUEL ANGEL PEROZO LEÓN

MARIO ALBERTO PINTO BARRETO

MONOGRAFÍA DE INVESTIGACIÓN PRESENTADA PARA OPTAR EL TÍTULO PROFESIONAL EN INGENIERÍA DE SISTEMAS

TUTOR: EDICSON PINEDA CADENA

INGENIERO DE SISTEMAS

UNIVERSIDAD PILOTO DE COLOMBIA

SECCIONAL DEL ALTO MAGDALENA

PROGRAMA DE INGENIERÍA DE SISTEMAS

SEMINARIO DE INVESTIGACIÓN APLICADA – GERENCIA ORGANIZACIONAL

GIRARDOT

2019

DEDICATORIA

Dedicamos esta monografía a nuestros padres que pase lo que pase siempre están detrás de nosotros acompañándonos y apoyándonos.

AGRADECIMIENTOS

Agradecemos a Dios, Por habernos permitido llegar hasta este punto, con salud para lograr nuestros objetivos, además de su infinita bondad y amor.

A Nuestros Maestros. que con dedicación nos entregan su conocimiento y guía.

TABLA DE CONTENIDO

LISTAS ESPECIALES

LISTAS DE ILUSTRACIONES

LISTA DE TABLAS

1. GLOSARIO

- **BASC:** Conocido como *Business Anti-Smuggling Coalition o Coalición Empresarial Anticontrabando,* nace de la necesidad de mitigar el contrabando a nivel internacional y sea crea una alianza entre el sector privado y diferentes agencias internacionales para trabajar en pro de un comercio internacional seguro. Esto aplica para todas las empresas que tienen como actividad económica exportar o importar productos. Y el obtener esta certificación BASC da la seguridad a los clientes que la compañía trabaja de manera legal y sus procesos son limpios. (Qué son las Normas BASC - Un aliado en la lucha contra el narcotráfico, 2019)

- **DIAGNOSTICO:** Por lo general se define como el resultado final de todo un proceso que va desde recoger información utilizando técnicas de recolección de información, pasar por un proceso de análisis de esta y esto arroja un estado actual donde se concluye en que está fallando, que riesgos tiene y como puede solucionarlos.

- **INFRAESTRUCTURA TECNOLOGICA:** Se entiende por infraestructura tecnológica todo lo implementado por una compañía para agilizar, optimizar y automatizar todos sus procesos, y esto abarca todo lo relacionado con software, hardware, telecomunicaciones y demás tecnologías que ayuden a la empresa a ser más competente a nivel global. (Tendencias de la infraestructura TIC, 2019).

- **LEY 1273 de 2009:** La siguiente ley de delitos informáticos se crea a partir del 2009 con la finalidad de proteger la información y los datos de cualquier usuario, tipifica una serie de conductas ilegales que se cometían y no eran judicializadas, tales como suplantación, acceso abusivo a sistemas de información, apoderarse de información, utilización de software malicioso y obstaculizar el normal uso de sistemas de información entre otros más que son castigados con multas económicas o prisión (Cuervo, 2019).

- **MATRIZ RAM:** La matriz se utiliza para determinar mediante valoración las probabilidades de que un riesgo se vuelva una amenaza real para la compañía, puede indicar incluso que tanto puede afectar y así mismo tomar decisiones que ayuden a evitarlos o mitigarlos.

- **RIESGOS INFORMATICOS:** Son condiciones a las que una persona o empresa que utilicen sistemas de información están expuestos a ser víctimas de ciberataques que pueda tener consecuencias de pérdidas de información, estafas y otras conductas ilegales que puedan afectar toda la infraestructura tecnológica (RIESGOS INFORMÁTICOS, 2019).

- **SEGURIDAD INFORMATICA:** Se puede definir la seguridad informática como la gestión e implementación de una serie de políticas que ayudan a salvaguardar los sistemas de información ya sea persona natural o empresa, ya que personas pueden ingresar de manera fraudulenta y apoderarse de información sensible con la finalidad de obtener ganancias, publicar información o utilizarla para su propio beneficio. Es por ello por lo que es importante que las compañías inviertan en software que les proteja toda su información

y puedan trabajar de manera segura (¿Qué es la seguridad informática y cómo puede ayudarme? | VIU, 2019).

- **SISTEMA DE GESTION DE CALIDAD:** Es la implementación de un programa que le permite a todas las organizaciones potenciar competencias como crear, planear, controlar, gestionar y ejecutar todos sus procesos con altos estándares de calidad. (Carrillo, 2019)

2. RESUMEN

La presente investigación es un diagnóstico en seguridad informática realizado a la empresa LyD Colombia S.A.S, que entre sus actividades económicas se encuentran operador logístico, generador de carga, comercializador de todo tipo de mercancías, distribución, transporte y almacenaje de todo tipo de mercancías.

Para el desarrollo de sus funciones utilizan la tecnología, ya sea para recibir órdenes de transporte o enviar evidencias de estas a través de los correos electrónicos, WhatsApp entre otros, debido a la confidencialidad e importancia de su labor, se hace necesario implementar medidas de seguridad informática para salvaguardar la información y asegurar su correcto uso, para revisar las etapas, medios y actores que intervienen se genera la oportunidad de realizar un diagnóstico, este se inicia revisando su actual infraestructura informática y a través de este encontrar oportunidades de mejora que le puedan ayudar a la compañía para asegurar sus activos tecnológicos y aprovechar el conocimiento adquirido en el seminario de investigación aplicada ya que una empresa no funciona en torno a un solo departamento (Financiero, Gerencia, Recurso Humano, Etc...), sino que debe ser analizada de forma macro y detallar en cada uno de sus procesos los posibles riesgos informáticos que se puedan generar para con sus labores cotidianas; la empresa dentro de sus estándares de cumplimiento tiene el deseo de certificarse en BASC (Es un programa de cooperación entre el sector privado, organismos nacionales y extranjeros, creado para fomentar un comercio internacional seguro.). El presente diagnóstico se basa y revisa cada uno de sus aspectos con base a la norma 5.0.1 ESTÁNDAR INTERNACIONAL DE SEGURIDAD BASC de fecha 10 de agosto de 2017 para EMPRESAS CON RELACIÓN DIRECTA CON LA CARGA Y CON

LAS UNIDADES DE TRANSPORTE DE CARGA (Ver Anexo 1 Estándar-Internacional-BASC-501 apartado 6).

Palabras clave: Empresa LyD, Diagnóstico, Seguridad Informática, Estándar, BASC.

3. ABSTRACT

The present investigation is a diagnosis in computer security made to the company LyD Colombia S.A.S, which among its economic activities are logistics operator, load generator, marketer of all types of merchandise, distribution, transport and storage of all types of merchandise.

For the development of their functions they use technology, either to receive transport orders or send evidence of these through emails, WhatsApp among others, due to the confidentiality and importance of their work, it is necessary to implement security measures information technology to safeguard the information and ensure its correct use, to review the stages, means and actors involved, the opportunity to make a diagnosis is generated, this begins by reviewing your current computer infrastructure and through this find opportunities for improvement that can help you to the company to secure its technological assets and take advantage of the knowledge acquired in the applied research seminar since a company does not work around a single department (Financial, Management, Human Resource, Etc ...), but it must be analyzed in a macro way and detail in each of its processes the possible computer risks that can be generated for your daily work; The company within its compliance standards has the desire to become certified in BASC (It is a cooperation program between the private sector, national and foreign organizations, created to promote safe international trade.). This diagnosis is based on and reviews each of its aspects based on the standard 5.0.1 BASC INTERNATIONAL SECURITY STANDARD dated August 10, 2017 for COMPANIES WITH DIRECT RELATIONSHIP WITH

THE CARGO AND WITH THE CARGO TRANSPORTATION UNITS (See Annex 1 Standard-International-BASC-501 section 6).

Keywords: LyD Company, Diagnosis, Computer Security, Standard, BASC.

4. INTRODUCCIÓN

En la actualidad es normal escuchar sobre ataques informáticos, sobre todo, en la era digital y la tecnología se convirtió en la base de todos los medios, lo que se transforma en una oportunidad para mejorar la calidad de vida en el aprovechamiento de la tecnología se convierte también en un contorno de ataques informáticos. La presente monografía tiene como finalidad realizar un diagnóstico a la infraestructura actual de la empresa LyD Colombia S.A.S e identificar oportunidades de mejora para mitigar los riesgos informáticos posibles de la compañía. En detalle, se busca identificarlas y formular posibles soluciones; siendo este un tema sensible que ha venido creciendo de manera exponencial como son los delitos informáticos en Colombia, a pesar de que se encuentran tipificados en la ley 1273 de 2009, en Colombia, no ha sido suficiente para disminuir esta infracción. Por el contrario, las denuncias se han incrementado en cuanto al hackeo de redes sociales, suplantación de identidades, clonación de tarjetas crédito y débito, lo que tiene como consecuencia estafar a los usuarios incluso extorsionarlos para evitar la divulgación de información privada; de acuerdo con el artículo de la revista Dinero:

En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos, entre abril-julio de 2019 y estos ataques son cada vez más sofisticados...Lo más preocupante de todo es que con el paso del tiempo, estas amenazas vienen creciendo exponencialmente tanto en volumen como en sofisticación (En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos, 2019).

Por lo tanto, es importante identificar los riesgos de seguridad informática que pueden llegar a tener las empresas y utilizar métodos que nos permitan mitigarlos; Ya que, en un mundo actual interconectado por la internet, las redes y telecomunicaciones los delincuentes utilizan estos medios desde dentro y fuera del país para cometer delitos en el anonimato.

5. JUSTIFICACIÓN

La tecnología es un factor importante para las empresas, el activo más importante es la información y son muchos los frentes de la empresa donde esta se mueve, existen normas y mejores prácticas que dan una guía de qué se debe asegurar para que los clientes de la compañía y proveedores los identifiquen que, como empresa les interesa trabajar con un estándar que aseguren un correcto funcionamiento tanto interno como externo de la compañía, de acuerdo a la certificación BASC en el apartado 6 de la certificación: Seguridad en los procesos relacionados con la tecnología y la información. La cual instruye a la compañía sobre los requerimientos que se deben implementar para asegurar confidencialidad y seguridad de la información tales como políticas que ayuden a gestionar el resguardo y la recuperación de la información en caso de ciber ataques.

Implementar políticas que permitan realizar mantenimiento y auditorias sobre el estado de la infraestructura, actualizaciones del acceso lógico a los diferentes softwares utilizados en cuanto a permisos de ingreso, utilizar software de seguridad que impida instalaciones de no licenciados. que pueda brindar seguridad a la compañía y mitigar riesgos de ataques que puedan acarrearle perdida de la información.

Una compañía que logre certificarse en BASC, da confiabilidad y seguridad a los clientes, al igual que toda su información estará segura, pero ¿cómo se analiza el cumplimiento de este apartado?, en la norma se establecen los puntos obligatorios que debe cumplir si o si la compañía,

además de que debería; que, aunque sea opcional influye directamente en el resultado de la mitigación para el riesgo informático.

6. OBJETIVOS

6.1. OBJETIVO GENERAL.

Realizar el análisis con el fin de diagnosticar los riesgos informáticos de la empresa LyD Colombia S.A.S, basados en el Estándar-Internacional-BASC-501 apartado 6, que regula las compañías de transporte que tienen contacto directo con la carga en los procesos relacionados con la tecnología y la información.

6.2. OBJETIVOS ESPECÍFICOS.

- Caracterizar la infraestructura tecnológica actual (línea base).
- Desarrollar la matriz de evaluación de riesgos (RAM), informáticos de la compañía.
- Proponer acciones de mitigación de los riesgos tecnológicos de la empresa LyD Colombia S.A.S.

7. MARCO TEÓRICO

7.1. ANTECEDENTES.

De acuerdo a las entrevistas realizadas (Ver anexo 3), al gerente y líderes de procesos en la compañía, se encontraron dos oportunidades de investigación, la primera es la necesidad de la empresa para certificarse en el estándar internacional BASC, el cual dentro de su apartado número 6 (Ver anexo 1), tipifica los requisitos mínimos para realizar la certificación, la segunda es que la empresa fue víctima de cifrado de información a través de un Ransomware hace aproximadamente un año, este ataque generó pérdidas económicas lo cual se representó en la contratación por 3 meses de 5 auxiliares de digitación para poder restablecer la contabilidad de 8 años todo esto generó la necesidad de buscar alternativas, blindarse como empresa en seguridad informática y lo más importante entender el valor de la información.

Por esta experiencia del cifrado de información el gerente tomó la decisión de invertir en infraestructura tecnológica, se implementó una storage o almacén de red para salvaguardar la información de los servidores y usuarios finales, se creó un dominio de red para administrar bajo perfiles los usuarios y se eliminaron los procedimientos de acceso remoto.

Con todo esto y entendiendo que la historia de los ciberataques viene creciendo de manera exponencial, nace la seguridad informática, esta rama del conocimiento agrupa las mejores prácticas que deben ser aplicadas a nivel de usuario, infraestructura y compañía para mitigar los

riesgos, y en el caso de que la seguridad sea violada, existen mecanismos de recuperación de desastres que en el menor tiempo posible puedan restablecer la operación de las empresas.

7.2. SEGURIDAD INFORMÁTICA EN EL MUNDO.

En un mundo globalizado, en donde todas las personas y las empresas se conectan a la internet para, ya sea comunicarse u ofrecer productos y servicios y realizar todo tipo de procesos que van desde utilizar correos electrónicos, transacciones financieras y almacenar información sensible y vital tanto para corporaciones como para personas naturales, desde un punto geográfico hacia cualquier parte de mundo con el objetivo de acercar nuevos mercados o clientes, ha hecho que las empresas y personas particulares estén más vulnerables a ataques cibernéticos.

En estos casos el recurso o activo más valioso que tenga la empresa o persona sea la información, como base fundamental para su estabilidad y crecimiento, lo cual indica que sea evidente la necesidad de ir un paso delante de los posibles riesgos de ciberataques, ya que todos los días a nivel mundial las empresas y personas naturales son víctimas del hackeo de sus cuentas, correos, contraseñas y más afectaciones que tienen como finalidad el robo de la información, la divulgación de la misma, estafar e incluso cometer delitos como extorsión para devolver lo hurtado.

Se debe tener en cuenta que todos los días se crean nuevos malware y que al momento de realizar ataques estos son más rápidos que el tiempo que se gasta la compañía en detectar y solucionar el problema, lo que acarrea con grandes pérdidas de información y dinero, por ende, las

empresas deben ver la necesidad de destinar un presupuesto en seguridad informática para su compañía si quieren salvaguardar su activo más importante como lo es la información. (Robo de datos y dinero: los ciberataques, entre las 5 amenazas globales más inquietantes, 2019)

7.3. SEGURIDAD INFORMÁTICA EN COLOMBIA

La concurrencia de estos delitos se venía cometiendo sin ningún tipo de ley que judicialice estas prácticas malignas, a partir del 2009 con las crecientes cifras de este tipo de delitos se vio la necesidad de crear la ley 1273 de 2009 donde se tipifican este tipo de faltas y se castigan con dinero y prisión, lo que puede dar una solución temporal en reducción de cifras. pero no corta de raíz el problema.

Por ello es importante que todos, tanto empresas como personas empiecen a implementar sistemas de seguridad que les permita utilizar la internet y demás redes de manera segura, ya sea para realizar procesos, transacciones, envío y recepción de información y almacenaje de la misma sin estar tan expuestos a estos riesgos.

Por todos estos antecedentes la compañía LyD COLOMBIA S.A.S., vio la necesidad de realizar un diagnóstico en seguridad informática que le permita identificar las posibles fallas en infraestructura tecnológica y riesgos a los que puede estar expuestos, de tal manera que les permita reestructurar y mejorar para que puedan seguir con su actividad económica con total normalidad y seguridad.

8. MARCO CONCEPTUAL

- **SEGURIDAD INFORMATICA:** Se puede definir la seguridad informática como la gestión e implementación de una serie de políticas que ayudan a salvaguardar los sistemas de información ya sea persona natural o empresa, ya que personas pueden ingresar de manera fraudulenta y apoderarse de información sensible con la finalidad de obtener ganancias, publicar información o utilizarla para su propio beneficio.

- **CREDENCIALES DE USUARIO:** Son los datos de usuario auténticos, que permiten acceder de manera privada a sitios web donde se requiere el uso de confidencialidad de la información.

- **GESTIÓN DE RIESGOS DE SEGURIDAD INFORMÁTICA:** Denominada también como Gestión de riesgos TIC, conceptualizada como un análisis, cuyo objetivo primordial es encontrar las vulnerabilidades en el ámbito informático mediante el uso de riesgos probabilísticos y de impacto.

- **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN:** Es un reglamento, puede ser físico o digital, donde se estipulan normatividades, contribuyendo al compromiso relacionado sobre seguridad informática en una empresa, negocio, etc.

- **REVISIÓN DE ACCESO:** Es el proceso de verificación, en la que, en tiempo real, es monitoreado los accesos a un sitio web, donde también se efectúa las credenciales de usuario accedidos en un listado de registros de acceso.

- **PERMISOS DE INSTALACIÓN DE SOFTWARE:** Son aquellas autorizaciones, siendo gestionadas por un súper-usuario o un usuario con privilegios administrativos, en la que cede a la instalación de un programa o un software, con fines de uso laboral eficiente.

- **PREVENCIÓN DE ATAQUES INFORMÁTICOS:** Dicha acción se define como un bloqueo de ataques, donde el software requerido para la protección (ya sea un cortafuegos, un antivirus, un puerto de enlace seguro, etc.) cumple su papel vital de prevenir que usuarios con intenciones delictivas, ingresen a documentos confidenciales de una entidad.

- **BACKUP:** O también conocida como copia de respaldo o de restauración o de seguridad, es el proceso en la que un archivo o sistema, es copiado en su totalidad en caso de que en un futuro presente pérdida de éste, con el objetivo de recuperar el contenido que almacenaba.

- **ACTUALIZACIÓN DE LA INFORMACIÓN:** para toda organización contar con información detallada, veraz y actualizada ayuda aumentar el nivel de confiabilidad en la toma de decisiones, en la que da una perspectiva clara de estados actuales, por otro lado, ayuda en la mitigación de errores en el procesamiento, almacenaje, envío y recepción de esta.

- **MONITOREO DE ACCESO A USUARIOS:** Se define como el control y vigilancia constante que se realiza al momento de que los usuarios entren a las bases de datos, sistemas de información y puedan tener acceso a información privilegiada, es importante definir los permisos para cada usuario para que puedan acceder a lo autorizado y requerido por el perfil que tengan.

- **TIEMPO DE ACTIVIDAD DE LOS USUARIOS: S**e interpreta con la frecuencia que los usuarios tienen acceso a la información y al software que usa una organización, las plataformas deben controlarse por tiempo de inactividad y permisos de accesos a la información.

- **RESTRICCIÓN DE CONEXIÓN DE DISPOSITIVOS DE SALIDA Y PERIFÉRICOS:** Se define como la prohibición de dispositivos ajenos a los permitidos por las compañías de tal manera que se eviten hurtos, trasmisión ilegal de datos o daño de sistemas de información.

- **REGLAMENTACIÓN DEL USO DE LOS EQUIPOS:** La organización debe identificar la necesidad y de esta manera contar con la infraestructura adecuada para suplirla, es importante contar con tecnología moderna, un reglamento que permita el uso adecuado restrinja la manipulación que pueda causar daños.

9. MARCO METODOLÓGICO

9.1. METODOLOGÍA DE LA INVESTIGACIÓN APLICADA

Para la elaboración del diagnóstico, la metodología que se usó para la elaboración de la investigación pertinente, fue la metodología de investigación mixta, ya que por la parte cualitativa, se trata de una recolección de muestreo de datos sobre un diagnóstico en la área de riesgo informático, elaborado mediante entrevistas directas y recolección física y visual de la información con los empleados de la compañía y el gerente de LyD Colombia S.A.S, y en la parte cuantitativa, los resultados dados en la matriz de riesgo RAM son dados bajo números, indicando probabilidad e impacto del riesgo informático en la estructura tecnológica física y lógica de la empresa.

Se entiende por metodología de investigación mixta, toda aquella que hace uso requerido de datos numéricos, a su vez, la observación directa juega un papel importante sobre el estudio de datos pertinentes y contribuyentes de la investigación para su posterior análisis, es decir, usando a la misma vez el enfoque cualitativo y cuantitativo. Según Sampieri:

Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (Hernández Sampieri, Baptista Lucio & Fernández Collado, 2008).

9.2. VARIABLES DE LA INVESTIGACIÓN MIXTA

9.2.1. VARIABLES INDEPENDIENTES.

- Seguridad informática.
- Credenciales de usuario.
- Gestión de riesgos de seguridad informática.
- Políticas de seguridad en la información.

9.2.2. VARIABLES DEPENDIENTES.

- Revisión de acceso.
- Permisos de instalación.
- Prevención de ataques informáticos.
- Backup.
- Actualización de la información.
- Monitoreo de acceso de usuarios.
- Tiempo de actividad de usuarios.
- Restricción de conexión de dispositivos de salida y periféricos.
- Información confidencial.
- Reglamentación de uso de los equipos.

9.3. POBLACIÓN Y MUESTRA.

9.3.1. POBLACIÓN.

La población que representa en el proceso de la metodología de la investigación es la empresa LyD Colombia S.A.S.

9.3.2. MUESTRA.

La muestra que representa en el proceso de la metodología de la investigación, son los líderes de proceso y empleados del área tecnológica de la empresa LyD Colombia S.A.S.

9.4. INSTRUMENTOS USADOS EN LA INVESTIGACIÓN.

9.4.1. ENTREVISTAS.

En la empresa LyD Colombia S.A.S. se aplicaron entrevistas directamente con el gerente, a su vez con los respectivos líderes de proceso, respondiendo preguntas relacionadas con la tecnología que tienen a la mano, y su estructura de red, a su vez, sobre el tipo de seguridad que manejan y las restricciones que tienen.

9.4.2. MATRIZ DE RIESGO RAM.

Se identificó en la empresa, la matriz de riesgo RAM, donde las variables principales, que dan el valor de significancia, están definidas sobre la probabilidad y el impacto que puede llegar a emerger, se caracterizó y se estableció el siguiente método de evaluación.

MATRIZ IDENTIFICACIÓN DE RIESGOS

MATRIZ DE PROBABILIDAD E IMPACTO CUALITATIVA

PROBABILIDAD	IMPACTO					RIESGO	ACCIÓN APLICADA
	Muy Bajo	Bajo	Medio	Alto	Muy Alto		
Prácticamente Seguro	5 (Nivel 4)	10 (Nivel 5)	15 (Nivel 5)	20 (Nivel 5)	25 (Nivel 5)	NIVEL 5	Tratamiento
Probable	4 (Nivel 3)	8 (Nivel 4)	12 (Nivel 4)	16 (Nivel 5)	20 (Nivel 5)		
Posible	3 (Nivel 2)	6 (Nivel 3)	9 (Nivel 3)	12 (Nivel 4)	15 (Nivel 4)	NIVEL 4	
Poco Probable	2 (Nivel 1)	4 (Nivel 2)	6 (Nivel 2)	8 (Nivel 3)	10 (Nivel 3)	NIVEL 3	Validar tratamiento provisional con verificación continua
Muy Raro	1 (Nivel 1)	2 (Nivel 1)	3 (Nivel 1)	4 (Nivel 2)	5 (Nivel 2)	NIVEL 2 Y 1	

Medidas cualitativas y cuantitativas de probabilidad

Nivel	Probabilidad Cualitativa	Valor	Probabilidad Cuantitativa
Nivel 5	Prácticamente Seguro	5	· Se han recibido amenazas directas que afectan la seguridad y han ocurrido. · Muy alta probabilidad de ocurrencia del evento afecta directamente la prestación del servicio. · Se espera que el evento del riesgo ocurra en la mayoría de las circunstancias o está ocurriendo ahora.
Nivel 4	Probable	4	· El evento del riesgo probablemente ocurrirá en la mayoría de las circunstancias. · Se ha recibido una amenaza creíble pero aun no ha ocurrido. · Los fallos se presentan con frecuencia afentando la prestación del servicio. · Le ha ocurrido a otras empresas del sector al que pertenecemos.
Nivel 3	Posible	3	· El evento del riesgo puede ocurrir en algún momento, pero generalmente solo sobre · Asociada a situaciones similares que hayan tenido fallos esporádicos, pero no en grandes · Se ha recibido una posible amenaza, pero no ha ocurrido.
Nivel 2	Poco probable	2	· El evento de riesgo podría ocurrir en algún momento, pero es improbable. · Ocasionalmente podría producirse un numero relativo bajo de fallos que probablemente afectan el · Alerta de amenaza, pero no ha ocurrido. · Le ha ocurrido a otras empresas del sector al que pertenecemos bajo circunstancias específicas.
Nivel 1	Muy raro	1	· El evento de riesgo es muy raro que pueda ocurrir en algún momento y afectar la prestación de · Seria irrazonable esperar que se produjera el fallo en la prestación de servicio. · No se han recibido amenazas creíbles.

Medidas cualitativas y cuantitativas de Impacto

Nivel	Impacto Cualitativo	Valor	Impacto Cuantitativo
Nivel 5	Muy alto	5	· Suplantación, infiltración de persona con intensión de causar daño a la organización. · Muy alta gravedad que origina total insatisfacción del cliente, o puede llegar a suponer un alto impacto. · Perdidas graves cuando hay un siniestro sin recuperación. · Incumplimiento legal, cancelación de la habilitación por MIN Transporte. · Perdida del cliente. · Perdida de ventaja competitiva e imagen a largo plazo.
Nivel 4	Alto	4	· Perdidas económicas considerables cuando hay un evento sin embargo se puede recuperación. · Alta clasificación de gravedad debido a la naturaleza del fallo que causa en el cliente un alto grado · Incumplimiento legal sanciones ante entidades competentes. · Perdida de ventaja competitiva e imagen a corto plazo.
Nivel 3	Medio	3	· Evento con perdidas económicas leve con recuperación. · Moderada gravedad del fallo que causaría al cliente cierto insatisfacción. Puede ocasionar · Desprestigio o daño a la imagen y reputación que impacte a las ventas a corto plazo
Nivel 2	Bajo	2	· Perdidas menores cuando los elementos afectados se pueden reparar. · Baja gravedad debido a la escasa importancia de las consecuencias del fallo, que causarían en el
Nivel 1	Muy bajo	1	· Perdidas menores los elementos se pueden reemplazar. · Irrazonable esperar que el fallo produzca un efecto perceptible en el rendimiento del proceso.

Ilustración 1: Evaluación Matriz de identificación de riesgos.
Fuente: Elaboración propia

CARACTERIZACION

REQUISITOS A CUMPLIR			
ISO 9001:2015	4.2- 4.4 6.1-6.3-7.1-7.1.3-7.1-7.5- 9.1- 9.2- 10.1, 10.3		
NORMA BASC V5 2017	4.1, 4.2, 4.3, 4.4, 5.1, 5.2, 5.3, 5.4, 6.1, 6.2, 7.1.3, 7.2.1, 7.2.2, 7.2.3, 8.1, 9.1, 9.2, 9.3, 9.4	**ESTANDAR 5.0.1**	1 - 4.2.1- 5 - 6
Otros LEGALES, CLIENTE Y EMPRESA	Ley 603/2000 Derechos de Autor; Ley 527/1999 Comercio Electrónico; Ley 1273/2009 Delitos Informáticos.		

INTERACCION DEL PROCESO

ENTRADAS		ACTIVIDADES				SALIDAS	
Proveedor	**Entradas**	**Actividades Generales**				**Salidas**	**Cliente**
		PLANIFICAR	**HACER**	**VERIFICAR**	**ACTUAR**		
Planeación Estratégica	Solicitudes de cambio o mejora de la infraestructura tecnológica.	Cambios en infraestructura tecnológica por solicitud.	Presentar soluciones a la gerencia sobre la infraestructura tecnológica.	Revisar que la infraestructura tecnológica cumpla para poder realizar la operación en la organización.	Tomar acciones para ajustar la infraestructura tecnológica.	Información para la toma de decisión sobre la infraestructura tecnológica.	Planeación Estratégica
Planeación Estratégica	Mantenimiento de equipos preventivo	Realizar la planificación del mantenimiento Cronograma Mantenimiento de Equipos informático	Realizar mantenimiento de equipos según cronograma.	Verificar el cumplimiento del cronograma de mantenimiento.	Reprogramar mantenimientos no realizados.	Actualización de: Cronograma Mantenimiento. Solicitud compra de repuestos, softw are, antivirus y otros requerimientos de TIC. Ficha técnica PC. Inventario.	Planeación Estratégica
Planeación Estratégica	Mantenimiento de equipos correctivo	Realizar la planificación del mantenimiento correctivo en Cronograma y Mantenimiento de Equipos informático	Realizar mantenimiento de equipos según cronograma.	Verificar el cumplimiento del cronograma de mantenimiento.	Reprogramar mantenimientos no realizados.	Solicitud compra de repuestos, softw are, antivirus y otros requerimientos de TIC. Ficha técnica PC. Inventario.	Planeación Estratégica
Planeación Estratégica	Solicitud compra de repuestos, softw are, antivirus y otros requerimientos de TIC.	Generar presupuesto para TICS	Cotizaciones técnicas de acuerdo a los requerimientos.	Cumplimiento de especificación técnica	Ajustes de requerirse	Cotizaciones Aprobación Gerencia	Financiero.
Todos los procesos	Solicitud de soporte, falla técnica o del servicio.	Identificar la falla técnica (SW-HW-Comunicaciones). Planificar la realización del soporte.	Realizar soporte presencial o Conexión remota. Solicitar reparación técnica por proveedor comunicaciones.	Equipo funcionando. Seguimiento proveedores de comunicaciones.	Plan de contingencia de requerirse.	Solución solicitud de soporte.	Todos los procesos
Planeación Estratégica SIG	Solicitud de asignación de claves	Revisar cambios de claves.	Realizar cambio de claves	Claves asignadas de modo seguro.	Plan de contingencia de requerirse.	Entrega de claves de manera segura	Planeación Estratégica SIG
Planeación Estratégica	Solicitud de Backus	Programación de backup.	Realizar backups	Verificar que el backups se realizó correctamente.	Reprogramar backups que no se realizaron correctamente	Backup de información.	Planeación Estratégica
Gestión de talento humano	Solicitud de capacitación	Planificar capacitaciones relacionadas con TICS	Realizar capacitación	Realizar evaluación de la eficacia	Reforzar conocimientos	Entrega soportes de capacitación: Asistencia. Evaluación.	Gestión de talento humano
Planeación Estratégica SIG	Solicitud de monitoreo	Planificar los equipos que deben monitorearse.	Realizar monitoreo	Verificar funcionamiento	Realizar ajustes equipos.	Estado de monitoreo de los equipos.	Planeación Estratégica SIG

RECURSOS REQUERIDOS

Infraestructura física	**Infraestructura tecnología**	**Recurso Humano**	**Recurso Financiero**	**Ambiente de trabajo**
Puesto de trabajo, línea Telefónica, implementos y útiles de oficina y archivo	Equipo de computo, internet, correo electrónico, herramienta de office y celular. Centro de cableado y equipos.	Participar activamente en los programas, procedimientos, simulacros organizados por el proceso de seguridad para prevenir riesgos en las instalaciones, operaciones y personal. Informar continuamente al proceso de seguridad cualquier requerimiento en materia de seguridad que se requiera con el objeto de prevenir riesgos. Asesor TICS.	Registros de participación en actividades programadas por el área de seguridad. Requerimientos en materia de seguridad Presupuesto asignado al proceso.	Puesto con las condiciones ergonomía necesarias. Condiciones de higiene para el puesto de trabajo. Archivo para documentos.

Ilustración 2: Matriz de identificación de riesgos.
Fuente: Elaboración propia.

I. IDENTIFICACIÓN DE RIESGOS											
No. DE RIESGO	FUENTE DEL RIESGO	PROCESO	RESPONSABLE	FECHA DE IDENTIFICACIÓN	FECHA DE REVISIÓN	NOMBRE DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSAS POTENCIALES	EFECTO POTENCIAL / CONSECUENCIA	TIENE CONTROLES	DESCRIPCIÓN DEL CONTROL EXISTENTE
1	Operativo	TIC	Encargado de TIC	16/09/2019	19/09/2019	Ataque informático y hackers	Posibilidad que personas ajenas a la compañía tenga acceso a la plataforma tecnológica y esto afecte el desempeño. Falla en el suministro y mantenimiento eléctrico.	1. Falla en la configuración del FIREWALL de la organización. 2. FIREWALL no disponibles. 3. Fallas en la actualización y ejecución del antivirus. 4. Interrupción del funcionamiento normal de los dispositivos electrónicos. 5. Ataque de virus informático 6. Falta de capacitación al personal 7.No planificación del proceso de TIC. 8. Incumplimiento en las actividades de TIC5.	1. Perdida de información 3. Hurto de mercancia. 4. Perdidas economicas. 5. Perdida de la imagen corporativa. 6. Incumplimiento de politcas de TICs 7. Demoras en el desarrollo normal de la operación.	Si	1. Antivirus. 2. FIREWALL 3. Inspecciones aleatorias a las instalaciones. 4.Manejo de contraseñas entropicas. 5. Backup de la información de los equipos y servidor.
2	Operativo	TIC	Encargado de TIC	16/09/2019	19/09/2019	Daño de perifericos	Daño fisico por desgaste o mala utilización de los equipos informaticos que puede generar perdida de la información y tiempos altos de indisponibilidad.	1. Daño normal de equipo electronico. 2. Daño por caida de tensión. 3. Mal uso de los equipos tecnologicos.	1. Perdida de la información. 2. Indisponibilidad de labor por falta de la herramienta tecnologica. 3. Demoras en la recuperación de la información.	Si	1. Backup de la información en tiempo real. 2. Equipos de soporte para reemplazo de piezas o equipo completo. 3. Capacitación en uso de equipos informaticos en la entrega del cargo.
3	Operativo	TIC	Encargado de TIC	16/09/2019	19/09/2019	Perdida de Conexión	Perdida de información por desconexion de internet e indisponibilidad para el proceso operativo ya que toda su estructura depende de internet.	1. Caida de servicio por parte de ISP. 2. Daños fisicos en la red externa o interna. 3. Daño en equipos de comunicaciones.	1. Indisponibilidad para ejercer la labor.	Si	1. Balanceador de carga de internet soportada con 3 operadores y tecnologias diferentes de ISP (Claro Fibra, Claro Coaxial y Etb)
4	Personas	TIC	Encargado de TIC	16/09/2019	19/09/2019	Perdida de integridad de la información en discos duros extraibles o usb	Daño, pérdida, adulteración de la información fisica generada por el proceso	1. No se asumen las funciones y responsabilidades de acuerdo a los perfiles de cargo 2. Falla de seguridad informática. 3. Empleados sobornables. 4. Falta de control a la información tanto fisica como virtual. 5. No realizar back ups en los tiempos programados. 6. No tener los back ups en disco externo y fuera de las instalaciones de la empresa. 7. No aplicación de la política de seguridad informática. 8. Falta de antivirus. 9. Falta de control y seguridad del archivo fisico. 10. Personal interno extraiga información.	1. Pérdidas de información, 2. Pérdidas económicas, 3. Soborno	Si	1. Cumplimiento de la politica de seguridad informática y del plan de mantenimiento a los equipos informáticos. 2. Realización de copias de seguridad a todos los equipos de la organización. 3. Repositorio de copias por version de cambios de hasta 32 veces por documento.
5	Personas	TIC	Encargado de TIC	16/09/2019	19/09/2019	Perdida de integridad de la información mágnetica o software	Daño, pérdida, adulteración de la información magnética generada por el proceso	1. No se le da inducción o formación adecuada al personal. 2. No investigar el personal al ingreso de la Empresa. 3. Empleados sobornables 4. Competencia desleal 5. Personal interno o externo extraiga información. 6. No realizar back ups en los tiempos programados. 7. No tener los back ups en disco externo y fuera de las instalaciones de la empresa.	1. Pérdidas de información, 2. Pérdidas económicas, 3. Soborno	Si	1. Cumplimiento de la politica de seguridad informática y del plan de mantenimiento a los equipos informáticos 2. Realización de copias de seguridad a todos los equipos de la organización. 3. Repositorio de copias por version de cambios de hasta 32 veces por documento.
6	Personas	TIC	Encargado de TIC	16/09/2019	19/09/2019	Falla en seguridad de la información	Fuga de información que afecte la integridad, disponibilidad y confidenciadad. Posiblibilidad de que cualquier persona entregue, de información confidencial para beneficio propio o de terceros afectanto la seguridad, rentabilidad y calidad de la operación	1. Conspiración interna (Prevalece el interes personal sobre la organización). 2. Fallas en el proceso de selección y contratación del personal. 3. Falla en el sistema de información. 4. Falla en el seguimeinto de las actividades realizadas por el equipo de trabajo. 5. Falla en los procedimientos de desvinculación del personal. 6. Manejo inadecuado del archivo fisico. 7. Fallas en la aplicación de directricez de SI. 8. No clasificación adecuada de la información. 9. Falta aplicación de controles de la información confidencial.	3. Soborno	Si	1. Procedimiento de selección y contratación. 2. Seguimeinto periodicos de las actividades realizadas por los procesos a la alta dirección 3. Backup de la información de hasta 32 versiones por documento, teniendo asi prueba de modificaciones por usuario o equipo.

Ilustración 3: Matriz de identificación de riesgos
Fuente: Elaboración propia.

II. EVALUACIÓN DE RIESGOS						III. PLAN DE TRATAMIENTO DE RIESGOS					IV. VALORACIÓN DE RIESGOS RESIDUAL				
VALORACIÓN INICIAL						DETALLE ACTIVIDADES DEL PLAN	RESPONSABLE DE LA ACTIVIDAD	REALIZACIÓN		OBSERVACIONES/ RECOMENDACIONES / CORRECCIONES SOBRE ACTIVIDADES DEL PLAN	VALORACIÓN DESPUES DE TRATAMIENTO				
PROBABILIDAD DE OCURRENCIA	PROBABILIDAD DE OCURRENCIA	GRADO DE IMPACTO	GRADO DE IMPACTO	RIESGO	ESTRATEGIA DE RIESGO			FECHA INCIO	FECHA FIN		PROBABILIDAD DE OCURRENCIA	PROV. OCURR	GRADO DE IMPACTO	GRAD IMP	RIESGO RESIDUAL
Probable	4	Muy alto	5	Nivel 5	Mitigar	1. Monitoreo frecuente 2. Cableado y electricado. 3. Plan de mantenimiento preventivo electrico. 4. Sensibilizacòn en el uso de tomas reguladas. 5. Seguimiento de Back ups	TICS	Permanente	Permanente		Posible	3	Alto	4	Nivel 4
Posible	3	Alto	4	Nivel 4	Mitigar	1. Revision periodica de los backup 2. Pruebas aleatorias de restauración backup 3. Capacitación a personal nuevo en el uso de las herramientas TICS	TICS	Permanente	Permanente		Poco probable	2	Alto	4	Nivel 3
Posible	3	Alto	4	Nivel 4	Mitigar	1. Monitoreo. 2. redes de contingencia	TICS	Permanente	Permanente		Poco probable	2	Medio	3	Nivel 2
Poco probable	2	Muy alto	5	Nivel 4	Evitar	1. Seguimiento a los cargos que poseen disco duro externo en sus procesos. 2. Resguardo de la informaciòn crìtica de la organización y asociados de negocios.	1. Personal involucrado con dispositivos externos. 2. Tics.	Permanente	Permanente		Poco probable	2	Alto	4	Nivel 3
Probable	4	Muy alto	5	Nivel 5	Mitigar	1. Contraseñas con permisos de seguridad que prohiban modificaciones de fondo. 2. Resguardo de la informaciòn crìtica de la organización y asociados de negocios.	1. Personal que utilice medios magneticos. 2. Tics.	Permanente	Permanente		Poco probable	2	Alto	4	Nivel 3
Probable	4	Muy alto	5	Nivel 5	Mitigar	1. Procedimiento de desvinculaciòn. 2. Seguimiento a los cargos crìticos. 3. Resguardo de la informaciòn crìtica de la organización y asociados de negocios. 4. Restricciòn al acceso de la red. 6. Restricciòn al correo electrònico publico, redes sociales y pàginas de internet que no tengan que ver con la organización	Gestión de Talento Humano. Asesor TICs Lideres Inmediatos	Permanente	Permanente		Posible	3	Alto	4	Nivel 4

Ilustración 4:Evaluación, plan de tratamiento y valoración del resigo residual.
Fuente: Elaboración propia.

9.5. PROCEDIMIENTO.

Para esta fase, en la empresa LyD Colombia S.A.S. se implementó la verificación por observación mediante una lista de chequeo de cumplimiento en base a las mejores prácticas para Estándar BASC.

La empresa debe establecer e implementar:

a) **Una política para impedir que se revele información confidencial:** Un reglamento donde se haga acatar que se prohíbe revelar documentos, archivos, entre otros que contengan información privada que pueda comprometer la integridad de la empresa.
b) **Una política de uso de los recursos informáticos:** Un reglamento específico que aclare el uso establecido de los dispositivos tecnológicos e informáticos de la empresa a fines laborales.

Seguridad de tecnología de la información.

La empresa debe:

a) **Establecer una política o procedimiento documentado para gestionar la seguridad informática que permita identificar, proteger y recuperar la información:** Reglamento especificado que haga gestión de la protección de la

información con fines privativos, a su vez que sea fácil reconocer y recuperarse en caso de pérdida por averíos en el hardware.

b) Utilizar cuentas asignadas de forma individual y cada usuario que acceda al sistema debe tener sus propias credenciales de acceso y mantener contraseñas; estas deben cambiarse periódicamente: Autenticación de credenciales y acceso a información detallada de manera individual, asignación de roles, y renovación de la clave secreta.

c) Revisar periódicamente los accesos asignados a los usuarios: Control de acceso y tiempo de actividad de los usuarios en la respectiva plataforma. (monitoreo).

d) Impedir la instalación de software no autorizado: Restricción y bloqueo de permisos para instalación de herramientas que no son de contribución en el entorno laboral tecnológico.

e) Implementar y mantener software y hardware que proteja la información de amenazas informáticas (virus, accesos no autorizados y similares): Adquisición e instalación de software antivirus contra los ataques durante la transmisión de datos, cortafuegos, SSH, entre otros métodos de protección.

f) Contar con copias de seguridad de la información sensible y una copia debe

almacenarse fuera de las instalaciones de forma segura con base a la gestión de riesgos: Software y servidores mediante RAID u otra herramienta de salvaguardado que se encarguen del respaldo y copia de seguridad de la información pertinente cada 30 días.

g) **Eliminar el acceso a la información a todos los colaboradores y usuarios externos al terminar su contrato o acuerdo:** Exterminación de credenciales de acceso a la información privada de la empresa a aquellos que ya no hacen pertenencia al entorno de trabajo.
h) **Mantener un registro actualizado de los usuarios y claves de acceso:** Creación de un changelog que muestre las actualizaciones de los datos de usuario y su respectiva contraseña.
i) **Cerrar/bloquear la sesión en equipos desatendidos:** Política mediante un software que cierre la sesión a los usuarios inactivos durante un determinado tiempo.

La empresa debería:

j) **Prohibir la conexión de dispositivos periféricos personales (teléfonos inteligentes,**

reproductores MP3, memorias USB, etc.) a cualquier dispositivo que esté conectado a la red informática. Los puertos USB deberían ser desactivados por

defecto: Restricciones del uso de dispositivos de salida y periféricos, herramientas de almacenamiento en la nube, entre otras.

Para la ejecución de la matriz se implementó un informe mediante una plantilla en Excel. (ver ilustración 2, 3 y 4 en listas de ilustraciones).

9.6. RESULTADOS.

De acuerdo con la descripción de la lista de chequeo anterior, se puede evidenciar que:

La empresa debe establecer e implementar:

a) **Una política para impedir que se revele información confidencial:** Cumple.
b) **Una política de uso de los recursos informáticos:** Cumple.

Seguridad de tecnología de la información.

La empresa debe:

a) **Establecer una política o procedimiento documentado para gestionar la seguridad informática que permita identificar, proteger y recuperar la información:** Cumple.

b) **Utilizar cuentas asignadas de forma individual y cada usuario que acceda sistema debe tener sus propias credenciales de acceso y mantener contraseñas; estas deben cambiarse periódicamente:** Cumple.

c) **Revisar periódicamente los accesos asignados a los usuarios:** Cumple.

d) **Impedir la instalación de software no autorizado:** Cumple.

e) **Implementar y mantener software y hardware que proteja la información de amenazas informáticas (virus, accesos no autorizados y similares):** Cumple.

f) **Contar con copias de seguridad de la información sensible y una copia debe almacenarse fuera de las instalaciones de forma segura con base a la gestión de riesgos:** No cumple, debido a que se evidencia que se hacen efectivas las copias de seguridad, pero no realizan el respectivo proceso de restauración.

g) **Eliminar el acceso a la información a todos los colaboradores y usuarios externos al terminar su contrato o acuerdo:** Cumple.

h) **Mantener un registro actualizado de los usuarios y claves de acceso:** Cumple.

i) **Cerrar/bloquear la sesión en equipos desatendidos:** Cumple.

La empresa debería:

j) **Prohibir la conexión de dispositivos periféricos personales (teléfonos inteligentes, reproductores MP3, memorias USB, etc.) a cualquier dispositivo que esté conectado a la red informática. Los puertos USB deberían ser desactivados por defecto:** No cumple, debido a que, aunque se evidencia que por política de dominio no se permite el uso de USB, no se tiene definido un bloqueo

para el envío de correos externos o uso de sistemas de almacenamiento en la nube como Google Drive o Dropbox.

De acuerdo con la matriz de riesgos implementada, en base a los resultados dados, se encontraron los siguientes riesgos:

- **Ataque informático y hackers.**
- **Daño de periféricos.**
- **Perdida de Conexión.**
- **Perdida de integridad de la información en discos duros extraíbles o USB.**
- **Perdida de integridad de la información magnética o software.**
- **Falla en seguridad de la información.**

10. MARCO LEGAL

Para la realización de este diagnóstico en seguridad informática, hay que tener en cuenta que se rigen bajo una serie de leyes y normas que hacen que la compañía legalmente cumpla con lo requerido por la ley en Colombia.

Para ello es importante resaltar la norma ISO 9001: 2015, apartado 4.2 y 4.4 lo cual indica que, si la organización tiene la capacidad potencial para suministrar bienes y servicios que cumplan los requerimientos del cliente, legales para los cuales aplica se debe tener en cuenta que son referentes a el sistema de gestión de calidad (Minvivienda, 2019).

Y esto indica que la organización debe gestionar la mejora continua del sistema de gestión de calidad en cuanto a sus procesos, con qué frecuencia se utilizan, determinar métodos que hagan más eficiente la operación y control de los mismos, también es importante asignar un presupuesto y asegurar que esté disponible cuando se requiera y consecuentemente asignar responsabilidades sobre dichos procesos y posteriormente realizar auditorías que permitan mitigar riesgos y potenciar oportunidades de mejora.

Y aquí se saca a colación el APARTADO 6.1 DE LA NORMA ISO 9001:2015, en el cual las organizaciones al momento de implementar los requerimientos del apartado 4.2 y 4.4, debe gestionar métodos que permitan evaluar la eficiencia de los procesos con el objetivo de obtener los resultados positivos previstos en el sistema de gestión de calidad y al mismo tiempo se reduzcan los riesgos.

Toda organización que requiera implementar un sistema de gestión de calidad debe tener en cuenta que el APARTADO 7.1 Y 7.1.2 DE LA NORMA ISO 9001: 2015 prioriza a la compañía a designar presupuesto para mantenerlo y mejorarlo continuamente en cuanto a funcionamiento y tener la infraestructura adecuada que le permita a la empresa operar eficientemente en todos sus procesos con el objetivo de dar confiabilidad, seguridad y satisfacción al cliente.

Es importante resaltar que las compañías como LyD Colombia S.A.S. cuya actividad económica es la importación y distribución de mercancía cuente con una certificación BASC, teniendo como premisa el apartado 6 de la certificación: SEGURIDAD EN LOS PROCESOS RELACIONADOS CON LA TECNOLOGIA Y LA INFORMACION. La cual instruye a la compañía sobre los requerimientos que se deben implementar para asegurar confidencialidad y seguridad de la información tales como políticas que ayuden a gestionar el resguardo y la recuperación de la información en caso de ciber ataques.

Implementar políticas que permitan realizar mantenimiento y auditorias sobre el estado de la infraestructura, actualizaciones del acceso lógico a los diferentes softwares utilizados en cuanto a permisos de ingreso, utilizar software de seguridad que impida instalaciones de no licenciados. que pueda brindar seguridad a la compañía y mitigar riesgos de ataques que puedan acarrearle perdida de la información. Una compañía que logre certificarse en BASC, da confiabilidad y seguridad a los clientes, al igual que toda su información estará segura.

Es importante resaltar que todas las empresas que manejen sistemas de información, que indique poseer infraestructura tecnológica y software para todos sus procesos, deben estar regidos bajo la LEY 603 DEL AÑO 2000 que tipifica el respeto por los derechos de autor, encaminando así a la empresa a utilizar software licenciado de alta calidad que le permita optimizar sus procesos de forma eficiente y controlada e impidiendo así que se puedan evadir tributos que le puedan acarrear problemas tributarios a la compañía.

Toda empresa que disponga de sistemas de información donde se puedan enviar y recibir información, donde se puedan generar, procesar y almacenar dichos mensajes de datos y adicional se les adhiera firma digital para dar validez, estarán regidos por la LEY 527 DE 1999 que reglamenta el uso y acceso de información la cual dichos procesos están estructurados bajo normas técnicas que den su correcto uso.

LyD Colombia S.A.S. al ser una empresa colombiana es claro que se rige bajo leyes colombianas y en este caso debe conocer la LEY 1273 DE 2009 que tipifica los delitos informáticos conociéndose estos como conductas maliciosas que puedan dañar software, tener acceso a sistemas de información sin autorización, suplantación, impedir el correcto funcionamiento de sistemas informáticos y recopilar información de manera fraudulenta, una vez la compañía obtenga certificaciones como la ISO 9001, la certificación BASC y se apegue a las demás leyes nombradas las posibilidades de sufrir ataques cibernéticos que causen daños potenciales se reducirán, blindando así la empresa toda su información y procesos dentro de su actividad económica.

11. MARCO CONTEXTUAL

En los siguientes esquemas, se encuentra estructurada la ubicación respectiva de los equipos.

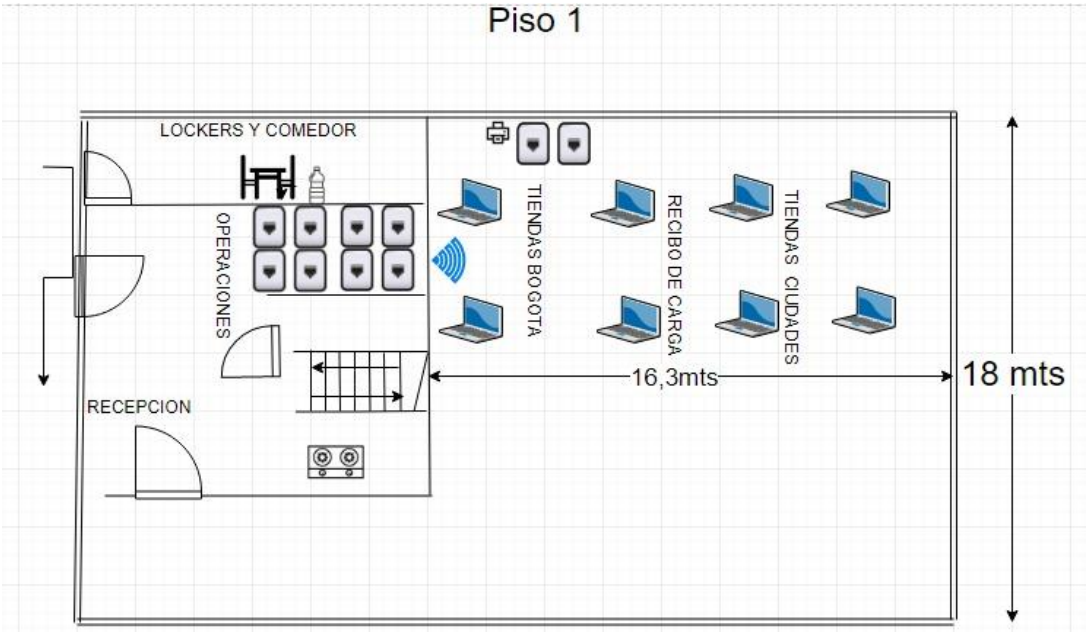

Imagen 1: Piso uno de la estructura tecnológica LyD Colombia S.A.S
Fuente: Elaboración propia.

En la primera imagen, se puede apreciar la ubicación respectiva de los equipos de cómputo en la primera planta, las cuales, en la sala de operaciones, la componen ocho (8) equipos de escritorio.

En el otro segmento, se puede ver que en el área de tiendas ciudades, la componen de cuatro (4) equipos portátiles, en recibo de carga, dos (2), y en tiendas Bogotá se encuentran dos (2) equipos de escritorio, dos (2) equipos portátiles, un router Wi-Fi y una impresora.

Imagen 2: Piso dos de la estructura tecnológica LyD Colombia S.A.S.
Fuente: Elaboración propia.

En la imagen 2, se puede ver en el segundo piso, en el área de gerencia, dos (2) equipos de escritorio.

En el área de contabilidad un (1) equipo de escritorio, una impresora, y el servidor principal.

En el área de operaciones, está compuesta por seis (6) equipos de cómputo.

En el área de calidad, sólo un (1) equipo compone dicha sección.

En el área de recursos humanos, la componen de dos (2) equipos de escritorio y una impresora.

La empresa LyD Colombia S.A.S cuenta con 30 equipos, compuestos por 8 portátiles y 22 de escritorio (o de mesa), cuyo sistema operativo se ejecuta Windows 7 y Windows 10.

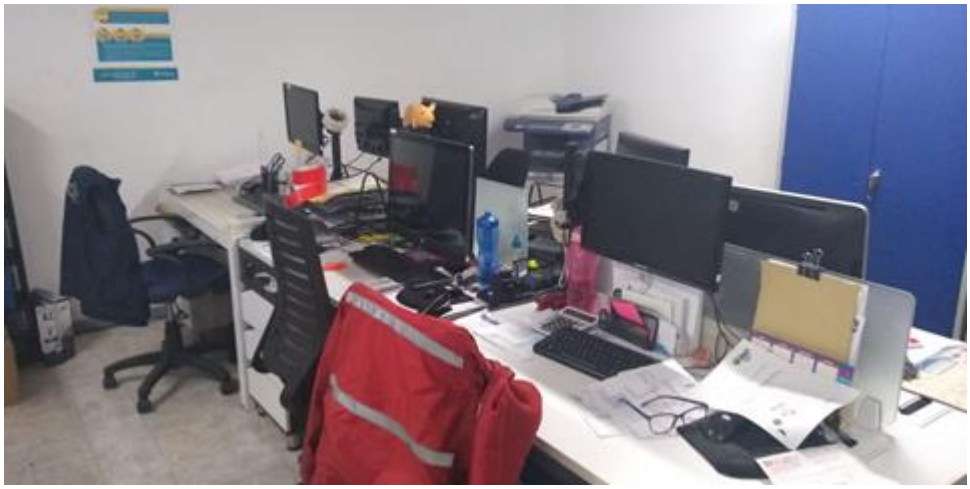

Imagen 3: Equipos de escritorio de la sala de operaciones.
Fuente: Elaboración propia.

En la imagen anterior, se puede ver los equipos de escritorio de la sala de operaciones.

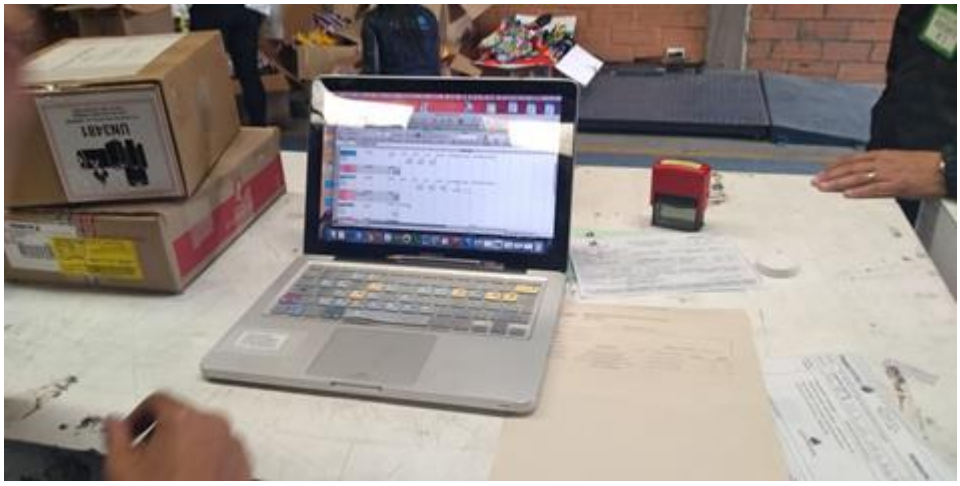

Imagen 4: Equipo portátil del área de recibo de carga.
Fuente: Elaboración propia.

Todos los equipos de escritorio se conectan a una red base mil, en el rango 192.168.20.0/24, clase C a través de un Switch de 24 puertos, marca TP-Link.

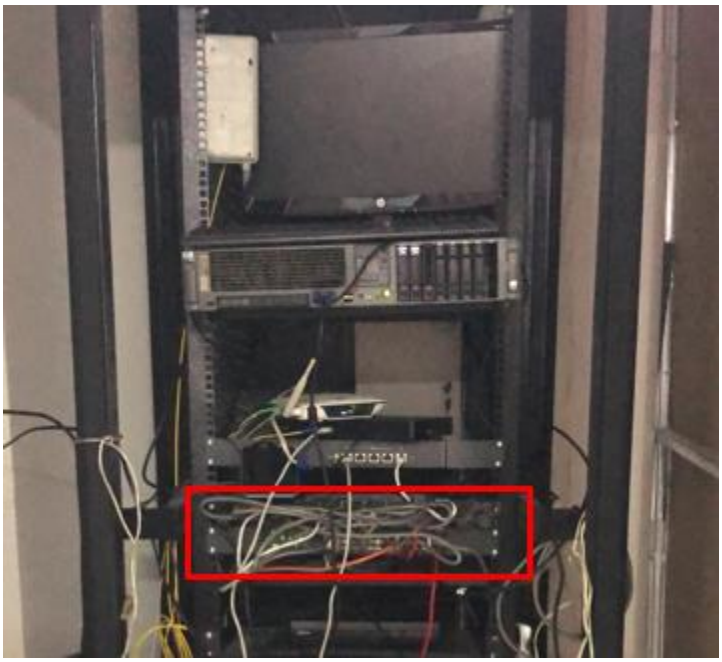

Imagen 5: Ubicación del switch TP-Link.
Fuente: Elaboración propia.

La red cuenta también con un balanceador de cargas TP-Link, cuya dirección IP interna es de 192.168.20.1/24 con dos canales de internet activos, a su vez, este equipo se encarga de suministrar el tráfico de red, donde abastece el uso continuo de la red local cuando uno de los dos canales se caiga.

Imagen 6: Balanceador de cargas TP-Link.
Fuente: (TP-Link, 2019)

Todos los equipos se conectan mediante el protocolo de red DHCP, donde reciben una IP automáticamente, desde 192.168.20.100 hasta 192.168.20.199.

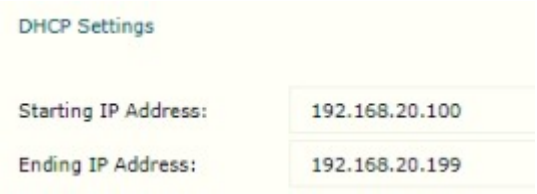

Imagen 7: Indicaciones de inicio y fin de las direcciones IP mediante DHCP del balanceador de cargas.
Fuente: Elaboración propia

La forma de distribución de los dos canales, en cuanto a la conexión de los equipos es la siguiente:

Imagen 8: Indicaciones de canales de distribución de internet.
Fuente: Elaboración propia.

El router cuenta con un sistema de seguridad ante ataques de intrusos que desean acceder a la red, es una configuración básica, pero funcional en su papel de protección de información.

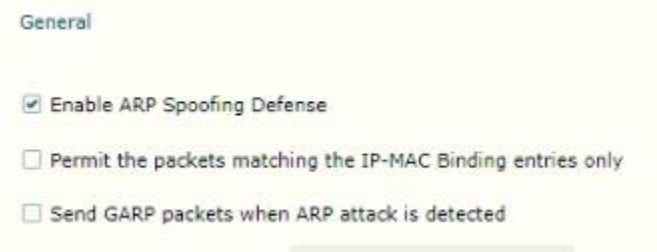

Imagen 9: Checkbox para la habilitación de defensa de Spoofing.
Fuente: Elaboración propia.

En la opción de transmisión de datos, algunos checkbox están habilitados para prevenir ataques mediante puertos WAN y TCP, y otras opciones para ping.

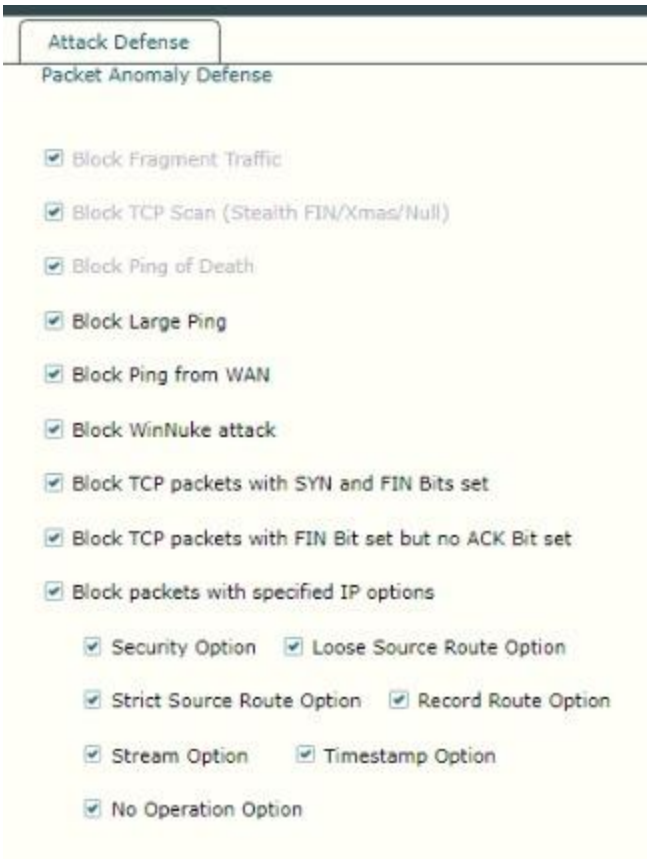

Imagen 10: Checkbox para el control de transmisión de paquetes de datos.
Fuente: Elaboración propia.

El router balanceador también cuenta con una funcionalidad, donde filtra el contenido, en la que posiblemente, se puede acceder, agregando una restricción sobre el ingreso a algunas páginas.

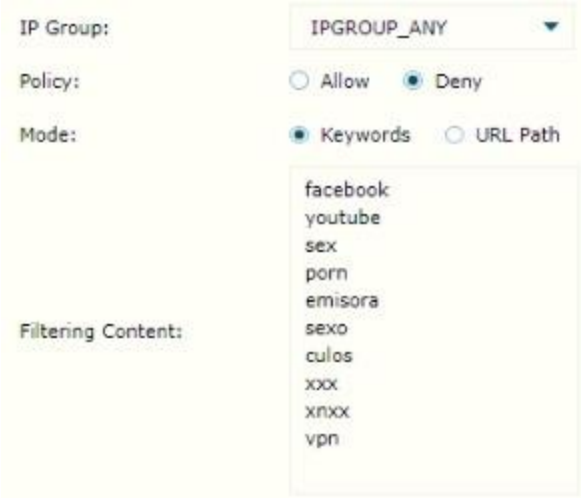

Imagen 11: Filtro de contenido mediante palabras.
Fuente: Elaboración propia.

La empresa también cuenta con otro router Wi-Fi, un TP-Link TL-WR941HP, cuya dirección IP es 192.168.20.254, este funciona como punto de acceso para brindar conexión inalámbrica a los portátiles de la bodega.

Imagen 12: Router TP-Link TL-WR941HP.
Fuente: (TP-Link, 2019)

El router es el encargado de suministrar red a las impresoras y cámaras, donde su rango respectivo está entre 192.168.20.210 hasta 192.168.20.254 mediante conexión DHCP.

La empresa también cuenta con un servidor Windows Server 2012 que administra la red mediante un dominio de nombre “lydcolombia.local”, cuya IP es 192.168.20.2, la cual, no cuenta con navegación a internet, ya que solamente lo usan para la administración del dominio.

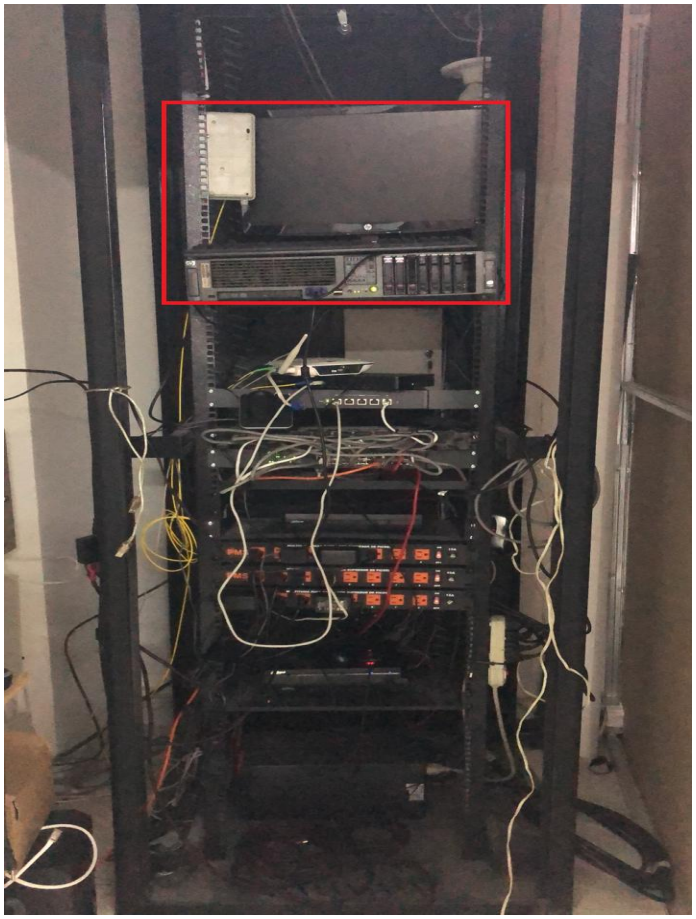

Imagen 13: Servidor de LyD Colombia S.A.S.
Fuente: Elaboración propia.

Todas las máquinas pertenecen al dominio “lydcolombia.com”, cuyas políticas abarcan el no uso de pendrives (dispositivos USB), uso del fondo corporativo de la empresa y cierre de sesiones por cada cinco (5) minutos de inactividad.

Imagen 14: Escritorio del servidor LyD Colombia S.A.S.
Fuente: Elaboración propia.

El servidor contiene dos (2) discos duros en espejo tipo RAID 1, única y exclusivamente para el dominio y para guardar los escaneos de las impresoras distribuidos en grupos creados por el dominio.

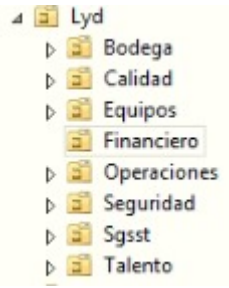

Imagen 15:Grupos del dominio.
Fuente: Elaboración propia.

Todos los usuarios están ingresados dentro de los grupos, cada usuario no puede instalar nada, solamente el administrador maneja soporte de las TIC's y la gerencia.

Los usuarios tienen claves encriptadas y entrópicas, como, por ejemplo: ca2xhR6KyV, donde se compone de mayúsculas, minúsculas, números y caracteres especiales de longitud diez (10).

La empresa cuenta con un sistema de almacenamiento remoto, que no se encuentra en LyD Colombia S.A.S. con un software que hace la gestión, llamado Drive, donde administra un SIG (Sistema Integrado de Gestión), donde se estipulan dos carpetas, una llamada Compartida y la otra Personal.

El sistema de almacenamiento remoto cuenta con una capacidad de siete (7) Terabytes (TB).

Imagen 16: Sistema de almacenamiento remoto de LyD Colombia S.A.S.
Fuente: Elaboración propia.

El almacenamiento remoto hace un Backup diario, donde la compone cuatro (4) discos duros, con tolerancia a daño RAID tipo 5.

La empresa LyD Colombia S.A.S. tiene contratado un hosting empresarial con la empresa HostDime, donde alojan la página web y el correo.

Artículo	Detalle
Paquete de alojamiento	New_EmpresarialHDCO
Nombre del servidor	sco8
cPanel Versión	80.0 (build 24)
Versión Apache	2.4.41
Versión PHP	5.6.40
Versión MySQL	10.3.15-MariaDB
Arquitectura	x86_64
Sistema operativo	linux
Dirección IP compartida	107.161.178.172
Ruta de acceso a Sendmail	/usr/sbin/sendmail
Ruta de acceso a Perl	/usr/bin/perl
Versión Perl	5.10.1
Versión Kernel	2.6.32-754.15.3.el6.x86_64

Imagen 17: Características del hosting de LyD Colombia S.A.S.
Fuente: Elaboración propia.

Server Load	2.87 (12 cpus)	✓
Memory Used	20.64 %	✓
Swap	24.56 %	✓
Disk / (/)	86 %	⚠
Disk /tmp (/tmp)	1 %	✓
Disk /boot (/boot)	38 %	✓
Disk /backup (/backup)	56 %	✓

Imagen 18: Características del hardware del hosting.
Fuente: Elaboración propia.

Esquema organizacional de la transmisión de datos:

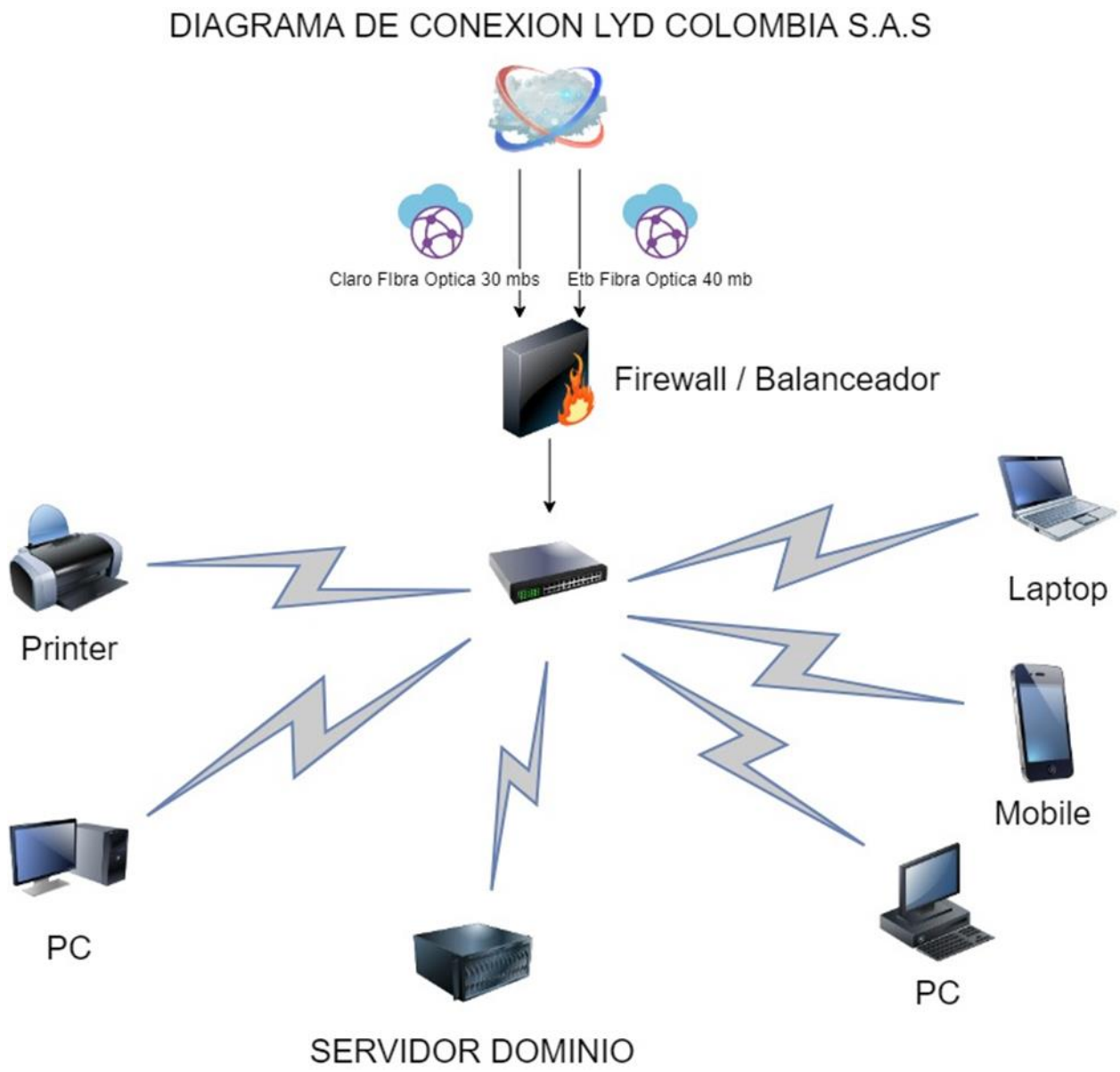

Imagen 19: Diagrama de conexión LyD Colombia S.A.S.
Fuente: Elaboración propia.

Aquí un resumen de las direcciones IP asignadas en cada dispositivo:

Dirección IP	Nombre de maquina	Observaciones
192.168.20.1	Balanceador de Carga	Equipo utilizado para asignar direcciones DHCP y balancear la navegación de dos canales de internet
192.168.20.2	Servidor de dominio	Equipo Windows 2012 server con dominio local lydcolombia.com
192.168.20.3 - 192.168.20.200	Rango reservado para asignar por DHCP a los equipos de la empresa	Rango reservado para asignar por DHCP a los equipos de la empresa
192.168.20.250	Toshiba Operaciones Piso 1	Impresora área de operaciones
192.168.20.251	Toshiba Administrativo Piso 2	Impresora todas las áreas
192.168.20.252	Kyocera Bodega Piso 1	Impresora Bodega
192.168.20.254	Router Wifi	Equipo utilizad para conectar a través de wifi los equipos inalámbricos como portátiles y celulares al balanceador de carga

Tabla 1: Direcciones IP de los equipos tecnológicos de LyD Colombia S.A.S.
Fuente: Elaboración propia.

12. CONCLUSIONES

La experiencia de realizar este diagnóstico fue gratificante para la Empresa que logró tener un concepto aterrizado de su funcionamiento y comprender qué es lo que tienen y necesitan mejorar, por ejemplo el rack que tienen con el tiempo, se fueron instalando diferentes equipos como alarmas y biometría lo que generó un desorden completo y necesita ser organizado e identificado nuevamente en caso de requerirse un soporte técnico, aunque se generan Backups de la información, nunca han realizado la prueba de restauración para evidenciar que se esté generando correctamente, los permisos de navegación aunque están bien definidos de la internet hacia la red, tienen huecos de seguridad desde la red hacia la internet, aunque los puertos USB están bloqueados para no sacar información a través de la web se pueden abrir programas de almacenamiento como Dropbox y Google Drive, donde fácilmente se podía sacar la data, se levantó la matriz de vulnerabilidades que aunque es un trabajo difícil y de interpretación, resultó ser una herramienta para identificar donde se tienen los vacíos y de qué forma es posible cerrarlos.

La metodología implementada brindo un proceso científico, donde realizado el caso de estudio, hace que el investigador se centre en identificar las verdaderas causas del problema que se detectó y se abarco, con el fin de gestionar de manera eficaz soluciones que permitan erradicar las fallas identificadas anteriormente.

Como estudiantes la oportunidad de que una compañía abra sus puertas y permita revisar uno a uno sus procesos de informática es muy difícil, la experiencia nos muestra un horizonte de

oportunidades que pueden ser explotadas en un ámbito laboral, ahora se entiende que se puede especializar en muchas áreas del conocimiento, ya sea redes, desarrollo, administración o bases de datos, el futuro es grande, inclusive, montar una empresa aunque requiere una inversión inicial, después de realizar este diagnóstico, se considera que es posible crear empresa en Colombia.

13. REFERENCIAS

- Qué son las Normas BASC - Un aliado en la lucha contra el narcotráfico. (2019). Recuperado el 20 de septiembre de 2019, desde: http://www.forodeseguridad.com/artic/discipl/disc_4037.htm
- Tendencias de la infraestructura TIC. (2019). Retrieved 21 September 2019, from https://destinonegocio.com/co/gestion-co/conoce-las-tendencias-de-infraestructura-tic/
- Cuervo, J. (2019). Legislación de Colombia. 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 q - Informática Jurídica. Recuperado el 20 de Septiembre de 2019, desde http://www.informatica-juridica.com/anexos/legislacion-de-colombia-ley-1273-de-5-de-enero-de-2009-por-medio-de-la-cual-se-modifica-el-codigo-penal-se-crea-un-nuevo-bien-juridico-tutelado-denominado-quot-de-la-proteccion-de-la-informacion-y-de-los-datos-quot-y-se-preservan-integralmente-los-sistemas-q
- RIESGOS INFORMÁTICOS. (2019). Recuperado el 19 de Septiembre de 2019, desde http://audisistemas2009.galeon.com/productos2229079.html
- ¿Qué es la seguridad informática y cómo puede ayudarme? | VIU. (2019). Recuperado el 20 de Septiembre de 2019, desde https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/

- Carrillo, J. (2019). Sistema de Gestión de Calidad, principales principios - ISO 9001:2015. Recuperado el 20 de Septiembre de 2019, desde https://www.nueva-iso-9001-2015.com/2018/04/sistema-de-gestion-de-calidad-principios/
- En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos. (2019). Recuperado el 19 de Septiembre de 2019, desde https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556
- Robo de datos y dinero: los ciberataques, entre las 5 amenazas globales más inquietantes. (2019). Recuperado el 21 de Septiembre de 2019, desde https://www.infobae.com/america/tecno/2019/02/20/robo-de-datod-y-dindero-los-ciberataques-entre-las-5-amenazas-globales-mas-inquietantes/
- Hernández Sampieri, R., Baptista Lucio, P., & Fernández Collado, C. (2008). Metodología de la investigación (5th ed., p. 546). México [etc.]: McGraw-Hill Interamericana.
- Minvivienda (2019). Recuperado el 20 de Septiembre de 2019, desde http://www.minvivienda.gov.co/Documents/Sobre%20el%20Ministerio/Sistemas-de-Gestion/NTC_ISO_9001_2015.pdf

14. BIBLIOGRAFÍA

- Hernández Sampieri, R., Baptista Lucio, P., & Fernández Collado, C. (2008). Metodología de la investigación (5ta edición., p. 546). México [etc.]: McGraw-Hill Interamericana.
- Costas Santos, Jesus, 2018, Seguridad Informatica, Bogotá, Colombia, Ra-Ma Editorial. Estándar Internacional De Seguridad Basc, 2017.

15. ANEXOS

- **Anexo 1 Estándar-Internacional-BASC-501 apartado 6**

6 SEGURIDAD EN LOS PROCESOS RELACIONADOS CON LA TECNOLOGÍA Y LA INFORMACIÓN

Orientaciones: Se considera seguridad de la información a las medidas y controles establecidos por la empresa para mantener la integridad, confidencialidad y disponibilidad de la documentación, registros y evidencias relacionadas con el SGCS.

6.1 Información

La empresa debe establecer e implementar:

a) Una política para impedir que se revele información confidencial.
b) Una política de uso de los recursos informáticos.

6.2 Seguridad en tecnología de la información

La empresa debe:

a) Establecer una política o procedimiento documentado para gestionar la seguridad informática que permita identificar, proteger y recuperar la información.
b) Utilizar cuentas asignadas de forma individual y cada usuario que acceda al sistema debe tener sus propias credenciales de acceso y mantener contraseñas; estas deben cambiarse periódicamente.
c) Revisar periódicamente los accesos asignados a los usuarios.
d) Impedir la instalación de *software* no autorizado.
e) Implementar y mantener *software* y *hardware* que proteja la información de amenazas informáticas (virus, accesos no autorizados y similares).
f) Contar con copias de seguridad de la información sensible y una copia debe almacenarse fuera de las instalaciones de forma segura con base a la gestión de riesgos.
g) Eliminar el acceso a la información a todos los colaboradores y usuarios externos al terminar su contrato o acuerdo.
h) Mantener un registro actualizado de los usuarios y claves de acceso.
i) Cerrar/bloquear la sesión en equipos desatendidos.

La empresa debería:

j) Prohibir la conexión de dispositivos periféricos personales (teléfonos inteligentes, reproductores MP3, memorias USB, etc.) a cualquier dispositivo que esté conectado a la red informática. Los puertos USB deberían ser desactivados por defecto.

- **Anexo 2 Acta**

ACTA DE AUTORIZACION DE DIAGNOSTICO PARA LA MITIGACION DE RIESGOS INFORMATICOS

Señores **LYD COLOMBIA SAS**
ciudad. Bogotá DC
Colombia

asunto: solicitud de autorización de ingreso.

con la presente el señor **CHRISTIAN QUISADO ISAZA** gerente de **LYD COLOMBIA SAS** ubicada en la ciudad de Bogotá, autoriza a los señores **WILLIAM DANILO DONCEL**, **MARIO ALBERTO PINTO BARRETO** y **MIGUEL ANGEL PEROZO** L. para realizar el Diagnóstico Para La Mitigación De Riesgos Informáticos de la empresa, permitiendo ingresar a las instalaciones de la empresa con la finalidad de recopilar información y tomar evidencia fotográfica de toda la infraestructura tecnológica. De tal manera que podamos realizar un diagnóstico de mitigación de riesgos informáticos.

Dada en la fecha 01 de agosto de 2019.

atentamente:

MIGUEL ANGEL PEROZO L.
CC. 1070.592.977 DE GIRARDOT

MARIO ALBERTO PINTO
CC. 80.240.304 DE BOGOTA

WILLIAM DANILO DONCEL
CC. 1070.617.771 DE GIRARDOT

CRISTIAN QUISADO LUGO
CC. 1032.428.430 DE BOGOTA

- **Anexo 3 Entrevistas**

Anexo 3 – recopilación de información mediante entrevistas

entrevistas Informe No. 1			
Actor:	Christian Quisado Isaza	Lugar:	Oficina gerencia
Fecha:	15/8/2019	Hora:	09:00
Tipo Instrumento:	Entrevista personal		
Estrategias:	Se realiza una entrevista personal al señor Christian Quisado Isaza, realizando las siguientes preguntas: 1) ¿Cuentan ustedes con equipos de cómputo modernos? **Rta\: El 70% de los equipos son modernos.** 2) ¿Qué aplicaciones utiliza para envío y recepción de información? **Rta\: Correo Electrónico a través de Outlook.** 3) ¿Cambia constantemente las claves de sus cuentas de correos? **Rta\: Cada 6 meses.** 4) ¿Realiza Backup de toda la información que maneja? **Rta\: Tenemos implementada una storage para toda la información personal y el sistema de gestión de calidad de la empresa.** 5) ¿Manejan software licenciado como Erp para los procesos que realiza? **Rta\: Usamos el aplicativo Seal que es propio y lo adaptaron conforme a la necesidad de manejo de ordenes de cargue con nuestros clientes.** 6) ¿Tiene usted la sensación de seguridad informática en su empresa? **Rta\: Actualmente estamos generando políticas de seguridad ya que la compañía necesita certificarse en la norma internacional Basc, donde uno de los factores importantes es tics, les agradecería que lo tuvieran en cuenta para el análisis que van a realizar a mi empresa.**		

entrevistas Informe No. 2			
Actor:	Cindy Borras	Lugar:	Oficina Ssgt
Fecha:	15/8/2019	Hora:	10:00
Tipo Instrumento:	Entrevista personal		
Estrategias:	Se realiza una entrevista personal a la señora Cindy Borras, realizando las siguientes preguntas: 1. ¿cuentan ustedes con equipos de cómputo modernos? **Rta\: Si.** 2. ¿qué aplicaciones utiliza para envío y Recepcion de información? **Rta\: WhatsApp, Skype y Correo.** 3. ¿cambia constantemente las claves de sus cuentas de correos? **Rta\: Si.** 4. ¿realiza Backup de toda la información que maneja? **Rta\: Si.** 5. ¿manejan software licenciado para los procesos que realizan? **Rta\: Si.** 6. ¿manejan usuarios y contraseñas de acceso para cada perfil? **Rta\: Si.**		

entrevistas Informe No. 3			
Actor:	Yulieth pulido	Lugar:	Oficina Talento Humano
Fecha:	15/8/2019	Hora:	11:00
Tipo Instrumento:	Entrevista personal		
Estrategias:	Se realiza una entrevista personal a la señora Yulieth pulido, realizando las siguientes preguntas: 1. ¿cuentan ustedes con equipos de cómputo modernos? **Rta\: El mío no.** 2. ¿qué aplicaciones utiliza para envío y recepción de información? **Rta\: Outlook.** 3. ¿cambia constantemente las claves de sus cuentas de correos? **Rta\: Si, los de sistemas, la cambian y la notifican cada 3 o 4 meses.** 4. ¿realiza Backup de toda la información que maneja? **Rta\: Si, tenemos una carpeta en la nube donde se guarda lo importante.** 5. ¿manejan software licenciado para los procesos que realizan? **Rta\: No sé.** 5. ¿manejan usuarios y contraseñas de acceso para cada perfil? **Rta\: Cada uno tiene un perfil propio.**		
entrevistas			

Anexo 3 – recopilación de información mediante entrevistas

Informe No. 4			
Actor	Juliana Álvarez	Lugar:	Oficina Financiera
Fecha:	15/8/2019	Hora:	14:00
Tipo Instrumento:	Entrevista personal		
Estrategias:	Se realiza una entrevista personal a la señora Juliana Álvarez, realizando las siguientes preguntas: 1. ¿cuentan ustedes con equipos de cómputo modernos? **Rta\: Si.** 2. ¿qué aplicaciones utiliza para envío y recepción de información? **Rta\: El Correo.** 3. ¿cambia constantemente las claves de sus cuentas de correos? **Rta\: Si.** 4. ¿realiza Backup de toda la información que maneja? **Rta\: Si.** 5. ¿manejan software licenciado para los procesos que realizan? **Rta\: Si.** 6. ¿utilizan plataformas seguras para realizar transacciones financieras? **Rta\: Cada banco en su plataforma y con los niveles de probación.** 7. ¿manejan software que brinde seguridad? **Rta\: Antivirus.** 8. ¿manejan usuarios y contraseñas de acceso para cada perfil? **Rta\: Si cada uno tiene contraseña única.**		

entrevistas Informe No. 5			
Actor:	Nicolás Garcia	Lugar:	Oficina Operaciones
Fecha:	15/8/2019	Hora:	15:00
Tipo Instrumento:	Entrevista personal		
Estrategias:	Se realiza una entrevista personal al señor Nicolás García, realizando las siguientes preguntas: 1. ¿Cuentan ustedes con equipos de cómputo modernos? **Rta\: Si.** 2. ¿Qué aplicaciones utiliza para envío y recepción de información? **Rta\: Correo electrónico.** 3. ¿Cambia constantemente las claves de sus cuentas de correos? **Rta\: No.** 4. ¿Realiza Backup de toda la información que maneja? **Rta\: No.** 5. ¿Manejan software licenciado para los procesos que realizan? **Rta\: Si.** 6. ¿Manejan usuarios y contraseñas de acceso para cada perfil? **Rta\: Si.**		

entrevistas Informe No. 6			
Actor	Jackelin Jiménez	Lugar:	Oficina SIG
Fecha:	15/8/2019	Hora:	16:00
Tipo Instrumento:	Entrevista personal		
Estrategias:	Se realiza una entrevista personal a la señora Jackelin Jiménez, realizando las siguientes preguntas: 1. ¿Cuentan ustedes con equipos de cómputo modernos? **Rta\: Si.** 2. ¿Qué aplicaciones utiliza para envío y Recepcion de información? **Rta\: El Correo electrónico.** 3. ¿Cambia constantemente las claves de sus cuentas de correos? **Rta\: Si.** 4. ¿Realiza Backup de toda la información que maneja? **Rta\: Si señor localmente en el pc y en la nube.** 5. ¿manejan software licenciado para los procesos que realizan? **Rta\: Si todo el software es con licencia.** 6. ¿Utilizan algún software que les ayuden a gestionar políticas integradas? **Rta\: Se están creando las políticas con el asesor de Basc.** 7. ¿Cuentan con la infraestructura tecnológica suficiente para el manejo de información? **Rta\: Si, tenemos 1 servidor robusto y la información se guarda en la carpeta de la nube.** 8. ¿Cuentan con el ancho de banda suficiente para la trasmisión de datos? **Rta\: Si, tenemos dos canales 1 es de Backup cuando el principal se satura.** 9. ¿Manejan usuarios y contraseñas de acceso para cada perfil? **Rta\: S.**		

entrevistas Informe No. 7			
Actor:	Vivian Bedoya	Lugar:	Oficina Seguridad
Fecha:	15/8/2019	Hora:	17:00
Tipo Instrumento:	Entrevista personal		
Estrategias:	Se realiza una entrevista personal a la señora Vivian Bedoya, realizando las siguientes preguntas: 1. ¿Cuentan ustedes con equipos de cómputo modernos? **Rta\: Si.** 2. ¿Qué aplicaciones utiliza para envío y recepción de información? **Rta\: WhatsApp, correo electrónico, plataforma Seal.** 3. ¿Cambia constantemente las claves de sus cuentas de correos? **Rta\: No.** 4. ¿Realiza Backup de toda la información que maneja? **Rta\: Si.** 5. ¿Manejan software licenciado para los procesos que realizan? **Rta\: No sé.** 6. ¿Manejan usuarios y contraseñas de acceso para cada perfil? **Rta\: Si.**		