PLAN DE MEJORA PARA LOS RIESGOS DE LA EMPRESA LABCORESOFT S.A.S. DESDE SU ESTRUCTURA DE CIBERSEGURIDAD Y SU IMPACTO EN LA INNOVACIÓN.

FRANCY ELISA PRECIADO GALINDO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE CIENCIAS SOCIALES Y EMPRESARIALES
PROGRAMA DE ADMINISTRACIÓN DE EMPRESAS
Bogotá
Mayo de 2024

PLAN DE MEJORA PARA LOS RIESGOS DE LA EMPRESA LABCORESOFT S.A.S. DESDE SU ESTRUCTURA DE CIBERSEGURIDAD Y SU IMPACTO EN LA INNOVACIÓN.

FRANCY ELISA PRECIADO GALINDO

Trabajo de grado presentado como requisito para optar al título de Administrador (a) de Empresas

Director
FERNANDO ALONSO OJEDA CASTRO
Economista de la Universidad Externado de Colombia

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE CIENCIAS SOCIALES Y EMPRESARIALES
PROGRAMA DE ADMINISTRACIÓN DE EMPRESAS
Bogotá
2024

Nota de aceptación

_____

_____

_____

_____

Evaluador

Bogotá D.C., junio del 2024.

Dedicatoria

Doy gracias a Dios, mis docentes y mis padres por su guía, apoyo y motivación para obtener este nuevo logro para mi vida.

Francy Elisa Preciado Galindo

Agradecimientos

Expreso mis agradecimientos a:

Al docente Fernando Alonso Ojeda Castro por su guía, paciencia y tiempo en todas las tutorías realizadas.

A mis Padres Francy Galindo y Efrén Preciado, por todo su apoyo tanto económico como emocional en todo mi proceso de mi carrera, por confiar en mi y vivir conmigo esta ilusión de obtener mi título profesional.

A la universidad Piloto de Colombia, por brindarme conocimientos, experiencias, nuevos puntos de vista, ayudarme en mi crecimiento tanto personal como profesional y por la guía para cumplir una parte de mi proyecto de vida que es obtener mi Titulo de Administración de Empresas.

A todas aquellas personas que de una u otra forma participaron en la elaboración de este proyecto.

INFORMACIÓN GENERAL DEL PROYECTO

	Descripción
Titulo Propuesto	PLAN DE MEJORA PARA LOS RIESGOS DE LA EMPRESA LABCORESOFT S.A.S. DESDE SU ESTRUCTURA DE CIBERSEGURIDAD Y SU IMPACTO EN LA INNOVACIÓN.
Modalidad Opción Grado	PLAN DE MEJORAMIENTO
Articulación con objetos de estudio del programa	Formar administradores de empresas con la capacidad de visualizar oportunidades e interpretar problemas de la organización, desde sus aspectos de gestión y sus relaciones con el entorno, para formular y desarrollar soluciones organizacionales y proyectos empresariales con enfoque sostenible.
Articulación con líneas de investigación de programa	Innovación en la gestión.
Articulación con el perfil de egresado	Profesional innovador en las prácticas de gestión organizacional para el emprendimiento y la interacción responsable con el entorno, apoyado en la toma de decisiones, basado en la dirección de proyectos para el manejo apropiado de los recursos y las nuevas tecnologías
Trabajo producto de semillero. Indique el semillero.	Mi trabajo de grado no es producto de semillero

CONTENIDO

Pág

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

Pág.

Resumen

TÍTULO: PLAN DE MEJORA PARA LOS RIESGOS DE LA EMPRESA LABCORESOFT S.A.S. DESDE SU ESTRUCTURA DE CIBERSEGURIDAD Y SU IMPACTO EN LA INNOVACIÓN.

Autor(es): Francy Elisa Preciado Galindo

Palabras clave: Diamante de la Innovación, riesgo, ciberseguridad, virus informático, ciberataque.

Abstract

TITLE: IMPROVEMENT PLAN FOR THE RISKS OF THE COMPANY LABCORESOFT S.A.S. FROM ITS CYBERSECURITY STRUCTURE AND ITS IMPACT ON INNOVATION.

Author(s): Francy Elisa Preciado Galindo

Keyword: Diamond of Innovation, risk, cybersecurity, computer virus, cyber attack.

INTRODUCCIÓN.

La razón de ser de este documento es conocer como minimizar los escenarios de riesgo, mejorando el imparto en Innovación relacionado en el ámbito de Ciberseguridad en la empresa Labcoresoft S.A.S., debido a que existe una relación estrecha entre la Ciberseguridad y la capacidad de un país de salvaguardar de manera correcta esta información, lo cual podría poner en tela de juicio la reputación de la misma.

Se recomienda con el uso del Diamante de la Innovación a la empresa Labcoresoft S.A.S., restructurar la gestión asociada a la ciberseguridad, esto ayudara a salvaguardar la información de todos los clientes que maneja cada hospital con el cual trabaja la compañía y garantizar una mejora en la innovación de la organización.

Se realiza la aclaración que el margen de análisis histórico se encuentra desde el año 2020 un año antes del COVID 19 y el segundo semestre del 2023, para rastrear el tema de la ciberseguridad antes y después de la Pandemia, sin dejar de lado que el trabajo se encuentra a portas de ser entregado y no se quiere incurrir en modificaciones continuas, si no determinar una línea del tiempo que lleva y el trabajo tenga un alcance histórico también, evitando que cada vez que se realice una modificación se deba actualizar el marco del arte o la organización.

Dejando claridad que se van a manejar gráficos, los cuales brindan un aporte a el planteamiento del problema y estos tendrán los títulos originales por respeto a los diferentes autores. En el marco conceptual se encuentran los conceptos explicados tal y como se van a usar a lo largo del trabajo.

En la primera parte del trabajo se realiza una muestra de la situación actual de la empresa de manera más técnica dando a conocer las falencias que se presentan en la misma y como esta falta de innovación en la compañía puede poner en desventaja competitiva a la organización en el mercado.

En la segunda parte del trabajo se genera el planteamiento de las posibles soluciones del problema presentado sobre la Ciberseguridad y como podría afectar este de manera positiva en la Innovación de la compañía, se propone una estructura de riegos teniendo en cuenta diferentes matrices, las cuales son alimentadas con información y datos directamente de la empresa, como lo son:

- POAM
- PCI
- DOFA
- Diagrama de Gantt
- Matriz de Riesgo.

Luego del análisis de las mismas se propone implementar una nueva área que trabaje de manera transversal con todas las demás dependencias de la compañía, encargada de la Ciberseguridad directamente, lo cual dará un valor agregado en temas de Innovación a la empresa, ayudando a que tenga un mejor nivel

reputacional. Se busca implementar la ISO 27001 la cual es la norma internacional de seguridad de la información, debido a que la empresa maneja datos personales y resultados de exámenes médicos los cuales puede ser sensibles y afectar a la integridad de las diferentes personas.

1. PRESENTACIÓN DEL TRABAJO DE GRADO.

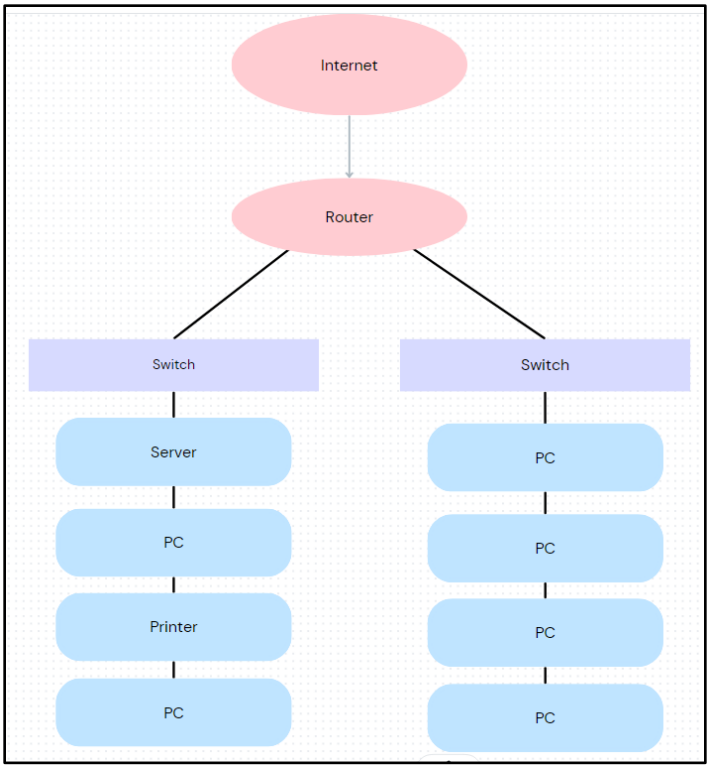
1.1. SITUACIÓN ACTUAL DE LA EMPRESA LABCORESOFT.

Labcoresoft S.A.S cuenta con una topología de red tipo árbol, en la cual después de su respectivo servicio de internet se despliega toda la red por medio de un *Router* el cual se encarga de distribuir internet e intranet a los diferentes computadores y servidores de la organización permitiendo así que todo estén interconectados, sin embargo esta topología no es suficiente para garantizar la seguridad de la información ya que esta puede quedar muy expuesta al exterior y entidades malintencionadas que pretendan tener acceso forzado a los sistemas de la información.

Si bien la compañía cuenta con un servidor de Dominio que le permite tener control interno sobre los dispositivos este no es suficiente para garantizar la protección de las bases que manejan información sensible de terceros (tratamiento de datos personales).

Figura 1.

Diagrama topología actual Labcoresoft S.A.S.



Nota. El grafico muestra la topología actual de la empresa Labcoresoft S.A.S. Fuente: Hecho por la autoría, según datos tomados de: La Empresa Labcoresoft S.A.S.

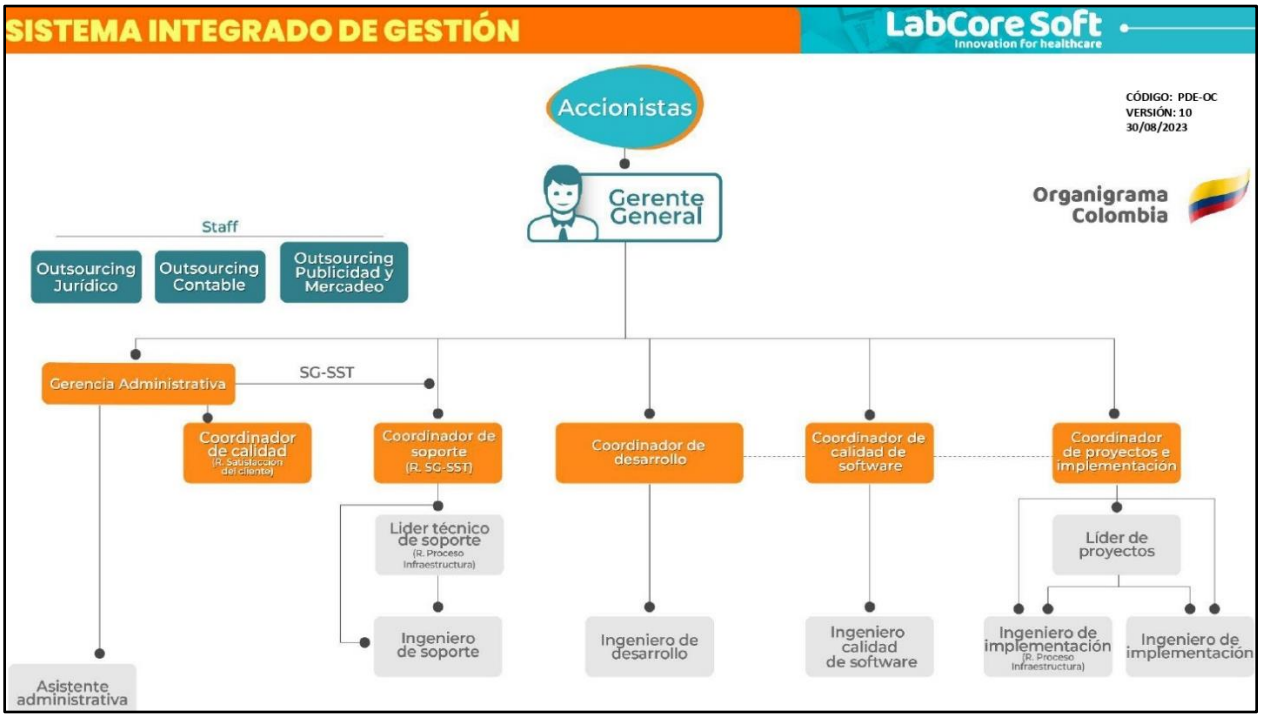
Si bien esta topología es utilizada en muchas organizaciones, no es la adecuada para el modelo de negocio de la compañía puesto que no ofrece la redundancia y protección necesaria para la continuidad de la operación.

Organigrama

Como se evidencia en la imagen adjunta actualmente la empresa Labcoresoft S.A.S., no cuenta con un área de Ciberseguridad implementada lo cual como se mencionaba anteriormente la pone en desventaja competitiva frente a las demás compañías. Con lo anterior es claro que es importante plantear acciones de mejora respecto a esta falencia tomando como referencia uno de los ocho puntos del Diamante de la Innovación, el cual es el de Ciberseguridad.

Figura 2.

Organigrama Labcoresoft S.A.S.



Nota. El grafico muestra el organigrama actual de la compañía Labcoresoft S.A.S. Fuente: hecho por la autora. Según datos logrados en: https://labcoresoft.atlassian.net/wiki/spaces/~898781351/pages/913473888/ORGANIGRAMA+COLOMBIA+PDE-OC

1.2. ANTECEDENTES.

Varias empresas presentan falencias en el área de Ciberseguridad ya que consideran que esta no es tan importante o que no puede llegar a afectar de manera significativa a las diferentes áreas de la compañía, lo cual es totalmente erróneo debido a que si no se toman las medidas necesarias esto puede perjudicar grandemente a la organización.

Como se observa en el artículo "Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales.", busca dar a conocer que las organizaciones no toman a tiempo las medidas técnicas y organizativas, en aquellos eventos que afecten los Datos Personales, en este caso pueden entrañar daños y perjuicios materiales o inmateriales para sus Titulares.

De ahí que la importancia de la gestión de los incidentes de seguridad deba ser desde: el diseño de las actividades del tratamiento, el complemento de las políticas de seguridad de la información y protección de datos y la ética corporativa de las empresas. (Montezuma L.A., Gómez C., Salazar C.E. & Hurtado A.L., 2020. Pág. 8)

En este caso se puede observar que la seguridad genera confianza. Si falla, es clave que la empresa este bien preparada y entrenada para actuar frente a los incidentes de seguridad de manera inmediata, profesional e inteligente. (Montezuma L.A., Gómez C., Salazar C.E. & Hurtado A.L., 2020. Pág. 21)

También vemos en el trabajo "Propuesta metodológica para la gestión de proyectos de innovación en una empresa del sector de la construcción inmobiliaria en Colombia.", como se evidencia que en la práctica empresarial surgió el término de "innovación", el cual se asocia con la sostenibilidad de las empresas a través del desarrollo de nuevos modelos de negocio, servicios, productos o sistemas organizacionales. Es allí, donde la presente monografía propone una búsqueda de antecedentes y buenas prácticas que se tienen documentadas en el desarrollo de proyectos de innovación y cómo la gestión de proyectos interviene para garantizar que las ideas de innovación se materialicen exitosamente. (Giraldo A. & Mafla M.A., 2021 pág.16)

Se obtiene como resultado que una de las principales razones de esta baja productividad se debe a la baja inversión en tecnología por parte de las empresas. La vulnerabilidad del sector frente a factores externos (como cambios económicos) resta a las empresas de incentivos para invertir en tecnología. Esto ha provocado un estancamiento del desarrollo tecnológico del sector y por tanto, las empresas presentan bajos niveles de adopción de tecnologías de alto valor agregado. Como consecuencia, las empresas del sector de la construcción ofrecen servicios (como los servicios inmobiliarios) que se han mantenido inmutables a lo largo del tiempo, haciendo que el sector se quede alejado de las tendencias globales de industria 4.0. (Giraldo A. & Mafla M.A., 2021 pág. 06)

En el boletín "Vigilancia Tecnológica en Ciberseguridad" basado en la edición 2021 del informe líder *Cost of a Data Breach Report*, de 2020 a 2021 a nivel mundial, como el Costo de una filtración de datos pasó de USD $3.86 millones a USD $4.24 millones; éste es el costo total promedio más alto jamás registrado. Según

el mismo reporte, las regiones con el mayor aumento promedio del costo son América Latina (aumento del 52.4%), Sudáfrica (aumento del 50%),
Australia (aumento del 30.2%), Canadá (aumento del 20%) (*IBM Segurity*, 2021). Además de los costos económicos, los ataques informáticos también tienen afectaciones a la infraestructura crítica, la cohesión social y el bienestar mental de la población (*World Economic Forum*, 2022; *ITU*, 2022). (Solleiro J.L., Castañón R., Guillén A.D., Hernández T.Y., & Solís N., 2022 pág. 8)

Como resultado se obtiene que es claro que la ciberseguridad ya no puede considerarse un tema exclusivamente técnico que se delegue en el personal de tecnologías de la información de las organizaciones, sino que debe abordarse como tema estratégico que alcanza a toda la organización. A medida que las amenazas cibernéticas continúan creciendo, los seguros contra riesgos informáticos serán cada vez más precarios y las propias empresas aseguradoras enfrentarán posibles juicios y represalias por intentar frenar los pagos por *ransomware*. Por lo tanto, cuando ocurre un ataque, las empresas se verán obligadas a pagar rescates cada vez más altos o sufrir las consecuencias reputacionales, financieras, regulatorias y legales de los ciberataques. Lo mejor es tener una estrategia robusta y coordinada dentro del ecosistema. (Solleiro J.L., Castañón R., Guillén A.D., Hernández T.Y., & Solís N., 2022 pág. 8)

Según el artículo “Cybersecurity, An Axis On Which Management Innovation Must Turn In The 21st Century” observamos que desde los inicios del servicio de internet se han generado problemas con el tema de la ciberseguridad, teniendo en cuenta las diferente guerras presentadas en esta etapa donde se buscaba robar información, desde el año 1949 empieza este tema relacionado con la informática y de este año se desprenden tanto las cosas buenas como las cosas malas que trae el internet, nos beneficia brindando información de manera amplia y global, pero también nos afecta porque nuestros propios datos o información confidencial puede estar en riesgo, ya sea por robo o por pérdida de la misma, por eso se han implementado diferentes técnicas para salvaguardar los datos que le pertenece a cada uno y que no debería ser violentada.

Es evidente que no manejar procesos estructurados de ciberseguridad hacia un país, organización o empresa, trae consecuencias evidentes sobre la innovación de estos. (Ojeda F.A., 2021 pág. 110)

De acuerdo a el trabajo “La ciberseguridad como solución de privacidad: Especial incidencia en la privacidad desde el diseño” comienza identificando a los principales actores que participan en el ámbito de la protección de datos y desgranar los principios más importantes a los que han de atender para adecuar sus organizaciones a la legislación actual. Se profundiza en uno de los principales cambios que ha traído consigo el nuevo RGDP, un aspecto fundamental para todo aquel que pretenda desarrollar y comercializar servicios digitales de seguridad de la información, esto es la protección de datos desde el diseño. (Gil Miñano, R. 2022 pág.3)

Se menciona el RGPD (Reglamento General de Protección de Datos) es la mayor revisión de las normas de privacidad desde el nacimiento de Internet. En este nuevo contexto, el modelo de cumplimiento ha cambiado, pasando de un modelo de cumplimiento formal a un modelo de responsabilidad proactiva, en el que no incumplir ya no es suficiente, sino que ahora hay que cumplir y demostrarlo. (Gil Miñano, R. 2022 pág.6)

Roberto indica que juntos, RGPD y LOPDGG, rigen el día a día de aquellas compañías que acceden y/o tratan datos de carácter personal. Estas empresas, en aras de tratar los datos personales de los ciudadanos con la mayor legalidad, seguridad y transparencia posible, han de cumplir con una serie de principios básicos que vienen regulados en estas normas. Uno de estos principios, que por su novedad ha supuesto uno de los grandes cambios que el RGPD ha traído consigo, es el principio de responsabilidad proactiva, o *accountability*, que implica la adopción de ciertas medidas que permitan cumplir (así como demostrar dicho cumplimiento) lo estipulado en el RGPD. Una de estas medidas, tal vez una de las más importantes, es la que tiene que ver con la aplicación de la protección de datos desde el diseño. (Gil Miñano, R. pág.54)

Por último, en el trabajo "MARCO DE GOBIERNO Y GESTIÓN DE CIBERSEGURIDAD PARA CIUDADES INTELIGENTES EN EL CONTEXTO COLOMBIANO" menciona que la tecnología se busca proporcionar servicios y resolver los problemas de las urbes, facilitando la movilidad, mejorando los servicios sociales, la sostenibilidad y la seguridad con una escucha activa y constante de las necesidades de los ciudadanos. De esa manera nacen productos que en sus primeras versiones buscan ofrecer servicios básicos y recolectar información en tiempo real que apalancan la toma de decisiones efectiva, la creación de nuevas y mejores herramientas enfocadas en proveer bienestar y disminuir el uso de recursos que cada vez son más limitados. (García L.E., & Nieto W., 2021 pág. 10)

Se puede evidenciar que los pilares de la seguridad de la información son la disponibilidad, la integridad y la confidencialidad, incluso algunos autores incluyen la autenticación como un cuarto pilar, cuando se quiere evaluar el tema de ciberseguridad a nivel de una ciudad son muchos más los aspectos a considerar para ejercer un control efectivo que permita garantizar a los ciudadanos la privacidad de sus datos directos o indirectos, la prestación de los servicios y la interconexión de los distintos sistemas desplegados." (García L.E., & Nieto W., 2021 pág. 75)

Con lo anterior se puede concluir que la innovación en el campo de la ciberseguridad es esencial para hacer frente a las crecientes amenazas y desafíos en el panorama digital actual. A medida que los ciberataques se vuelven más sofisticados y generalizados, la necesidad de soluciones innovadoras y adaptativas se vuelve cada vez más crítica, lo cual a su vez puede llegar a afectar las compañías que manejan datos sensibles de manera digital. (Chat GTP, 2024 22 de abril, 00:10) Ver Anexo 1.

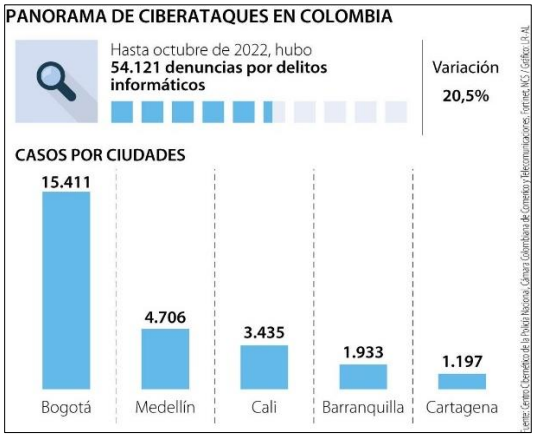
1.3. PLANTEAMIENTO DEL PROBLEMA.

La empresa Labcoresoft es una compañía de software para laboratorios clínicos que se especializa en brindar soluciones y optimizar la trazabilidad en las fases preanalítica, analítica y post analítica de la toma de pruebas, análisis y resultados. Brinda un soporte de digiturno, facturación y base de datos del paciente. Cuenta con presencia en varios hospitales de América latina, es una empresa reconocida en más de 10 países, pero como se mencionaba anteriormente esta no cuenta con un sistema de ciberseguridad, esto puede afectar directamente a su innovación en los procesos clínicos de los hospitales por robo de la información

que afecte proyectos asociados a la innovación de los softwares que manejan, como lo son: Labcore, *Patcore* y *Bbcore*.

Figura 3.

Panorama de ciberataques en Colombia.



Nota: El grafico muestra los diferentes casos de ciberataques presentados por ciudades en el año 2022. Tomado de: Diario La República. (2022). EPM y Afinia, entre las compañías que han sido víctimas de ciberataques. Obtenido de: https://www.larepublica.co/empresas/epm-y-afinia-entre-las-companias-que-han-sido-victimas-de-ciberataques-en-el-ano -3510742

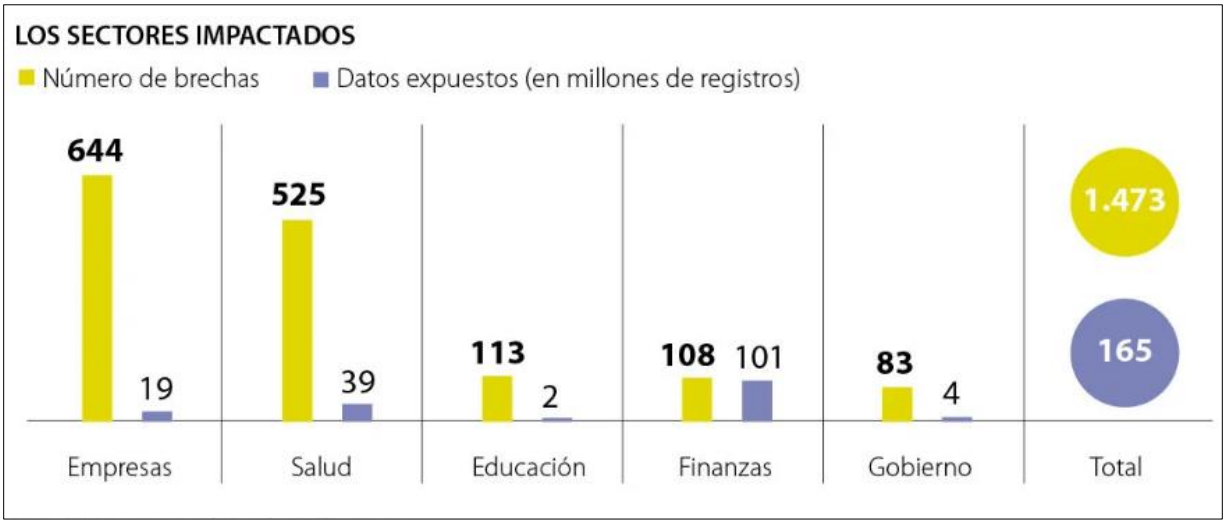
De acuerdo a la gráfica anterior se puede evidenciar en las ciudades donde se presenta mayor problema con ciberataques son: Cartagena (1.197), Barranquilla (1.933), Cali (3.435), Medellín (4.706) y Bogotá D.C., con la cifra más alta obteniendo un total de 15.411, es decir con un aproximado de más del 70% comparado con el resto de las ciudades anteriormente mencionadas en ciberataques hasta octubre del 2022.

Según lo descrito por Gutiérrez (2022) “Hoy más que nunca, en la era de la tecnología, uno de los activos más valiosos para cualquier empresa es la información. Por eso mismo, la data es una mina de oro para los delincuentes.” (Párrafo 1). Diana Robles, líder de *IBM Security* para Colombia, Perú, Ecuador, Venezuela y Región Caribe, indicó que el punto de quiebre estaría en la prevención, pues indica que es clave que las empresas busquen una estrategia que se anticipe a los ataques y no tanto de detención, “eso hace la diferencia”. Además, porque, según la experta, el tiempo promedio para identificar y contener una filtración de datos en las empresas es de 331 días (251 para identificar y 80 para contener), lo cual es demasiado tiempo, expresa.” (Párrafo 12)

Con lo anteriormente mencionado se ve reflejado que Bogotá es la ciudad donde se presenta mayor cantidad de ciberdelincuencia, donde se encuentra la empresa Labcoresoft S.A.S., y es evidente que si la compañía no toma las medidas necesarias estaría afectando directamente su innovación en el mercado, poniendo en riesgo su reputación y los resultados de exámenes médicos de todos los pacientes con sus datos respectivos.

Figura 4.

Los sectores impactados.



Nota: Esta grafica muestra los sectores más afectados o impactos a nivel de ciberataques. Tomado de: Diario La República. (2020). Este es el costo en el que incurren las empresas al no detectar a tiempo un ciberataque Obtenido de: https://www.larepublica.co/internet-economy/este-es-el-costo-de-no-detectar-a-tiempo-un-ciberataque-3062686

Como se evidencia en la gráfica número 4, podemos observar que los datos expuestos en mayor cantidad son los financieros con un total de 101 millones de registros, seguido de los datos en el sector de la salud con un total de 39 millones de registros y finalmente llegando al grupo empresarial con un total de 19 millones de registros expuestos, estos son datos hasta el 2020, los cuales nos hacen ver que realmente es preocupante el impacto de la falta de ciberseguridad tanto en las empresas como en el sector de la salud que en este caso se relaciona con el objeto del estudio.

"Uno de los datos más llamativos es el tiempo que tarda una organización en identificar que está comprometida. Un adversario entra la red y se queda a vivir allí por casi siete meses sin ser detectado. Cada año las empresas incrementan su gasto en ciberseguridad, pero las brechas no paran de crecer", expresó Ricardo Villadiego, fundador y *CEO* de *Lumu Technologies.* (Párrafo 3)

Pablo Iragorri, director ejecutivo y jefe de Kroll en Colombia, agregó que, como consecuencia del covid-19, el riesgo en seguridad cibernética es mayor, así como en el de los fraudes, ya que los equipos laboran en una situación atípica, con una supervisión limitada y con una percepción de que están siendo monitoreados menos de lo normal. (Párrafo 7)

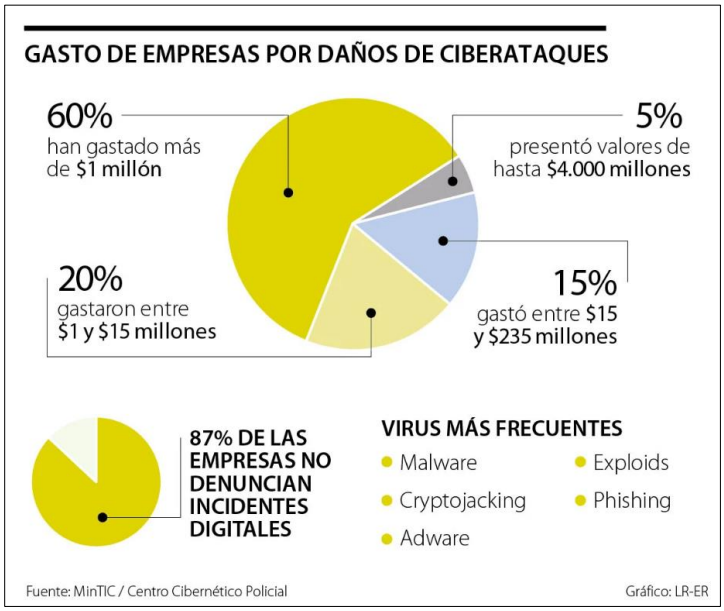
Según lo descrito por Blanco (2020) Con la pandemia, desde Kroll Colombia consideran que las industrias con mayor riesgo de fraudes son la salud, el *e-commerce*, el transporte, los envíos, el sector de

infraestructura y las empresas que realizan gran parte de su trabajo con equipos en campo que están lejos de las oficinas principales. “Muchos de estos negocios han estado operando durante la crisis y, debido a la necesidad de suplir la demanda de manera rápida, pueden haber contratado proveedores, servicios, personal e instrumentos de trabajo sin pasar por los debidos procesos de compras”, dijo Iragorri. (Párrafo 10). Los datos financieros que se pueden ver violentados con datos personales que pueden salir tanto de empresas como de sector salud, donde tienen información personal, la cual pueden estar expuestos en una historia clínica, esta puede afectar a los diferentes pacientes con robos de identidad, extorciones, daños psicológicos y demás que afectan directamente la integridad de la persona.

En el 2020 se generó diferentes ciberataques, el 37% de estos se genera por acceso no autorizado, mientras que el 39% de se presenta por *Hacking*, es decir robo de información por medio de plataformas informáticas, mientras que los porcentajes más pequeños como el 2%, 4% y 6%, hacen referencia a robos de información física o exposición accidental online, como se ve la mayoría de ataques se genera por medio de internet, esto evidencia un riesgo grande para la compañía en cuestión de ciberataques, por lo cual se reitera la importancia de generar conciencia en la empresa sobre este problema el cual afectaría directamente la innovación de la misma, generando perdidas en diferentes ámbitos: económicos, reputacionales, mano de obra, entre otros.

Figura 5.

Gastos de empresas por ciberataques.



Nota: Este grafico muestra la cantidad de dinero que gastan las diferentes empresas cuando enfrenten daños provocados directamente por la ciberseguridad. Tomado de: Diario La República. (2019). ¿Cuánto gastan las empresas para recuperarse después de un ciberataque? Obtenido de: https://www.larepublica.co/internet-economy/cuanto-gastan-las-empresas-para-recuperarse-despues-de-un-ciberataque-2889536

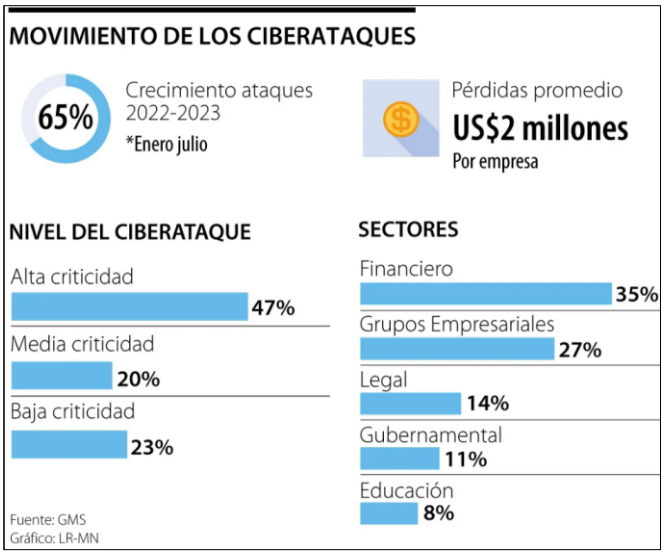
Por otro lado hasta el 2019 se registraba que el 87% de las empresas no generan denuncias sobre los robos digitales, pero estos hechos generan un perdida en las diferentes compañías, es así como se registra que el 60% ha gastado más de COP 1.000.000, el 20% de COP 1.000.000 y COP 15.000.000, 15% más de COP 235.000.000 y 5% más de COP 4.000.000.000, con todo esto podemos concluir que si una compañía no tiene brindada la información que maneja, si no salvaguarda bien los datos que se posee actualmente se puede llegar a grandes gastos de dinero los cuales no están programados y pueden generar un daño directamente a la empresa, por lo cual es importante tener un líder de departamento para salvaguardar la información, generar conciencia de la importancia de esta, llevar a cabo planes de trabajo para la seguridad de la información de la empresa y de esta manera contrarrestar este tipo de gastos inesperados, por no detectar a tiempo un ciberataque, los cuales si llegan a ser muy altos pueden llevar a la quiebra a una empresa en cualquier momento. Ojeda. F.A. (2019)

Al respecto, Jorge Guillermo Neira, gerente *senior* de *BDO*, hizo un llamado a las empresas, al destacar que "hoy en día, la auditoría TI es una obligación, más que una necesidad, para evitar la pérdida de información, intrusión de terceros, fraudes informáticos y la destrucción de información de las firmas".

Según Loaiza (2019) Para prevenir y solucionar este tipo de problemas se pueden hacer dos tipos de auditorías. Una, a los controles generales de los sistemas de tecnología e información, que revisa aspectos fundamentalmente del funcionamiento para garantizar la seguridad y la continuidad de las plataformas; y otra, una auditoría de propósito específico, encaminada a la revisión de aspectos puntuales en los que se vean amenazas focalizadas para cada empresa. (Párrafo 4)

Figura 6.

Movimientos de los ciberataques



Nota: En esta grafica se evidencia la afectación de ciberataques en los diferentes sectores. Tomado de: Diario La República. (2023). Ciberataques subieron 65% siendo los bancos e industriales sus blancos más comunes.. Obtenido de: https://www.larepublica.co/empresas/reporte-ciberseguridad-2023-a-empresas-y-sectores-3701737

En la actualidad de enero 2022 a julio 2023, se evidencia que el sector el cual cuenta con mayor cantidad de ciberataques es el financiero con un 35% y luego viene el empresarial con un 27%, en este caso se puede observar que el nivel de criticidad es alta con un 47%, esto refleja nuevamente que el riesgo es alto y que el sector empresarial es uno que actualmente se encuentra más afectados.

Según López (2023) Mientras los procesos digitalizan cada vez más, también obliga a las empresas a protegerse de nuevos ataques por parte de hackers. Según el reporte Ciberseguridad: 'Panorama regional 2022 - 2023' realizado por GMS Seguridad, los ciberataques en lo corrido de este año han tenido un aumento de 65% si se compara con 2022. (Párrafo 2). “La ciberseguridad es esencial para la supervivencia de cualquier organización en la era digital. Las empresas deben invertir en la protección de sus activos digitales y en la educación de sus empleados para evitar las fugas de información. De acuerdo con nuestros reportes, en promedio en América Latina una empresa al año pierde US$2 millones por el impacto de los ciberataques” manifestó Alejandro Navarro, gerente general de GMS Seguridad en Colombia. (párrafo 4)

Finalmente se observa que al no tomar medidas tempranas sobre los ciberataques se afecta la empresa directamente en el tema financiero, generando gastos y perdidas de maneras descomunales, se presenta una perdida reputacional, los datos que se encuentran en la red son altamente expuestos y esto puede generar daños a las diferentes personas o empresas que se encuentren en esta brecha de exposición, aunque el sector financiero es el más afectado por la problemática, el sector empresa y salud no se quedan atrás y son los que busca analizar, ya que la empresa está relacionada con un software y con datos de pacientes en diferentes hospitales de Colombia y países de Latinoamérica, todo esto pone en riesgo la innovación de la compañía, lo cual deja en desventaja a la empresa frente a sus competidores, no solo por el robo de datos que se puede generar a los diferentes pacientes, si no al software como tal, los diferentes programas: *Labcore*, *Patcore* y *Bbcore*, que al estar expuestos pueden ser robados, duplicados o suplantados lo cual generaría pérdidas directas a la compañía afectando toda su estructura.

Actualmente la compañía se está centrando en ofrecer el producto, venderlo, facturar, generar ganancias de forma mensual, cerrar proyectos, pero dejan a un lado una parte muy importante que es la ciberseguridad, salvaguardar no solo su información, sino también el de todos los pacientes y colaboradores que se relacionan con esta, poniendo en riesgo toda la trayectoria y ganancias de Labcoresoft S.A.S.

Descripción de la situación problema.

Se detecta un problema de tipo organizacional, ya que la gestión del Big Data debe tener un Manager, una persona encargada de cuidar este tipo de información, pero en este caso no se evidencia o no se cuente con esta persona.

En la empresa Labcoresoft S.A.S., se encuentra una falencia en el proceso de ciberseguridad, ya que no se presenta de manera correcta el manejo de la información en las diferentes áreas, las contraseñas: son conocidas por toda la empresa, cuando se realiza un retiro de algún colaborador no se genera cambio de las mismas o los correos, las contraseñas de los computadores son genéricas y la mayoría de los colaboradores tienen conocimiento de estas, por ende no son seguras, no se cuenta con respaldo de la información en los diferentes equipos lo cual pone en riesgo la información, no existen capacitaciones sobre el tema de ciberseguridad al personal administrativo, no se realizan campañas de concientización sobre las amenazas en la red, no se genera el cambio de contraseñas en los clientes, lo cual genera un riesgo para los datos

personales de los pacientes, porque aunque las contraseñas de los clientes estén encriptadas la información del paciente como tal no, lo cual representa un riesgo grande para los diferentes pacientes ya que podrían ser víctimas de un ciberataque donde se les puede generar un robo de toda su información personal, como nombres, cedula, dirección de residencia, teléfonos, personas cercanas o contactos relacionados a la persona como tal, los diferentes resultados de los estudios realizados en los hospitales, lo cual atenta grandemente a la privacidad del paciente.

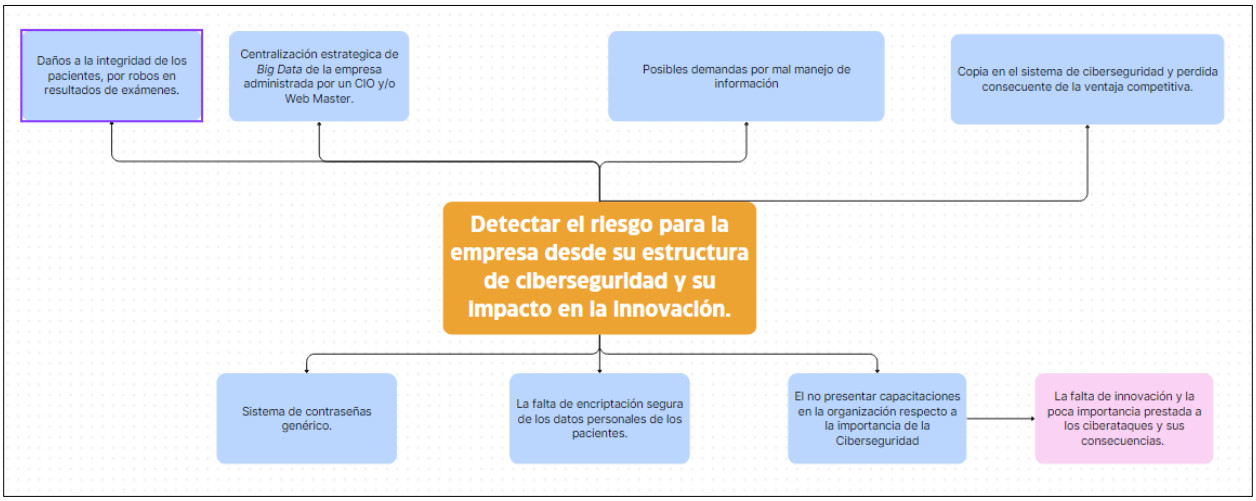
Si dejar de lado que algunos accesos se pueden generar en cualquier equipo y en cualquier parte del mundo, es decir que no es necesario estar conectado a la red de la compañía para acceder a esta información. De forma remota también se puede tener acceso a esta, algunas veces sin clave lo cual pone en riesgo la seguridad de la información.

Lo anteriormente mencionado nos indica que uno de los efectos importantes de no cuidar una organización, país, ciudad o empresa. Su seguridad, su Big Data es expuesta potencialmente a que un tercero utilice esos datos y frustre la capacidad de innovación de las mismas. Directamente existen personas que tienen conocimiento de los diferentes desarrollos de la compañía, como lo son *Labcore*, *Patcore* y *Bbcore*. De los cuales se han generado conexiones de manera irregular, donde los clientes tienen el servicio, pero no generan pago por este, porque quizás un colaborador retirado de la compañía le brindo el acceso de manera fraudulenta.

Árbol de problemas.

Figura 7.

Árbol de problemas.



Nota. El grafico muestra el árbol de problemas presentado en la empresa Labcoresoft S.A.S. Fuente: Hecho por la autoría, según datos tomados de: La Empresa Labcoresoft S.A.S.

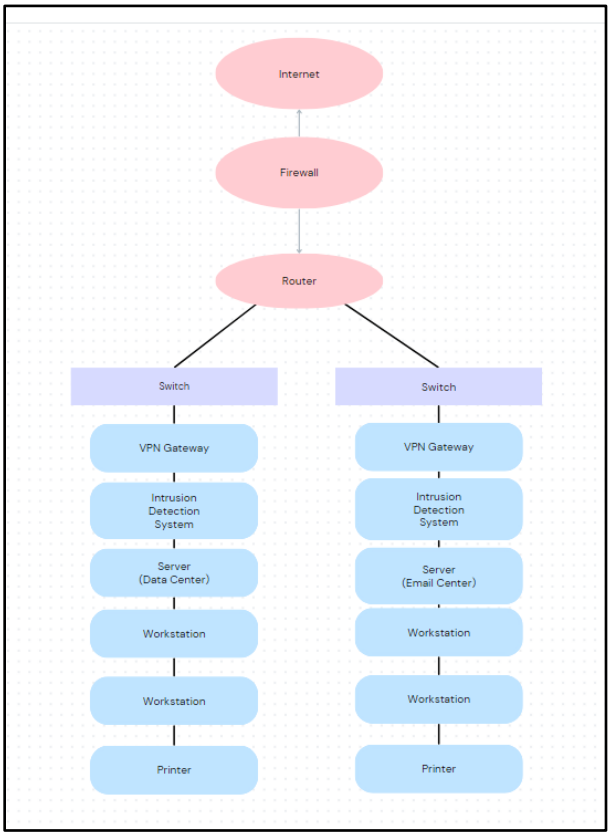
1.4. ALTERNATIVAS DE SOLUCION

Se plantea una topología que cumple con la NORMA ISO 27001 la cual está debidamente estandarizada y permite una ampliación continua además de mejorar constantemente la infraestructura para así estar a la vanguardia que permite la Ciberseguridad en la protección de datos.

Diagrama tipología tipo Jerárquica ofrecida:

Figura 8.

Tipología tipo Jerárquica ofrecida.



Nota. El grafico muestra la tipología ofrecida para las falencias de ciberseguridad presentadas en la empresa Labcoresoft S.A.S. Fuente: Hecho por la autoría, según datos tomados de: La Empresa Labcoresoft S.A.S.

Este tipo de topología o infraestructura proporciona una capa adicional de seguridad y protección para los datos lo cual es muy beneficioso y necesario para la compañía, ya que de esta manera se garantiza que la

información sea netamente de la misma evitando filtraciones de seguridad. Contar con los siguientes dispositivos ofrecen una mayor seguridad por lo descrito a continuación:

***Firewall*:**

- Control de acceso: un firewall actúa como una barrera entre las redes internas y externas, filtrando el tráfico de red entrante y saliente de acuerdo con reglas predefinidas. Esto ayuda a prevenir ataques no autorizados y protege los recursos de la red de intrusos.

- Bloqueo de amenazas conocidas: el firewall puede bloquear el tráfico malicioso conocido, como virus, malware, phishing y ataques de denegación de servicio (DDoS), antes de que lleguen a su red interna.

- Segmentación de la red: al dividir una red en zonas seguras y no seguras, un firewall puede controlar el acceso entre diferentes partes de la red, limitando así la propagación de ataques y reduciendo la superficie de ataque.

- Registro y monitoreo: el firewall registra y monitorea el tráfico de la red para identificar patrones sospechosos y actividades anómalas para ayudar a detectar y responder a incidentes de seguridad.

Servidores de cifrado:

- Confidencialidad de datos: los servidores de cifrado utilizan algoritmos criptográficos para convertir datos a un formato ilegible mientras están en tránsito por una red. Esto garantiza que los datos confidenciales permanezcan protegidos incluso si el tráfico de la red es interceptado y no puede ser leído por personas no autorizadas.

- Protección de integridad: el cifrado también protege la integridad de los datos al garantizar que no se modifiquen durante la transmisión. Los cambios en los datos cifrados se detectan fácilmente y se consideran no válidos.

- Cumplimiento normativo: a menudo se requiere el uso de cifrado para cumplir con las regulaciones de protección de datos como GDPR, HIPAA y PCI-DSS que requieren proteger la confidencialidad e integridad de la información del usuario.

- *Cloud Security*: para las organizaciones que utilizan los servicios en la nube, los servidores de cifrado pueden proporcionar una capa adicional de seguridad al cifrar los datos antes de almacenarlos o enviarlos a través de la red.

En resumen, los firewalls y servidores de cifrado en esta topología de red ayudan a proteger sus datos y su infraestructura de red de amenazas externas e internas y garantizan la confidencialidad, integridad y disponibilidad de su información.

Estas medidas son esenciales para mantener la seguridad de la red en un entorno cada vez más digital y conectado.

Creación de cargo para el manejo del área de Ciberseguridad.

En este caso se busca realizar una creación de un nuevo cargo para el área de Ciberseguridad en la compañía, esto ayudaría a contrarrestar las diferentes falencias presentadas en la empresa relacionadas con la seguridad informática que actualmente está establecida en Labcoresoft S.A.S.

Mejoras que se pueden implementar en la infraestructura de Labcoresoft S.A.S.

Después de dejar a una persona encargada del área de ciberseguridad, se debe contratar un sistema de seguridad para empezar a filtrar todo el tema de tráfico, quien ingresa a la red y los diferentes usuarios, restringir el acceso a los servidores, manejo de las claves, crear un directorio para el control de acceso a los diferentes usuarios por áreas con restricciones específicas a nivel de un servidor y licencias manejando un Windows Pro que permita tener unas configuraciones más específicas, configuración de red para ingreso solamente de los clientes, otra diferentes para los invitados y otra para los colaboradores de la empresa, por ultimo mejora en las aplicaciones impidiendo insertar en algunos campos caracteres especiales, como porcentajes, guiñes, asteriscos, entre otros, porque esto sería inyección de base de datos y se podría generar ataques o ingreso de virus al sistema, los diferentes clientes o al mismo software.

1.5. DESCRIPCION DE LA ALTERNATIVA SELECCIONADA

Creación del nuevo cargo para el área de Ciberseguridad para la empresa Labcoresoft S.A.S.

La creación del cargo Coordinador de Ciberseguridad, es fundamental para la buena gestión del proceso o área de ciberseguridad, esto ayudaría a tener innovación en el proceso, agregando valor y logrando los objetivos para cumplir con los propósitos de la empresa.

Para este se va a realizar un cargo tipo *Organizational Process,* el cual hace referencia a un trabajo transversal para todas las áreas, es decir que no es totalmente centrado en su área, sino que tiene contacto con todas las otras áreas de la compañía, lo cual permite adaptarse y tener un conocimiento de los demás cargos, permitiendo desarrollar pensamientos analíticos, habilidad de resolver problemas junto con las demás dependencias, resiliencia, manejo del estrés, razonamiento y resolución de problemas entre otros.

Finalmente se generará el perfil y las funciones de este cargo como tal.

1.6. ALCANCE.

Se genera un plan de mejora relacionado directamente con uno de los ocho puntos del Diamante de la Innovación, con este se busca dar un valor agregado y brindar solución a la falencia presentada respecto a Ciberseguridad en la compañía, realizando una creación de cargo de manera transversal el cual se comunique directamente con las demás áreas de la compañía logrando un mejor funcionamiento del mismo y un valor agregado a la organización.

1.7. JUSTIFICACIÓN.

Actualmente Colombia es uno de los países con mayor vulnerabilidad en temas de ciberseguridad, debido a que las empresas no toman con seriedad esta problemática, afectando directamente la innovación de las compañías en el mercado, como lo es el caso de Labcoresoft S.A.S., la cual presento un problema de *backup* de la información con un cliente en específico, afectando al este hospital debido a que gracias al virus que logro ingresar al sistema del mismo imposibilito la toma de información de los pacientes de manera digital y toda esta recolección de datos se tuvo que generar de manera física y manual, provocando así demoras en la entrega de los resultados de los diferentes pacientes, lo cual puede afectar de manera significativa la salud de los mismos, impidiendo tomar medidas a tiempo de algunas enfermedades que se puedan descubrir con dichos exámenes.

Este inconveniente puso en riesgo de manera directa a la compañía de forma económica, legal y reputacional, debido a que no se manejaba un respaldo de información, lo cual claramente podría generar demandas por parte del Hospital a Labcoresoft S.A.S., pero gracias a un tiempo de trabajo el cual claramente no fue compensado económicamente por la entidad afectada se logró recuperar información, brindando una solución al cliente después de tres días de trabajo dedicados 100% a este inconveniente.

Después de este suceso se implemento un modelo de almacenamiento en la nube el cual guarda información diariamente, permitiendo tener un *backup* por si algo vuelve a fallar, este servicio se contrato con un operador el cual genera un cobro mensual de $ 599.000 COP, pero es preferible este gasto mensual a una demanda de millones la cual pueda llevar a la bancarrota a la compañía.

Por todo lo anteriormente mencionado vemos que es importante generar medidas ante posibles problemas de ciberseguridad, esto también permite aplicar la innovación y que la empresa tenga una ventaja competitiva en el sector.

1.8. OBJETIVOS

Objetivo General.

Revisar los principales escenarios de riesgo para la empresa Labcoresoft S.A.S. desde su estructura de ciberseguridad y su impacto en la innovación.

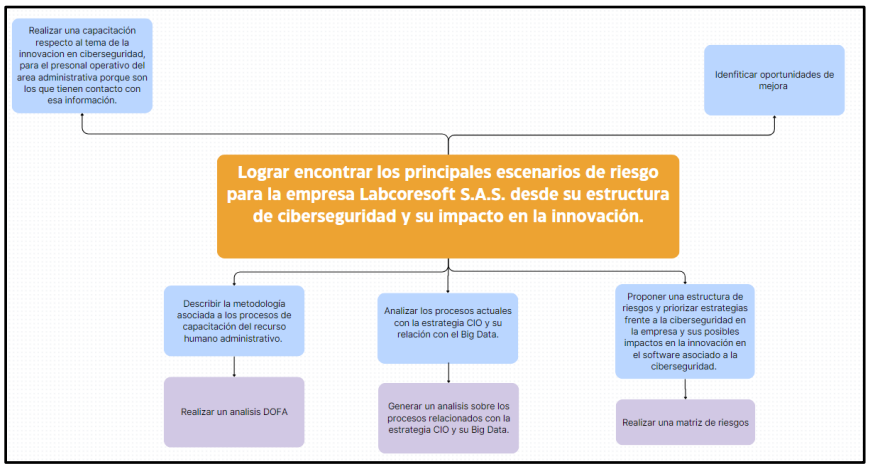
Objetivos Específicos.

1. Describir la metodología asociada a los procesos de capacitación del recurso humano administrativo.
2. Analizar los procesos actuales con la estrategia CIO y su relación con el Big Data.
3. Proponer una estructura de riesgos y priorizar estrategias frente a la ciberseguridad en la empresa y sus posibles impactos en la innovación en el software asociado a la ciberseguridad.

Árbol de objetivos

Figura 9.

Árbol de objetivos:



Nota. El grafico muestra el árbol de objetivos para la empresa Labcoresoft S.A.S. Fuente: Hecho por la autoría, según datos tomados de: La Empresa Labcoresoft S.A.S.

2. MARCO CONCEPTUAL.

En el marco conceptual se manejarán los siguientes conceptos: Diamante de la Innovación, riesgo, ciberseguridad, virus informático, ciberataque.

Estos puntos se relacionan con el análisis que se quiere lograr en ámbitos del Diamante de la Innovación de la ciberseguridad, como la falta de este puede llegar a afectar su innovación no solo poniendo en riesgo a la compañía, sino la información sensible y que se debe salvaguardar de una manera adecuada para que no se presenten plagios, reprocesos en los diferentes por no resguardar de manera adecuada su *Big Data*.

El artículo de reflexión, como indica en la página de Colciencias, (2010) “presenta resultados de investigación terminada desde una perspectiva analítica, interpretativa o crítica del autor, sobre un tema específico, recurriendo a fuentes originales.” (Pág. 9). Para su desarrollo será necesario evaluar los principales escenarios de riesgo para la empresa, desde su estructura de ciberseguridad y su imparto en la innovación.

Como se mencionaba anteriormente se manejara uno de los ocho puntos del Diamante de la innovación, como lo nombra Ojeda, F. (2019) “que: La Innovación de una estructura empresarial, de un país, ciudad, sector, región, depende principalmente de: Competitividad, Grado de Apertura de la Economía, su aporte al PIB, Nivel de Educación, Número de Ingenieros − año, Número de patentes año, Ciberseguridad y Corrupción, donde cualquier proceso resultante minimiza el impacto ambiental” (Pag 50, parr 4)

Centrándose particularmente en la relación con el Diamante de la Innovación con la Ciberseguridad, según lo menciona Ojeda, F. (2019) “Índice de Ciberseguridad Global (GCI). En la sociedad de la información y el Big data corporativo, el respeto por el uso e implantación de los sistemas de recogida de datos es determinante, generando un entorno de confianza hacia la empresa y el entorno tecnológico que la rodea. Su Indicador, la Ciberseguridad Global para este punto del Diamante, es emanado de Naciones Unidas y su organismo encargado de las Telecomunicaciones, Unión Internacional de Telecomunicaciones o ITU (ITU, *International Telecomunications Union*).” (Pag 51, parr 5)

Se busca analizar los impactos de innovación, como dice Ojeda. F. (2019) “donde esta clave ciberseguridad-innovación es indivisible como factor determinante no solo en económico-social, sino también en las relaciones. Internacional, Oeste-Este, de las próximas décadas” (Pag 98, parr 8). Luego de tener las tres matrices (POAM, PCI Y DOFA), se genera un análisis y se realiza la matriz de riesgos para identificar los posibles riesgos que pueden llegar a afectar en temas de innovación y por falta de la ciberseguridad en la empresa.

Se pretende realizar un artículo de reflexión sobre la ciberseguridad, como dice Anchundia, C (2017) “Existe una tendencia en la ciberseguridad en el mundo actual de masificación e hiperconectividad a nivel mundial que hace que cada dispositivo represente un nuevo blanco de ataques para los ciberdelincuentes, si no se conocen las medidas necesarias para prevenirlos (Vallés, 2016). En general, se podría decir que la Ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (Leyva, 2015)”. (Pag, 204, parr 3).

Asimismo, se busca revisar los procesos que relaciona con la estrategia CIO y la conexión con su Big Data, Según la página web de Gartner, (2012) Big Data es “son activos de información de gran volumen, alta velocidad y/o gran variedad que exigen formas innovadoras y rentables de procesamiento de información que permitan mejorar el conocimiento, la toma de decisiones y la automatización de procesos.” (Parr 1).

También se construirá una estructura de riesgos, como dice Chávez. S, (2018) “el diccionario de la Real Academia Española (1992), define peligro como: 1) riesgo o contingencia inminente de que suceda algún

mal; 2) Lugar, paso, obstáculo o situación en que aumenta la inminencia del daño; por lo que los términos riesgo y peligro, en el idioma español son y se emplean como sinónimos. Luhmann (1996), refiere que esta situación es de tipo lingüístico ya que en inglés las palabras *risk, hazard, danger*, en general se utilizan en el mismo sentido. Situaciones parecidas ocurren con el término desastre y catástrofe, ya que para autores como Aneas (2000), son sinónimos, mientras que para otros como Soldano (2009) y López (2004), tienen significado diferente; o bien los términos peligro y amenaza que, de acuerdo al diccionario de la Real Academia Española, tienen significado diferente, y autores como, Coburnetal., (1991); y Cardona (1993) los emplean como sinónimos." (Pag 46, parr 1). Para realizar esta estructura o matriz de riesgo es necesario generar anteriormente un cronograma de actividades junto con dos matrices adicionales, las cuales son la matriz POAM y la matriz PCI.

En el cronograma de actividades se manejará el Diagrama de Gantt, como nombra Handl. K (2014), "El diagrama de Gantt es una herramienta que se emplea para planificar y programar tareas a lo largo de un período determinado de tiempo. Gracias a una fácil y cómoda visualización de las acciones a realizar, permite realizar el seguimiento y control del progreso de cada una de las etapas de un proyecto. Reproduce gráficamente las tareas, su duración y secuencia, además del calendario general del proyecto y la fecha de finalización prevista. Es una útil herramienta gráfica cuyo objetivo es exponer el tiempo de dedicación previsto para diferentes tareas o actividades a lo largo de un tiempo total determinado. Fue Henry Laurence Gantt quien, entre 1910 y 1915, desarrolló y popularizó este tipo de diagrama en Occidente. Desde su introducción los diagramas de Gantt se han convertido en una herramienta básica en la gestión de proyectos de todo tipo, con la finalidad de representar las diferentes fases, tareas y actividades programadas como parte de un proyecto o para mostrar una línea de tiempo en las diferentes actividades haciendo el método más eficiente" (Pag 3 – 4). Con ayuda de este diagrama se definirán los diferentes tiempos para la realización de las tareas y cumplimiento de las matrices a trabajar.

La matriz POAM, como indica Belloso. R (2018), "el formato del perfil de oportunidades y amenazas del medio (POAM), el cual según Serna (2010; p.150), está definido como "la metodología que permite identificar y valorar las oportunidades y amenazas potenciales de una empresa". Es importante resaltar que dependiendo de su impacto o importancia un grupo puede determinar si un factor dado es considerado una oportunidad o una amenaza." (Pag 55, par 3). Gracias a esta herramienta se podrá llevar a cabo el análisis de las oportunidades y amenazas en la empresa, generar un análisis más detallado de los diferentes componentes que afectan a la compañía de manera externa.

Mientras tanto la matriz PCI, como lo dice Viajan. J. (2016) "El perfil de capacidad interna (PCI) es un medio para evaluar las fortalezas y debilidades de la empresa en relación con las oportunidades y amenazas que les presenta el medio externo. Es una manera adecuada de realizar un diagnóstico involucrando cada uno de los factores que afectan su operación organizacional (Serna, 2008, p.167). El PCI examina cinco categorías; capacidad directiva, capacidad competitiva (o de mercado), capacidad financiera, capacidad tecnológica y capacidad del talento humano (Serna 2008, p.169)" (Pag 51). Esta matriz ayudara a validar las fortalezas y debilidades que tiene la empresa de manera interna, así con estas dos matrices se puede llegar a desarrollar la matriz DOFA y luego pasar a la matriz de riesgos.

Con estas dos últimas matrices se genera el DOFA, como nombra Villaroel, M. “La matriz de: amenazas, oportunidades, debilidades y fortalezas mejor conocida como matriz (DOFA), es un instrumento de ajuste importante que ayuda a los líderes a desarrollar cuatro tipos de estrategias: estrategias de fortalezas y debilidades, estrategias de debilidades y oportunidades, estrategias de fortalezas y amenazas, estrategias de debilidades y amenazas. Observar los factores internos y externos clave es la parte más exigente para desarrollar una matriz DOFA y requiere juicios sólidos, además de que no existe una serie mejor de adaptaciones. Según Fred, R. (2003) es factible diferenciar estas estrategias unas de otras, para Fred, R. (2003) las estrategias FO usan las fuerzas internas de la organización para aprovechar la ventaja de las oportunidades externas. Todos los líderes buscan organizaciones en una posición tal que puedan usar las fuerzas internas para aprovechar las tendencias y los hechos externos. Por regla general, las organizaciones siguen a las estrategias de DO, FA o DA para colocarse en una situación donde puedan aplicar estrategias FO. Cuando una organización tiene debilidades importantes, luchará por superarlas y convertirlas en fortalezas. Cuando una organización enfrenta amenazas importantes, tratará de evitarlas para concentrarse en las oportunidades.” (Pag 80, parr 3), finalmente se generaría la matriz de riesgos.

3. METODOLOGIA

3.1. Desarrollo De Metodología Asociada A Los Procesos De Capacitación Del Recurso Humano Administrativo

Actualmente la empresa Labcoresoft S.A.S. maneja una plataforma llamada E-Learning, esta se creó para entrenar a los usuarios *Labcore* ya fueran clientes internos (hace referencia a los colaboradores) o externos, esta fue desarrollada para reducir la mano de obra al momento de dar las capacitaciones al usuario y reducir los tiempos, logística para capacitar a un grupo específico de usuarios y se ejecutó en una plataforma llamada Moodle,

Para el desarrollo de este se definieron los temas a tratar dentro de cada módulo y se definieron los parámetros de grabación, se grabaron y subieron los videos a la plataforma, teniendo en cuenta que después de que cada usuario finaliza el curso se genera un certificado del mismo.

3.2. Desarrollo de procesos estratégicos del CIO y su relación con el Big Data.

En este caso se evidencia que no se cuentan con procesos estratégicos por parte del CIO relacionados con el BigData, ya que en el mes de septiembre de 2023 se generó un inconveniente con uno de los hospitales con el que tiene contrato la compañía, este tuvo un ciberataque en el cual fue violentada toda la información, lo cual provoco una pausa y atraso en las diferentes labores del hospital, ya que el personal no tenía acceso a la información de los pacientes, como datos o historias clínicas, en el tema de ingresos y toma de muestras de laboratorio todo se generaba de manera manual, en este momento la empresa Labcoresoft estaba el riesgo de una demanda debido a que no tenía una copia de toda la información y del sistema Labcore para dicho hospital, por lo cual se tuvo que generar la creación de todo absolutamente desde cero, lo cual produjo perdida en la empresa porque fue una semana en la cual se detuvieron a realizar nuevamente un sistema para un hospital, este tiempo se pudo emplear para un nuevo proyecto del cual estuvieran generando

ganancias, pero en este caso no fue así, porque se presenta una pausa en los demás proyectos, perdiendo dinero y tiempo.

Después de este inconveniente la empresa decidió contratar un servicio de Claro Cloud, en el cual se puede salvaguardar la información con un costo de $ 599.900, para este se generó una capacitación la cual se brindó a los ingenieros encargados de salvaguardar esta información para su buen manejo.

Con lo anterior se puede evidenciar que al no existir un mecanismo o sistema para salvaguardar la información se puede presentar varios problemas, generar daños no solo a la empresa si no a las diferentes personas, ya que se está hablando de temas de la salud y en un hospital que tiene tanto flujo como el Hospital de la Misericordia, por eso se contrata este servicio para generar una reducción de riesgo en estos casos tan alto como el mencionado anteriormente.

4. ENCUENTRO CON LOS OBJETIVOS ESPECIFICOS

En este punto se desarrollará la parte metodológica la cual permitirá validar las falencias presentadas en el ámbito de ciberseguridad, como este puede afectar directamente la innovación en la empresa y sus posibles soluciones.

4.1. Matriz POAM

Primero se desarrolló la matriz POAM: La cual permite identificar y valorar las amenazas y oportunidades de la empresa de manera externa relacionadas con la ciberseguridad.

Tabla 1.

Valoración de la Matriz POAM de la empresa Labcoresoft S.A.S.

TABLA DE VALORACIÓN DE LA EMPRESA LABCORESOFT S.A.S.		
ALTO	3	PRIORIDAD MAXIMA
MEDIO	3	PRIORIDAD ALTA
MEDIO	2	PRIORIDAD MEDIA
BAJO	1	PRIORIDAD BAJA

Nota: Esta tabla muestra la valoración de la Matriz POAM para la empresa Labcoresoft S.A.S. Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Seguimiento de Matriz POAM

Tabla 2.

Seguimiento de Matriz POAM: factores económicos.

PERFIL DE LAS AMENAZAS Y OPORTUNIDADES				
FACTORES ECONÓMICOS	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Tasa de interés	Bajo	1	Medio	2
Inflación	Medio	2	Bajo	1
Tipos de Cambio	Medio	2	Medio	1
Precios	Medio	2	Bajo	1
Nivel de deuda	Bajo	1	Medio	2

PERFIL DE LAS AMENAZAS Y OPORTUNIDADES				
FACTORES ECONÓMICOS	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Consumo	Medio	2	Bajo	1
Inversión	Medio	2	Bajo	1
Demanda	Medio	2	Bajo	1
Recesión	Bajo	1	Medio	2
Riesgo País	Bajo	1	Medio	2
	suma	16	suma	14
	promedio	1,6	promedio	1,4

Como resultado se puede observar que en los factores económicos están en niveles bajos y medios respecto a la innovación de la ciberseguridad, lo cual no es tan relevante en este punto del diamante de la innovación.

Nota: Esta tabla muestra el seguimiento de los factores económicos de la Matriz POAM para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Tabla 3.

Seguimiento de Matriz POAM: factores sociales.

PERFIL DE LAS AMENAZAS Y OPORTUNIDADES				
FACTORES SOCIALES	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Orden Publico	Bajo	1	Medio	2
Seguridad	Bajo	1	Alta	3
Desempleo	Bajo	1	Bajo	1
Desplazamiento	Medio	2	Medio	2
Grupos Armados	Bajo	1	Medio	2
	suma	6	suma	10
	promedio	1,2	promedio	2

En los factores sociales se evidencia que la amenaza más alta está en la seguridad, la cual es importante en el punto del Diamante de la innovación respecto a la ciberseguridad, ya que con la falta de esta seguridad se puede violentar la ciberseguridad de la empresa

Nota: Esta tabla muestra el seguimiento de los factores sociales de la Matriz POAM para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Tabla 4.

Seguimiento de Matriz POAM: factores tecnológicos.

PERFIL DE LAS AMENAZAS Y OPORTUNIDADES				
FACTORES TECNOLÓGICOS	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Innovación	Alta	3	Bajo	2
Automatización	Medio	2	Medio	2
Ciberseguridad	Bajo	1	Alta	3
Inteligenciar artificial	Medio	2	Bajo	1
Nuevas soluciones digitales	Alta	3	Medio	2
Telecomunicaciones	Alta	3	Bajo	1
	suma	14	suma	11
	promedio	2,33333333	promedio	1,83333333

Respecto a los factores tecnológicos, se observa que la innovación, nuevas soluciones digitales y las telecomunicaciones son oportunidades altas, mientras que la ciberseguridad es una amenaza alta, ya que no se implementa en la compañía.

Nota: Esta tabla muestra el seguimiento de los factores tecnológicos de la Matriz POAM para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Matriz PCI

Segundo se realiza la matriz PCI: La cual permite identificar y valorar las fortalezas y debilidades de la empresa de manera externa relacionadas con la ciberseguridad.

Tabla 5.

Valoración de la Matriz PCI de la empresa Labcoresoft S.A.S.

TABLA DE VALORACIÓN DE LA EMPRESA LABCORESOFT S.A.S.		
ALTO	3	PRIORIDAD MAXIMA
MEDIO	2	PRIORIDAD MEDIA
BAJO	1	PRIORIDAD BAJA

Nota: Esta tabla muestra la valoración de la Matriz PCI para la empresa Labcoresoft S.A.S. Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Table 6.

Seguimiento de Matriz PCI: capacidad tecnológica.

PERFIL DE CAPACIDAD INTERNA				
CAPACIDAD TECNOLOGICA	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Habilidad del uso de tecnología	Alto	3	Bajo	2
Capacidad de Innovación	Medio	2	Bajo	2
Nivel de tecnología	Alto	3	Bajo	2
Fuerza de patentes y procesos	Medio	2	Bajo	2
Aplicación de tecnología a los computadores.	Medio	2	Bajo	2
	suma	12	suma	10
	promedio	2,4	promedio	2

Respecto a la capacidad de tecnología la empresa se encuentra en oportunidades en: Habilidad del uso de tecnología y nivel de tecnología, respecto a las amenazas todas son bajas.

Nota: Esta tabla muestra el seguimiento de la capacidad tecnológica de la Matriz PCI para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Table 7.

Seguimiento de Matriz PCI: capacidad directiva.

PERFIL DE CAPACIDAD INTERNA				
CAPACIDAD DIRECTIVA	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Comunicación	Medio	2	Medio	2
Control Gerencial	Medio	2	Medio	2
Habilidad para captar y retener personal creativo	Bajo	1	Medio	2
Velocidad de respuesta a condiciones de cambio	Medio	2	Medio	2
Conocimiento y experiencia en el mercado	Medio	2	Bajo	1
	suma	9	suma	9
	promedio	1,8	promedio	1,8

Si observamos la capacidad directiva las oportunidades y amenazas son medias y bajas respecto a la innovación de la ciberseguridad.

Nota: Esta tabla muestra el seguimiento de la capacidad directiva de la Matriz PCI para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Table 8.

Seguimiento de Matriz PCI: capacidad talento humano.

PERFIL DE CAPACIDAD INTERNA				
CAPACIDAD DEL TALENTO HUMANO	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Nivel Académico	Medio	2	Bajo	2
Experiencia	Medio	2	Bajo	2
Estabilidad	Medio	2	Bajo	2
Rotación	Bajo	1	Medio	2
Ausentismo	Medio	2	Bajo	1
Motivación	Bajo	1	Medio	2
Nivel de remuneración	Medio	2	Bajo	2
Accidentalidad	Bajo	1	Medio	2
	suma	13	suma	15
	promedio	1,625	promedio	1,875

En la capacidad de talento humano las oportunidades y amenazas son medias y bajas respecto a la innovación de la ciberseguridad.

Nota: Esta tabla muestra el seguimiento de la capacidad talento humano de la Matriz PCI para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Table 9.

Seguimiento de Matriz PCI: capacidad talento financiera.

PERFIL DE CAPACIDAD INTERNA				
CAPACIDAD FINANCIERA	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Acceso a Capital	Medio	2	Bajo	2
Capacidad de Endeudamiento	Medio	2	Bajo	2
Rentabilidad, retorno de inversión	Medio	2	Bajo	2
Liquidez, disponibilidad de fondos internos.	Medio	2	Bajo	2
Elasticidad de la demanda con respecto a los precios.	Medio	2	Bajo	2
	suma	10	suma	10
	promedio	2	promedio	2

En la capacidad financiera, las oportunidades y amenazas son medias y bajas respecto a la innovación de la ciberseguridad.

Nota: Esta tabla muestra el seguimiento de la capacidad financiera de la Matriz PCI para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Table 10.

Seguimiento de Matriz PCI: capacidad talento competitiva.

PERFIL DE CAPACIDAD INTERNA				
CAPACIDAD COMPETITIVA	OPORTUNIDADES		AMENAZAS	
	NIVEL	Puntos	NIVEL	Puntos
Productos Ofrecidos	Medio	2	Medio	2
Concentración de consumidores	Medio	2	Medio	2
Concentración de Proveedores	Medio	2	Bajo	1
Diferencia Competitiva	Medio	2	Bajo	1
Diferencia Comparativa	Medio	2	Bajo	1
Administración de clientes	Medio	2	Alto	3
	suma	12	suma	10
	promedio	2	promedio	1,66666667

Por último, en la capacidad competitiva, las oportunidades y amenazas son medias y bajas respecto a la innovación de la ciberseguridad.

Nota: Esta tabla muestra el seguimiento de la capacidad competitiva de la Matriz PCI para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autoría Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Seguimiento de Matriz PCI

Como tercer paso se realiza el seguimiento estratégico.

Tabla 11.

Seguimiento en estrategia de calidad año 2024 - Valoración POAM

Labcoresoft S.A.S., seguimiento en estrategia de calidad año 2024 - Valoración POAM				
NIVEL	REVISION DE CALIFICACIÓN	AREA/DPTO/PERSONA	ESPACIO ASIGNADO	FECHA/HORA
A3	Implantación de acción inmediata en DOFA - ampliado	Andrés Ramírez - líder De Soporte	Sala de juntas	10:00 a. m.
M2	Revisión trimestral	Carlos Carrascal - Director De Proyectos	Vía meet	Correo de convocatoria una semana antes del día de la reunión, a las 9:00 am vía meet
B2	Revisión semestral	Personal operativo por área	Sala de juntas	8:00 a. m.
B3	Revisión semestral			
Margarita Quijano, coordinadora de calidad				

Metodología: quien esta a cargo de la "custodia" de la información. Seguimiento a personas -áreas que hagan uso de la información especificar quienes y bajo que situaciones deben tener acceso a la información. Registrar el uso de la información bajo un formato de "registro de uso de la información del plan de seguimiento de calidad.

Andrés Ramírez seria la persona encargada de realizar el seguimiento a el nivel a3, porque los factores que se encuentran en este nivel están relacionados con el tema de ciberseguridad, el cual sería área del líder de soporte en la compañía.
Carlos Carrascal seria la persona encargada de realizar el seguimiento a el nivel M2, porque los factores que se encuentran en este nivel pueden llegar afectar o no los proyectos que se tengan en el momento en marcha con los diferentes clientes y le correspondería directamente a el como coordinados de proyectos.
El personal operativo por área sería el encargado de realizar el seguimiento a los niveles B2 y B3, porque los factores que se encuentran en este nivel no tienen tanto impacto en el punto del diamante de la innovación específicamente en la ciberseguridad.

Nota: Esta tabla muestra el seguimiento de la estrategia POAM para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Tabla 12.

Seguimiento en estrategia de calidad año 2024 - Valoración PCI.

Labcoresoft S.A.S., seguimiento en estrategia de calidad año 2024 - Valoración PCI				
NIVEL	REVISION DE CALIFICACIÓN	AREA/DPTO/PERSONA	ESPACIO ASIGNADO	FECHA/HORA
A3	Implantación de acción inmediata en DOFA - ampliado	Andrés Ramírez - líder de soporte	Sala de juntas	10:00 a. M.
M2	Revisión trimestral	Carlos carrascal - director de proyectos	Vía meet	Correo de convocatoria una semana antes del día de la reunión, a las 9:00 am vía meet
B2	Revisión semestral	Personal operativo por área	Sala de juntas	8:00 a. M.
Margarita Quijano, coordinadora de calidad				

Metodología: quien está a cargo de la "custodia" de la información. Seguimiento a personas -áreas que hagan uso de la información especificar quienes y bajo que situaciones deben tener acceso a la información. Registrar el uso de la información bajo un formato de "registro de uso de la información del plan de seguimiento de calidad.

Andrés Ramírez seria la persona encargada de realizar el seguimiento a el nivel A3, porque los factores que se encuentran en este nivel están relacionados con el tema de ciberseguridad en la compañía, el cual sería área del líder de soporte.
Carlos Carrascal seria la persona encargada de realizar el seguimiento a el nivel m2, porque los factores que se encuentran en este nivel pueden llegar afectar o no los proyectos que se tengan en el momento en marcha dentro de la compañía y le correspondería directamente a el como coordinados de proyectos.
El personal operativo por área sería el encargado de realizar el seguimiento a los niveles B2 y B3, porque los factores que se encuentran en este nivel no tienen tanto impacto en el punto del diamante de la innovación específicamente en la ciberseguridad dentro de la empresa.

Nota: Esta tabla muestra el seguimiento de la estrategia PCI para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

4.2. DOFA

Cuarto se realiza la matriz DOFA: La cual permite identificar las debilidades, fortalezas, oportunidades y amenazas, de la empresa de manera interna y externa relacionadas con la ciberseguridad.

DOFA reducido

Aquí se puede observar un DOFA reducido ya que solo se tiene en cuenta los elementos con mayor calificación de las matrices anteriores POAM y PCI.

Tabla 13.

DOFA reducido.

DOFA - (TIPO MATRIZ PESTEL)		
Internos	FORTALEZAS	DEBILIDADES
	- Habilidad del uso de tecnología - Nivel de tecnología	- Administración de clientes
Externos	OPORTUNIDADES	AMENZAS
	- Innovación - Telecomunicaciones - Nuevas soluciones digitales	- Seguridad - Ciberseguridad

Nota: Esta tabla muestra la Matriz DOFA para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

DOFA Ampliado

La matriz de DOFA ampliado permite identificar las debilidades, fortalezas, oportunidades y amenazas, de la empresa de manera interna y externa relacionadas con la ciberseguridad, de una manera mas especifica.

Tabla 14.

DOFA ampliado.

FACTOR	DEBILIDADES	OPORTUNIDADES	FORTALEZAS	AMENAZAS	ESTRATEGIA ¿Qué?
PCI - Habilidad del uso de tecnología			X		Capacitación
PCI - Nivel de tecnología			X		Convención
PCI - Administración de clientes	X				Implementación de seguridad
POAM - Innovación		X			Proyectos
POAM - Telecomunicaciones		X			Capacitación
POAM - Nuevas soluciones digitales		X			Proyectos
POAM - Seguridad				X	Capacitación
POAM - Ciberseguridad				X	Implementación de seguridad

Nota: Esta tabla muestra la Matriz DOFA ampliado para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Tabla 15.

DOFA ampliado 2.

FACTOR	ESTRATEGIA ¿Qué?	¿Cómo?	¿Quién?	¿Cuándo?	¿Cuánto? - Valorado en COP a precios de octubre 2023	Total - Valorado en COP a precios de octubre 2023
PCI - Habilidad del uso de tecnología	Capacitación sobre el uso de la tecnología.	Se generarían capacitaciones para potenciar la habilidad del uso de la tecnología que actualmente se maneja en la empresa Labcoresoft S.A.S.	Ingeniero - Área de Implementación - Jhon Galeano	01 de Enero de 2024 al 01 de febrero de 2024 - Los días viernes de 3:00 pm a 5:00 pm - (Clase virtual)	$ 150.000 por hora al ingeniero Jhon Galeano - Total 8 horas	$ 1.200.000
PCI - Nivel de tecnología	Convención sobre las nuevas tecnologías.	Se asistiría a una convención relacionada con los nuevos niveles de tecnología que se pueden manejar en las empresas.	Juan Avendaño - Ingeniero Electrónico	02 noviembre 2023 - 04 noviembre 2023 - 8 horas diarias de 8:00 am a 5 pm con una hora de almuerzo	$ 130.000 por hora - Total 24 horas - Transporte ida y vuelta $ 500.000 diario (3 días)	$ 4.620.000

FACTOR	ESTRATEGIA ¿Qué?	¿Cómo?	¿Quién?	¿Cuándo?	¿Cuánto? - Valorado en COP a precios de octubre 2023	Total - Valorado en COP a precios de octubre 2023
PCI - Administración de clientes	Implementación de seguridad	Se generará una implementación de seguridad para el manejo de la información de los clientes	Ingeniero de Ciberseguridad - Julián Ríos	01 de Diciembre 2023 - 31 de diciembre de 2023 - De lunes a viernes - 8:00 pm a 5:00 pm con una hora de almuerzo - Total de horas diarias 8 - Total de días hábiles 19	$ 170.000 por hora (8 horas por 19 días hábiles – Alquiler del lugar por un mes $ 1.700.000.)	$ 27.540.000
POAM - Innovación	Implementación de ciberseguridad en la data de los clientes.	Se generará una implementación de seguridad para el manejo de la información de los clientes	Dirección de Proyectos	2 de febrero al 31 de marzo de 2024 - De lunes a viernes - 8:00 pm a 5:00 pm con una hora de almuerzo - Total de horas diarias 8 - Total de días hábiles 20	$ 130.000 por hora al señor Carlos Carrascal, director de proyectos.	$ 20.800.000

FACTOR	ESTRATEGIA ¿Qué?	¿Cómo?	¿Quién?	¿Cuándo?	¿Cuánto? - Valorado en COP a precios de octubre 2023	Total - Valorado en COP a precios de octubre 2023
POAM - Telecomunicaciones	Diplomado de Tópicos en telecomunicaciones	Se tomará un Diplomado Tópicos avanzados en sistemas de telecomunicaciones	Universidad Católica	01 de abril al 30 de abril de 2023 - 84 horas - Viernes 6:00 p.m. a 10:00 p.m. Y sábados 8:00 a.m. a 5:00 p.m.	$ 2.100.000 COP por cada persona - Total de lideres 6	$ 12.600.000
POAM - Nuevas soluciones digitales	Diplomado de transformación digital.	Se asistiría a una convención relacionada con las nuevas soluciones digitales que se pueden manejar	Diplomado en Transformación Digital	01 de junio al 15 de agosto de 2023 - 10 semanas (96 horas)	$ 3.380.000 COP por persona - Total de lideres 6	$ 20.280.000
POAM - Seguridad	Capacitación sobre la normatividad ISO 27001	Se realizará un Diplomado de Seguridad de la Información Estándar ISO 27001	Universidad Distrital	01 septiembre al 30 de septiembre de 2023 - Lunes, Miércoles y Viernes de 6pm a 10pm	$ 2.100.000 COP por cada persona - Total de lideres 6	$ 12.600.000
POAM - Ciberseguridad	Implementación de seguridad	Contratar servicios con una empresa de consultoría de ciberseguridad	Arus - Consultoría	01 de enero de 2024	$ 4.000.000 COP mensuales - Total de lideres 6	$ 24.000.000

Nota: Esta tabla muestra la Matriz DOFA ampliado 2 para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Información obtenida de:

- *Diplomado Tópicos avanzados en sistemas de telecomunicaciones*. (2023, September 14). Universidad Católica De Colombia. https://www.ucatolica.edu.co/portal/Educacion_Continuada/diplomado-topicos-avanzados-en-sistemas-de-telecomunicaciones/
- *ARUS*. (n.d.). Com.co. Retrieved November 25, 2023, from https://www.arus.com.co/

4.3. Matriz de Riesgos

Por último, se maneja un borrador de la Matriz de Riesgo para evaluar y medir los posibles riesgos que se pueden presentar en temas de ciberseguridad y lo cual puede afectar directamente la innovación:

Tabla 16.

Matriz de Riesgo Consecuencia y Probabilidad

		MATRIZ DE RIESGO				
		CONSECUENCIA				
		Improbable	**Posible**	**Ocasional**	**Probable**	**Frecuente**
PROBABILIDAD		**1**	**2**	**4**	**8**	**16**
Catastrófico	**5**	5	10	20	40	80
Mayor	**4**	4	8	16	32	64
Moderado	**3**	3	6	12	24	48
Menor	**2**	2	4	8	16	32
Insignificante	**1**	1	2	4	8	16

Nota: Esta tabla muestra la Matriz de Riesgo Consecuencia y Probabilidad para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Tabla 17.

Matriz de Riesgo – Nivel de Riesgo.

NIVEL DE RIESGO	**COLOR**
Riesgo Aceptable	
Riesgo Tolerable	
Riesgo Alto	
Riesgo Extremo	

Nota: Esta tabla muestra la Matriz de Riesgo – Nivel de Riesgo para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Tabla 18.

Matriz de Riesgo – Eventos

EVENTO	PROBABILIDAD	CONSECUENCIA	NIVEL DE RIESGO
PCI - Habilidad del uso de tecnología	Menor	Posible	Riesgo Aceptable
PCI - Nivel de tecnología	Moderado	Posible	Riesgo Aceptable
PCI - Administración de clientes	Mayor	Ocasional	Riesgo Alto
POAM - Innovación	Moderado	Posible	Riesgos Tolerable
POAM - Telecomunicacione	Moderado	Posible	Riesgos Tolerable
POAM - Nuevas soluciones digitales	Menor	Posible	Riesgo Aceptable
POAM - Seguridad	Mayor	Ocasional	Riesgo Alto
POAM - Ciberseguridad	Mayor	Probable	Riesgo Extremo

Nota: Esta tabla muestra la Matriz de Riesgo – Eventos para la empresa Labcoresoft S.A.S., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023

Es esta Matriz se Riesgos se evidencia y confirma las prioridades del DOFA, el riesgo más elevado en el tema de la administración de clientes, la seguridad y la ciberseguridad, lo cual nos indica que son eventos los cuales se deben entrar a trabajar, para lo cual es realmente importante generar una creación de área relacionada directamente con esta falencia es decir la Ciberseguridad.

Creación del nuevo cargo

Teniendo en cuenta todo lo anteriormente mencionado se debe generar un plan de mejora en el cual se implemente la creación de un nuevo cargo responsable del buen funcionamiento del área de Ciberseguridad, este incluirá el ciclo PHVA, acciones de mejoramiento, personal responsable a ejecutar y verificar las acciones respectivas, tiempos establecidos junto con el seguimiento del responsable.

Ciclo PHVA

Tabla 19.

Explicación del siglo PHVA

Ciclo de Deming	
1. Planificar	**2. Hacer**
Se establecen los objetivos y los procesos necesarios para lograr los resultados, de acuerdo con las políticas de la organización, junto con los indicadores de medición que serán utilizados.	Consiste en la implementación de las acciones necesarias para lograr las mejas planteadas con el objetivo de ganar en eficiencia y poder corregir errores de la ejecución.
4. Actuar	**3. Verificar**
Se valida si las verificaciones fueron exitosas o no, si en este caso es negativa la respuesta se realiza un ajuste a las acciones, para poder mejorar en el desarrollo de los procesos.	Se establece un periodo de seguimiento para mirar si se está cumpliendo todo lo planeado y realizar un informe sobre los resultados.

Nota: Esta tabla muestra la explicación del siglo PHVA., Fuente: Hecho por la autora. Basado en: Material Académico suministrado por el Profesor Fernando Ojeda – 2023.

Planificar: Entre los objetivos necesarios para cumplir el plan de mejora se incluyen:

Identificación de necesidades

- Evaluar el estado actual de la seguridad de la información en la organización.
- Identificar las amenazas y vulnerabilidades existentes.
- Determinar los recursos necesarios para establecer un área de ciberseguridad eficaz.

Establecer objetivos:

- Definir los objetivos de seguridad de la información que se desean alcanzar.
- Establecer metas específicas y medibles para mejorar la ciberseguridad de la organización.
- Priorizar los riesgos y amenazas para centrarse en los aspectos más críticos.

Planificación de actividades:

- Diseñar un plan estratégico para la creación del área de ciberseguridad.
- Establecer políticas y procedimientos de seguridad de la información.
- Seleccionar y adquirir las herramientas y tecnologías necesarias para la gestión de la ciberseguridad.
- Definir roles y responsabilidades dentro del equipo de ciberseguridad.

Hacer: Las acciones implementadas para cumplir el plan de mejora son los siguientes.

Implementación:

- Crear el área de ciberseguridad de acuerdo con el plan estratégico establecido.
- Desplegar las herramientas y tecnologías de seguridad seleccionadas.
- Capacitar al personal en buenas prácticas de seguridad de la información.

Ejecución de actividades

- Realizar auditorías de seguridad de forma regular para identificar posibles brechas o vulnerabilidades.
- Monitorear continuamente los sistemas en busca de actividad sospechosa o incidentes de seguridad.

Verificar: Para realizar la verificación del plan de mejora es necesario realizar un seguimiento el cual permite:

Evaluación de resultados

- Comparar el estado actual de la seguridad de la información con los objetivos y metas establecidos.
- Analizar los resultados de las auditorías de seguridad para identificar áreas de mejora.
- Obtener retroalimentación del personal y otros *stakeholders* sobre la eficacia del área de ciberseguridad.

Medición de indicadores:

- Establecer indicadores clave de rendimiento (KPIs) para evaluar el desempeño del área de ciberseguridad.
- Monitorizar regularmente los KPIs para identificar tendencias y tomar acciones correctivas cuando sea necesario.

Actuar: Finalmente para validar si este plan de mejora fue efectivo o no se implementan acciones derivadas a las de verificación.

Mejora continua

- Basándose en los resultados de la evaluación, identificar áreas de mejora y tomar medidas correctivas.
- Actualizar políticas, procedimientos y tecnologías de seguridad según sea necesario.
- Proporcionar formación adicional al personal para reforzar la cultura de seguridad de la información.

Adaptación

- Permanecer al tanto de las nuevas amenazas y tendencias en ciberseguridad.
- Adaptar continuamente el área de ciberseguridad para hacer frente a los cambios en el panorama de amenazas.
- Mantener un proceso de mejora continua para garantizar que la seguridad de la información siga siendo efectiva a lo largo del tiempo.

Diagrama de Gantt.

Con ayuda de esta herramienta de gestión de proyectos o procesos, se puede plasmar el periodo de tiempo en el cual se llevará a cabo el plan de mejora y los lapsos de tiempo en los que se deberán ejecutar cada tarea asignada

Tabla 20.

Diagrama de Gantt.

ACCIONES DE MEJORAMIENTO	PERSONA (S) RESPONSABLE (S) DE EJECUTAR	PERSONA (S) RESPONSABLE (S) VERIFICAR	mar-24				abr-24				may-24				jun-24				jul-24				ago-24				sept-24				oct-24				nov-24				dic-24				ene-25				feb-25			
			SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4	SEM 1	SEM 2	SEM 3	SEM 4
Identificación de necesidades	Jury Natalia Quiceno Valencia	Francy Elisa Preciado Galindo	x																																													
Establecer objetivos	Jenny Johana	Francy Elisa Preciado Galindo	x																																													
Planificación de actividades	Jury Natalia Quiceno Valencia	Francy Elisa Preciado Galindo		x																																											
Implementación	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada	Francy Elisa Preciado Galindo		x	x																																									
Ejecución de actividades	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian González	Francy Elisa Preciado Galindo			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
Evaluación de resultados	Jury Natalia Quiceno	Jorge Guillermo Estrada					x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x										
Medición de indicadores	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian González	Francy Elisa Preciado Galindo																									x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
Mejora continua	Jury Natalia Quiceno, Jorge Guillermo Estrada	Jorge Guillermo Estrada																																								x	x	x	x	x	x	x	x	x
Adaptación	Jury Natalia Quiceno	Jorge Guillermo Estrada																																								x	x	x	x	x	x	x	x	x

Nota. El gráfico muestra el diagrama de Gantt para el desarrollo de la creación del perfil de cargo para la empresa Labcoresoft S.A.S. Fuente: hecho por la autora. Según datos logrados en: https://labcoresoft.atlassian.net/wiki/spaces/~898781351/pages/913473888/ORGANIGRAMA+COLOMBIA+PDE-OC

Plan de gestión de calidad (Proceso sistema integrado de gestión)

El proceso tiene como objetivos establecer, documentar, implementar y mantener el Sistema Integrado de Gestión, a través de un trabajo en equipo, fomentando la autogestión e implementación de mecanismos de control. Esta información se salvaguardara en una intranet de que manejaría la compañía.

Este es un proceso seguimiento, evaluación y control, su responsable es Coordinador de Calidad (Responsable Satisfacción del Cliente) (Ver Anexo 1)

Perfil de cargo.

Para este cargo se debe tener en cuenta una persona que trabaje de manera transversal en la organización, es decir trabajaría estrechamente con otros departamentos, como TI, legal y recursos humanos, para garantizar la integración de la seguridad cibernética en todas las áreas de la organización. Colaborar con equipos internos y externos en la investigación de amenazas y la implementación de soluciones de seguridad. (Ver Anexo 2)

Descripción del cargo:

- El Coordinador de Ciberseguridad es responsable de liderar y coordinar todas las iniciativas relacionadas con la seguridad cibernética dentro de la organización. Este rol implica diseñar e implementar políticas de seguridad, supervisar la infraestructura de seguridad, gestionar incidentes y liderar la respuesta a amenazas cibernéticas.

Requisitos del cargo:

- Experiencia previa en roles de seguridad cibernética, preferiblemente en una posición de liderazgo.
- Conocimiento profundo de tecnologías de seguridad, estándares de la industria y regulaciones relevantes (por ejemplo, GDPR, HIPAA, ISO 27001).
- Habilidades sólidas en gestión de proyectos, resolución de problemas y toma de decisiones.
- Excelentes habilidades de comunicación y capacidad para trabajar en equipo.
- Certificaciones en seguridad cibernética, como CISSP, CISM o CISA, son altamente valoradas.
- Este perfil proporciona una descripción general de las responsabilidades y requisitos clave para el rol de Coordinador de Ciberseguridad. Dependiendo de la organización y sus necesidades específicas, pueden agregarse o ajustarse funciones adicionales

Responsabilidades:

- Desarrollar y Mantener Políticas de Seguridad: Crear y mantener políticas de seguridad cibernética que cumplan con las regulaciones y estándares relevantes. Actualizar regularmente estas políticas para abordar nuevas amenazas y vulnerabilidades.
- Gestión de la Infraestructura de Seguridad: Supervisar la implementación y el mantenimiento de herramientas y tecnologías de seguridad, como firewalls, sistemas de detección de intrusiones, antivirus, entre otros. Asegurar que la infraestructura de seguridad esté configurada correctamente y actualizada.
- Monitoreo y Detección de Amenazas: Supervisar continuamente los sistemas de seguridad para detectar posibles intrusiones, actividades maliciosas o vulnerabilidades en la red. Implementar sistemas de monitoreo de seguridad y responder rápidamente a las alertas de seguridad.
- Gestión de Incidentes: Coordinar la respuesta a incidentes de seguridad cibernética, incluida la evaluación de la situación, la contención de la amenaza, la recuperación de datos y la mitigación de futuros riesgos. Documentar y analizar incidentes para mejorar los procesos de seguridad.
- Educación y Concientización: Desarrollar programas de capacitación en seguridad cibernética para el personal, incluida la concientización sobre las mejores prácticas de seguridad y la prevención de ataques de phishing u otras amenazas. Fomentar una cultura de seguridad cibernética en toda la organización.
- Evaluación de Riesgos y Cumplimiento: Realizar evaluaciones periódicas de riesgos de seguridad cibernética y trabajar para mitigar los riesgos identificados. Garantizar el cumplimiento de las regulaciones y normativas de seguridad cibernética relevantes.

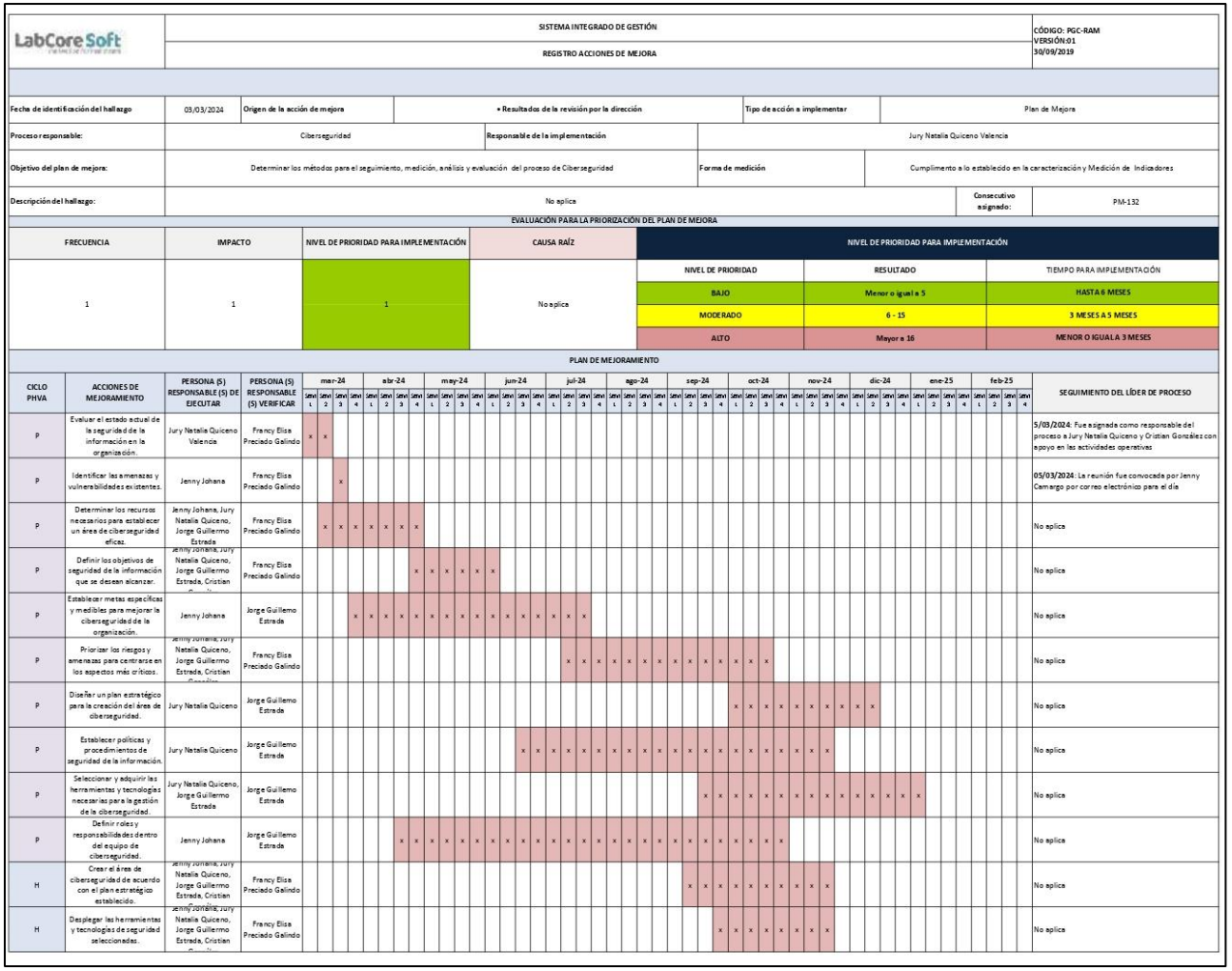
5. EVIDENCIA DEL PLAN DE MEJORAMIENTO PROPUESTO

5.1. Las matrices registradas en el trabajo – Las cuales se encuentran anteriormente graficadas desde la tabla 1 hasta la tabla 20.

5.2. Diagrama de Gantt – Tabla

5.3. El plan de mejoramiento

Anexo 1.



LabCore Soft	SISTEMA INTEGRADO DE GESTIÓN REGISTRO ACCIONES DE MEJORA	CÓDIGO: PGC-RAM VERSIÓN:01 30/09/2019

Fecha de identificación del hallazgo	03/03/2024	Origen de la acción de mejora	• Resultados de la revisión por la dirección	Tipo de acción a implementar	Plan de Mejora
Proceso responsable:	Ciberseguridad	Responsable de la implementación	Jury Natalia Quiceno Valencia		
Objetivo del plan de mejora:	Determinar los métodos para el seguimiento, medición, análisis y evaluación del proceso de Ciberseguridad	Forma de medición	Cumplimento a lo establecido en la caracterización y Medición de Indicadores		
Descripción del hallazgo:	No aplica			Consecutivo asignado:	PM-132

EVALUACIÓN PARA LA PRIORIZACIÓN DEL PLAN DE MEJORA

FRECUENCIA	IMPACTO	NIVEL DE PRIORIDAD PARA IMPLEMENTACIÓN	CAUSA RAÍZ	NIVEL DE PRIORIDAD PARA IMPLEMENTACIÓN		
				NIVEL DE PRIORIDAD	RESULTADO	TIEMPO PARA IMPLEMENTACIÓN
1	1	1	No aplica	BAJO	Menor o igual a 5	HASTA 6 MESES
				MODERADO	6 - 15	3 MESES A 5 MESES
				ALTO	Mayor a 16	MENOR O IGUAL A 3 MESES

PLAN DE MEJORAMIENTO

CICLO PHVA	ACCIONES DE MEJORAMIENTO	PERSONA (S) RESPONSABLE (S) DE EJECUTAR	PERSONA (S) RESPONSABLE (S) VERIFICAR	mar-24				abr-24				may-24				jun-24				jul-24				ago-24				sep-24				oct-24				nov-24				dic-24				ene-25				feb-25				SEGUIMIENTO DEL LÍDER DE PROCESO
				Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	
P	Evaluar el estado actual de la seguridad de la información en la organización.	Jury Natalia Quiceno Valencia	Francy Elisa Preciado Galindo	x	x																																										5/03/2024: Fue asignada como responsable del proceso a Jury Natalia Quiceno y Cristian González con apoyo en las actividades operativas
P	Identificar las amenazas y vulnerabilidades existentes.	Jenny Johana	Francy Elisa Preciado Galindo			x																																								05/03/2024: La reunión fue convocada por Jenny Camargo por correo electrónico para el día
P	Determinar los recursos necesarios para establecer un área de ciberseguridad eficaz.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada	Francy Elisa Preciado Galindo	x	x	x	x	x	x	x	x																																				No aplica
P	Definir los objetivos de seguridad de la información que se desean alcanzar.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian González	Francy Elisa Preciado Galindo							x	x	x	x	x	x																																No aplica
P	Establecer metas específicas y medibles para mejorar la ciberseguridad de la organización.	Jenny Johana	Jorge Guillermo Estrada			x	x	x	x	x	x	x	x	x	x	x	x	x	x																													No aplica
P	Priorizar los riesgos y amenazas para centrarse en los aspectos más críticos.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian González	Francy Elisa Preciado Galindo																	x	x	x	x	x	x	x	x	x	x	x	x																	No aplica
P	Diseñar un plan estratégico para la creación del área de ciberseguridad.	Jury Natalia Quiceno	Jorge Guillermo Estrada																													x	x	x	x	x	x	x	x	x	x							No aplica
P	Establecer políticas y procedimientos de seguridad de la información.	Jury Natalia Quiceno	Jorge Guillermo Estrada													x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x											No aplica
P	Seleccionar y adquirir las herramientas y tecnologías necesarias para la gestión de la ciberseguridad.	Jury Natalia Quiceno, Jorge Guillermo Estrada	Jorge Guillermo Estrada																									x	x	x	x	x	x	x	x	x	x	x	x	x	x							No aplica
P	Definir roles y responsabilidades dentro del equipo de ciberseguridad.	Jenny Johana	Jorge Guillermo Estrada						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x															No aplica
H	Crear el área de ciberseguridad de acuerdo con el plan estratégico establecido.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian González	Francy Elisa Preciado Galindo																											x	x	x	x	x	x	x	x	x										No aplica
H	Desplegar las herramientas y tecnologías de seguridad seleccionadas.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian González	Francy Elisa Preciado Galindo																													x	x	x	x	x	x	x	x	x								No aplica

H	Capacitar al personal en buenas prácticas de seguridad de la información.	Jenny Johana	Jorge Guillermo Estrada																												x	x	x	x	x	x	x	x	x	x	x											No aplica
H	Realizar auditorías de seguridad de forma regular para identificar posibles brechas o vulnerabilidades.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian	Francy Elisa Preciado Galindo							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x													No aplica
H	Monitorear continuamente los sistemas en busca de actividad sospechosa o incidentes de seguridad.	Jury Natalia Quiceno	Jorge Guillermo Estrada							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			No aplica
V	Comparar el estado actual de la seguridad de la información con los objetivos y metas	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada	Francy Elisa Preciado Galindo																								x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			No aplica
V	Analizar los resultados de las auditorías de seguridad para identificar áreas de mejora.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian	Francy Elisa Preciado Galindo																											x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			No aplica
V	Obtener retroalimentación del personal y otros stakeholders sobre la eficacia del área de	Jenny Johana	Jorge Guillermo Estrada																																x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			No aplica
V	Establecer indicadores clave de rendimiento (KPIs) para evaluar el desempeño del área de ciberseguridad.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian	Francy Elisa Preciado Galindo																																		x	x	x	x	x	x	x	x	x	x	x	x	x			No aplica
V	Monitorizar regularmente los KPIs para identificar tendencias y tomar acciones correctivas cuando sea	Jury Natalia Quiceno	Jorge Guillermo Estrada																																			x	x	x	x	x	x	x	x	x	x	x	x			No aplica
A	Basándose en los resultados de la evaluación, identificar áreas de mejora y tomar medidas correctivas.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian	Francy Elisa Preciado Galindo																																													x	x	x	x	No aplica
A	Actualizar políticas, procedimientos y tecnologías de seguridad según sea necesario	Jury Natalia Quiceno	Jorge Guillermo Estrada																																													x	x	x	x	No aplica
A	Proporcionar formación adicional al personal para reforzar la cultura de seguridad de la información.	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada	Francy Elisa Preciado Galindo																																													x	x	x	x	No aplica
A	Permanecer al tanto de las nuevas amenazas y tendencias en ciberseguridad.	Jenny Johana	Jorge Guillermo Estrada																																													x	x	x	x	No aplica
A	Adaptar continuamente el área de ciberseguridad para hacer frente a los cambios en el panorama de	Jenny Johana, Jury Natalia Quiceno, Jorge Guillermo Estrada, Cristian	Francy Elisa Preciado Galindo																																													x	x	x	x	No aplica
A	Mantener un proceso de mejora continua para garantizar que la seguridad de la información siga	Jury Natalia Quiceno	Jorge Guillermo Estrada																																													x	x	x	x	No aplica
EFICACIA		**El plan de mejora fue eficaz**	**SI**			**No Aplica**																																														
			NO																																																	

5.4. El perfil de cargo

Anexo 2.

LabCoreSoft	SISTEMA INTEGRADO DE GESTIÓN PERFIL DE CARGO	CÓDIGO: PTH-PC VERSIÓN: 06 07/03/2023
IDENTIFICACIÓN DEL CARGO		
Nombre del cargo:	Coordinador de Ciberseguridad (Responsable proceso de Ciberseguridad)	
Proceso al que pertenece	Proceso de Implementación/Proceso de Ciberseguridad	
Cargo del jefe directo:	Gerente General	
Tipo de contrato:	Indefinido	
INFORMACIÓN ESPECÍFICA DEL CARGO		
Objetivo del cargo *(Defina el propósito del cargo: el qué, en qué proceso, de acuerdo con qué marco de actuación y el para qué)*	Responsable de liderar y coordinar todas las iniciativas relacionadas con la seguridad cibernética dentro de la organización. Este rol implica diseñar e implementar políticas de seguridad, supervisar la infraestructura de seguridad, gestionar incidentes y liderar la respuesta a amenazas cibernéticas.	
NIVEL DE AUTORIDAD		
Supervisado por:	Gerente General	
Supervisa a:	No aplica	
Autoridad para:	Suplir funciones y responsabilidades del coordinador / líder.	
REQUISITOS DEL CARGO		
- Experiencia previa en roles de seguridad cibernética, preferiblemente en una posición de liderazgo.		
EXPERIENCIA LABORAL		
Años de experiencia en áreas afines al cargo	Preferiblemente 2 años de experiencia.	
FUNCIONES DEL CARGO		
Desarrollar y Mantener Políticas de Seguridad: Crear y mantener políticas de seguridad cibernética que cumplan con las regulaciones y estándares r		
Gestión de la Infraestructura de Seguridad: Supervisar la implementación y el mantenimiento de herramientas y tecnologías de seguridad, como fir		
Monitoreo y Detección de Amenazas: Supervisar continuamente los sistemas de seguridad para detectar posibles intrusiones, actividades maliciosa		
Gestión de Incidentes: Coordinar la respuesta a incidentes de seguridad cibernética, incluida la evaluación de la situación, la contención de la amen		
Educación y Concientización: Desarrollar programas de capacitación en seguridad cibernética para el personal, incluida la concientización sobre las		
Evaluación de Riesgos y Cumplimiento: Realizar evaluaciones periódicas de riesgos de seguridad cibernética y trabajar para mitigar los riesgos ident		
Colaboración Interdepartamental: Trabajar estrechamente con otros departamentos, como TI, legal y recursos humanos, para garantizar la integración de la seguridad cibernética en todas las áreas de la organización. Colaborar con equipos internos y externos en la investigación de		
RESPONSABILIDADES DEL CARGO ANTE EL SISTEMA DE SEGURIDAD Y SALUD EN EL TRABAJO		
Conocer, entender y aplicar la política de Seguridad y Salud en el Trabajo.		
Conocer los riesgos de Seguridad y Salud en el Trabajo de sus actividades y aplicar las medidas para controlarlos.		
Procurar el cuidado integral de su salud.		
Suministrar información clara, completa y veraz sobre su estado de salud.		
Cumplir las normas de Seguridad y Salud en el Trabajo y reglamentos propios de la Organización.		
Participar en la prevención de riesgos laborales mediante las actividades que se realicen en la Organización.		
Cumplir las normas internas de SST establecidas en la Organización y/o por requisito legal		
Reportar inmediatamente todo accidente de trabajo o incidente.		
Informar al Coordinador del SG-SST sobre actos o condiciones inseguras, detectadas en el lugar de trabajo.		
RESPONSABILIDADES DEL CARGO ANTE EL SISTEMA DE GESTIÓN DE CALIDAD		

Controlar los riesgos y oportunidades asociados al proceso que lidera.
Rendir cuentas a la Gerencia en relación a la eficacia del proceso (presentación de indicadores y oportunidades de mejora).
Asegurar el cumplimiento de los requisitos de las normas técnicas del Sistema Integrado de Gestión y de la normatividad legal aplicable al proceso que lidera.
Asegurar el cumplimiento de los objetivos del proceso que lidera y del Sistema Integrado de Gestión a los que se encuentra asociado.
Asegurar que el Sistema Integrado de Gestión se mantenga cuando se planifiquen e implementen cambios.
Cumplir y mantener la información documentada en la cual intervenga (procedimientos, instructivos, registros).
Asegurar que las actividades realizadas dentro del proceso, estén enfocadas al cumplimiento de los requisitos del cliente.
Presentar informes que se encuentren dentro de la naturaleza de las funciones asignadas.
Realizar control documental de acuerdo con lo establecido por el Sistema Integrado de Gestión.
Gestionar los planes de mejora asignados.
Participar activamente en las actividades programadas por el Sistema Integrado de Gestión.
Conservar y cuidar en buen estado los recursos asignados para el desarrollo del cargo.

PROGRAMA DE INDUCCIÓN Y ENTRENAMIENTO		
PROGRAMA	**TEMA**	**RESPONSABLE**
Inducción general	Bienvenida Antecedentes de la empresa Descripción de la empresa Visión Misión Valores Política del Sistema Integrado de Gestión Organigrama Presentación Corporativa	Gerente Administrativa
Reglamento Interno de Trabajo	Lectura Reglamento Interno de Trabajo	Coordinador de Calidad (Responsable de Satisfacción del Cliente)
Código de Ética y Buen Gobierno	Lectura del Código de Ética y Buen Gobierno	Coordinador de Calidad (Responsable de Satisfacción del Cliente)
Programa de Ética Empresarial y Anticorrupción	Lectura y presentación del Programa de Ética Empresarial y Anticorrupción	Coordinador de Calidad (Responsable de Satisfacción del Cliente)
Manual Buenas Prácticas Empresariales de Labcoresoft	Lectura y presentación de Buenas Prácticas Empresariales de Labcoresoft	Coordinador de Calidad (Responsable de Satisfacción del Cliente)
Protocolo de Bioseguridad para el Manejo del Covid-19 en Labcoresoft	Lectura y presentación del Protocolo de Bioseguridad para el Manejo del Covid-19 en Labcoresoft	Coordinador de Calidad (Responsable de Satisfacción del Cliente)
Información general por Proceso	Se realiza descripción de cada uno de los procesos de la empresa	Coordinadores de Proceso

Documentos asociados al cargo	Se realiza lectura de los documentos asociados al cargo de acuerdo a lo establecido por el Sistema Integrado de Gestión. * Lectura de procedimientos, caracterización del proceso, instructivos, registros y demás documentos pertinentes	Coordinador de Proceso
Divulgación perfil de cargo	Se realiza entrega del perfil de cargo al colaborador para su lectura y posterior firma	Gerente Administrativa

ACTA DE LECTURA Y ACEPTACIÓN DEL PERFIL DE CARGO Y RESPONSABILIDADES

Yo _____ identificado con documento de identidad número _____certifico que he leído, comprendido y aceptado mi perfil de cargo y las responsabilidades que por medio me han sido entregadas para su cumplimiento. Por lo anterior, firmo en señal de aceptación y compromiso, en la ciudad de _____ el _____ de _____ del _____.

_____ Firma Colaborador

_____ Firma Talento Humano

CONCLUSIONES

Según los resultados encontrados se concluye que uno de los ocho puntos del Diamante de la Innovación como lo es el de la Ciberseguridad, puede afectar directamente a las empresas, no solamente en su parte de Innovación sino en todo lo que este abarque, como su economía, reputación y parte legal. Actualmente las empresas no toman con seriedad o con importancia este tema que realmente puede traer muchas consecuencias, no solamente a las compañías, también a los datos de las personas implicadas, los diferentes clientes con los que se trabaje.

Se debe tomar conciencia de que, al no invertir de manera correcta en una infraestructura de ciberseguridad, existe la posibilidad de incurrir en gastos mucho más elevados los cuales pueden llevar a la quiebra a las diferentes organizaciones.

La empresa Labcoresoft S.A.S., debe comenzar a implementar un sistema de ciberseguridad mucho más sólido, creando un área exclusiva para este tema, pero que al mismo tiempo trabaje de manera transversal con las demás dependencias de la compañía, debido a que esta no es una responsabilidad de solo un área como tal, sino de todas las personas que laboren en la misma.

Una dificultad actual que se puede presentar en este proceso de implementación de ciberseguridad es la Gerencia General, debido a que no prestan mucho cuidado a las diferentes consecuencias que abarca una falla de este tipo, dejan a un lado todos estos posibles problemas por la inversión que se tiene que realizar en la misma. La Gerencia esta más enfocada a reunir dinero y no quieren “perder” este en algo que ellos consideran que es innecesario para la empresa.

Hace relativamente poco se presentó un problema de ciberseguridad con un virus en el Hospital de la Misericordia, en el cual se tuvo que manera aproximadamente por tres días un servicio totalmente manual por los problemas generados en el sistema por el virus, este inconveniente puso en riesgo la empresa tanto en lo legal, reputacional y económico, pero se pudo solucionar después de tres días de trabajo continuo.

Este problema hizo que se ejecutaran algunas medidas al respecto, pero de una manera muy leve, es decir que en cualquier momento se puede volver a generar algún problema adicional y la empresa aun se encuentra en decidid para suplir este tipo de contingencias, también se ha ofrecido por medio de la aseguradora SURA unas pólizas las cuales respalden este tipo de problemáticas, pero como se mencionaba anteriormente la empresa no las ha tomado porque considera que este es un riesgo mínimo.

Esta nueva área debe ir de la mano con el sistema de Calidad el cual debe ayudar a implementar los diferentes documentos, procesos, cargos, entre otros de manera transversal para que se pueda llegar a cumplir los objetivos del área de Ciberseguridad de manera correcta, tomando medidas que se acoplen a la situación actual como lo es que América Latina es uno de los más afectados en temas de ciberataques en la actualidad, sin dejar a un lado que el mercado de los Hospitales también es uno de los más perjudicados.

Si no se ejecuta de manera correcta y a tiempo medidas de ciberseguridad se puede llegar a afectar de manera directa a la empresa, el software que se maneja, adicional a esto puede poner en desventaja competitiva a la organización, generando perdidas a largo plazo, es importante proyectar esta implementación para que se pueda salvaguardar toda la información que se maneja, de lo contrario como se mencionaba anteriormente la empresa se puede ver totalmente afectada.

6. BIOBLIOGRAFIA

- Anchundia, C. (2017, 12 de enero). Ciberseguridad en los sistemas de información de las universidades. Universidad de Cuenca, Campus Central, Cuenca, Azuay. Recuperado el 01 de octubre de 2023 de: file:///C:/Users/User/Downloads/DialnetCiberseguridadEnLosSistemasDeInformacionDeLasUnive-6102849.pdf

- Blanco, H. M. (2020, 19 de febrero). Este es el costo en el que incurren las empresas al no detectar a tiempo un ciberataque. Diario La República. Recuperado el 12 de septiembre de 2023, de https://www.larepublica.co/internet-economy/este-es-el-costo-de-no-detectar-a-tiempo-un-ciberataque-3062686

- Chávez, S. (2018). El concepto de riesgo THE RISK CONCEPT. Recursos Naturales y Sociedad, 2018. Vol. 4 (1): 32-52. https://doi.org/10.18846 renaysoc.2018.04.04.01.0003. Recuperado el 01 de octubre de 2023 de: https://www.cibnor.gob.mx/revista-rns/pdfs/vol4num1/03_CONCEPTO.pdf

- Colciencias (2010) Servicio Permanente de Indexación de Revistas de Ciencia, Tecnología e Innovación Colombianas. Colombia. Recuperado de: https://minciencias.gov.co/sites/default/files/upload/paginas/M304PR02G01-guiaserviciopermanente-indexacion.pdf

- Colina, Parra, Trompiz (2018). Capitulo III – MARCO METODOLÓGICO. Universidad privada Dr Rafael Belloso Chain. Recuperado el 01 de octubre de 2023 de: https://virtual.urbe.edu/tesispub/0107187/cap03.pdf

- CRC. En 2022, Colombia alcanzó cerca de 50 millones de conexiones a Internet. (s/f). CRC. Recuperado el 23 de agosto de 2023, de: https://www.crcom.gov.co/es/noticias/comunicado-prensa/en-2022-colombia-alcanzo-cerca-50-millones-conexiones-internet.

- Díaz, LL (2023, 15 de agosto). Ciberseguridad: Colombia tuvo 5.000 millones de intentos de ataques el primer semestre . El tiempo. Recuperado el 21 de agosto del 2023 de: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/colombia-tuvo-mas-de-5-000-intentos-de-ciberataques-al-inicio-del-2023-796252.

- García L.E., & Nieto W. (2021). (Rep.). MARCO DE GOBIERNO Y GESTIÓN DE CIBERSEGURIDAD PARA CIUDADES INTELIGENTES EN EL CONTEXTO COLOMBIANO. Universidad del Norte. Recuperado el 21 de agosto del 2023 de: https://manglar.uninorte.edu.co/bitstream/handle/10584/10205/Marco%20de%20gobierno%20y%20gesti%C3%B3n%20de%20ciberseguridad%20para%20ciudades%20inteligentes%20en%20el%20contexto%20colombiano.pdf?sequence=1&isAllowed=y

- Garther (2015). Grandes datos. Gartner. Recuperado el 01 de octubre de 2023 de: https://www.gartner.com/en/information-technology/glossary/big-data

- Gil Miñano, R. (2022). (Rep.). La ciberseguridad como solución de privacidad: Especial incidencia en la privacidad desde el diseño. Universidad Internacional de La Rioja Máster Universitario en Propiedad Intelectual y Derecho de las Nuevas Tecnologías. Recuperado el 21 de agosto del 2023 de: https://reunir.unir.net/bitstream/handle/123456789/10021/Gil%20Mi%C3%B1ano%2C%20Roberto.pdf?sequence=1&isAllowed=y

- Giraldo A. & Mafla M.A. (2021). (Rep.). Propuesta metodológica para la gestión de proyectos de innovación en una empresa del sector de la construcción inmobiliaria en Colombia. Universidad Pontificia Bolivariana Bucaramanga. Recuperado el 21 de agosto del 2023 de: https://repository.upb.edu.co/bitstream/handle/20.500.11912/9622/341_1%20(1).pdf?sequence=1

- Gutierrez, A. (2022, 17 de diciembre). EPM y Afinia, entre las compañías que han sido víctimas de ciberataques. (s/f). (2022). Diario La República. Recuperado el 12 de septiembre de 2023, de https://www.larepublica.co/empresas/epm-y-afinia-entre-las-companias-que-han-sido-victimas-de-ciberataques-en-el-ano -3510742

- Handl, K. (2014). APLICACIÓN PRÁCTICA DEL DIAGRAMA DE GANTT EN LA ADMINISTRACIÓN DE UN PROYECTO. Universidad Nacional de Tucumán. Recuperado el 01 de octubre de 2023 de: https://face.unt.edu.ar/web/iadmin/wp-content/uploads/sites/2/2014/12/Aplicaci%C3%B3n-pr%C3%A1ctica-Diagrama-de-Gantt-para-Jornada-IA-Handl.pdf

- Loaiza, A. V. (2019, 27 de julio). ¿Cuánto gastan las empresas para recuperarse después de un ciberataque? Diario La República. Recuperado el 12 de septiembre de 2023, de https://www.larepublica.co/internet-economy/cuanto-gastan-las-empresas-para-recuperarse-despues-de-un-ciberataque-2889536

- Lopez, J. (2023, 11 de septiembre) Ciberataques subieron 65% siendo los bancos e industriales sus blancos más comunes. (s/f). Diario La República. Recuperado el 12 de septiembre de 2023, de: https://www.larepublica.co/empresas/reporte-ciberseguridad-2023-a-empresas-y-sectores-3701737

- Ministra de las TIC.(2022, 11 de junio). Ciudades capitales cuentan con 5,4 millones de accesos fijos a Internet. (s/f). MINTIC Colombia. Recuperado el 23 de agosto de 2023, de https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/237029:Ciudades-capitales-cuentan-con-5-4-millones-de-accesos-fijos-a-Internet.

- Montezuma L.A., Gómez C., Salazar C.E. & Hurtado A.L. (2020) (Rep.). Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales. Superintencia de Industria y Comercio. Recuperado el 21 de agosto del 2023 de: https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

- Murcia, P. (2023, 17 de junio). Estos son los ciberataques más comunes en Colombia, ¿cómo proteger su información personal? Valora Analitik. Recuperado el 21 de agosto del 2023 de: https://www.valoraanalitik.com/2023/06/17/estos-son-los-ciberataques-mas-comunes-en-colombia/.

- Ojeda, F.A. (2021,31 de diciembre). (Rep.). Cybersecurity, An Axis On Which Management Innovation Must Turn In The 21st Century. Revista Socioeconomic Challanges. Volumen 5 Número 4, pp. 98-113: República de Ucrania. DOI: https://doi.org/10.21272/sec.5(4).98-113.2021. Recuperado el 21 de agosto del 2023 de: https://armgpublishing.com/journals/sec/volume-5-issue-4/article-8/

- Ojeda, F.A. (2021,31 de diciembre). (Rep.). Origin, Use and Meaning of the Innovation Diamond. Revista Socioeconomic Challanges. Volumen 5 Número 4, pp. 48-58: República de Ucrania. DOI: https://doi.org/10.21272/sec.5(4).98-113.2021. Recuperado el 02 de octubre del 2023 de: https://armgpublishing.com/journals/sec/volume-5-issue-4/article-8/

- Portafolio. (2023, 17 de mayo) ¿cómo está Colombia en conectividad y ciberseguridad? Portafolio.co. Portafolio. Recuperado el 23 de agosto de 2023, de: https://www.portafolio.co/economia/dia-de-internet-como-esta-colombia-en-conectividad-y-ciberseguridad-582974.

- Solleiro J.L., Castañón R., Guillén A.D., Hernández T.Y. & Solís N. (2022). (Rep.). Vigilancia Tecnológica en Ciberseguridad. Universidad Nacional Autónoma de México. Recuperado el 21 de agosto del 2023 de: https://www.icat.unam.mx/wp-content/uploads/2022/09/Vigilancia_Tecnologica_en_Ciberseguridad_Boletin.pdf

- Viajan, R. (2016). ELABORACIÓN DEL PLAN ESTRATÉGICO Y DISEÑO DEL CUADRO DE MANDO INTEGRAL PARA LA E.S.E CENTRO DE SALUD TOTA. Universidad pedagógica y tecnológica de Colombia administración de empresas seccional Sogamoso. Recuperado el 01 de octubre de 2023 de: https://repositorio.uptc.edu.co/bitstream/handle/001/1676/TGT367.pdf;jsessionid=576993C12883A3E519106E6762417099?sequence=1

- Villarroel, M. (2010, Julio). LINEAMIENTOS ESTRATÉGICOS DE LIDERAZGO TRANSFORMACIONAL BASADO EN LAS COMPETENCIAS GERENCIALES DIRIGIDO A

LOS VOCEROS Y VOCERAS DEL CONSEJO COMUNAL NUESTRO FUTURO UNO DEL BARRIO BELLA VISTA DE CAGUA. Universidad Nacional Experimental Politécnica de la Fuerza Armada Nacional Bolivariana. Recuperado el 02 de octubre de 2023 de: https://www.eumed.net/libros-gratis/2011d/1042/matriz_dofa.html