PROPUESTA DE MEJORAMIENTO PARA LA PARAMETRIZACIÓN DE LOS USUARIOS EN LOS APLICATIVOS DE LA EMPRESA COLOMBIANA DE COMERCIO CORBETA S.A

Autores:
MARÍA PAULA SUAREZ ALZATE

Universidad Santo Tomás de Aquino

Facultad de ingeniería de telecomunicaciones

Proyecto de Prácticas Profesionales

Bogotá D.C

2021

PROPUESTA DE MEJORAMIENTO PARA LA PARAMETRIZACIÓN DE LOS USUARIOS EN LOS APLICATIVOS DE LA EMPRESA COLOMBIANA DE COMERCIO CORBETA S.A

Autores:
MARÍA PAULA SUAREZ ALZATE (2212914)

Proyecto de Pasantía empresa Colombiana de Comercio Corbeta S.A

Dirigido por:

ING. JOHN ALEXANDER CARDOZO RAMIREZ

Universidad Santo Tomás de Aquino Facultad

de ingeniería de telecomunicacionesProyecto

de Prácticas Profesionales

Bogotá D.C

2021

Nota de aceptación

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del Jurado

_____

Firma del Jurado

26 de febrero del 2022, Bogotá, D.C

RECTOR GENERAL

Padre José Gabriel Mesa Angulo, O.P.

VICERRECTOR ADMINISTRATIVO Y FINANCIERO GENERAL

Padre Wilson Mendoza Rivera, O.P.

VICERRECTOR ACADÉMICO GENERAL

P. Eduardo Gonzáles Gil, O.P

SECRETARIA GENERAL

Ingrid Lorena Campos Vargas

SECRETARIA DE DIVISIÓN

E. C. Luz Patricia Rocha Caicedo

DECANO FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

Ingeniero Germán Macías Muñoz

Agradecimientos

En primer lugar, agradecer a mis profesores quienes me guiaron por el camino de la excelencia, la determinación y la moralidad para convertirme en una profesional íntegra capaz de lograr cada uno de los objetivos que se planteen a lo largo de mi vida tanto personal como profesional.

Un agradecimiento a la universidad Santo Tomás por brindarme la oportunidad de ser parte de esta prestigiosa facultad de ingeniería de telecomunicaciones donde se me permitió explorar cada una de sus ramas y encontrar mi vocación.

Por último, el agradecimiento más importante es para mis padres quienes me formaron como una persona capaz de desenvolverme como hija, hermana, amiga, estudiante, compañera y profesional, quienes me brindaron todo su apoyo a lo largo de mi vida y mi carrera, son mi impulso y mi motivación para ser una profesional.

Tabla de contenido

Índice De Figuras.

Índice De Tablas

Resumen Ejecutivo.

En el presente documento se establecerá una propuesta en la cual se busca realizar un estudio en el área de gestión de accesos con el fin de parametrizar los usuarios que ingresan a la compañía otorgándoles los accesos a los diferentes aplicativos, sistemas y herramientas de manera más eficiente.

Para Realizar este posible análisis se abarcará los siguientes ítems con los cuales se podrá lograr una propuesta de reingeniería, donde se describirá el flujo del proceso de gestión de acceso en la compañía Colombiana de Comercio Corbeta S.A.S con el fin de realizar un análisis detallado de los problemas, las pérdidas de información y la gestión que se realiza en el área frente a la creación, parametrización, modificación de los usuarios que ingresan o pertenecen a la compañía.

Se establecerá el gestor de identidades que maneja la compañía actualmente con el cual se realizará un breve análisis de las falencias que se encuentran día a día al momento de realizar una creación, modificación o parametrización de los usuarios, el tiempo de respuesta del gestor, las fallas que presenta al momento de replicar los accesos a los usuarios, el rendimiento y los aplicativos sobre los cuales gobierna.

Finalmente se establecerá la pérdida de información que se presenta en la base de datos, los usuarios que pueden acceder a ella, las vulnerabilidades, riesgos y cómo afecta esto en el proceso diario que realiza el área gestión de accesos con

el fin de tener una propuesta de mejora para la compañía frente a los problemas que se evidenciaron en la práctica profesional.

Introducción

En la Empresa Colombia de comercio S.A. Se ha determinado la necesidad de contar con una política para el proceso de la implementación de la automatización (RPA), Siempre han sido objeto de necesidad humana. Aunque los desafíos son morales, religiosos y legales, en este trabajo solo nos centraremos en los últimos. Desde el punto de vista legal, los desafíos incluyen responsabilidad contractual y civil fuera del contrato-responsabilidad por acciones de terceros, programas informáticos y la tecnología se puede utilizar para promover.

Por consiguiente y con una automatización de procesos, vinculación de aplicativos al gestor de identidades para incentivar a la autogestión de los usuarios dando salvaguarda de la información crítica que garantice la disponibilidad e integridad de los activos informáticos dispuestos en el centro de datos de su sede principal.

El presente documento describe las políticas de automatización de procesos, copias de preferencias de usuario a usuario, información y almacenamiento junto con los procedimientos y mecanismos para la realización de las actividades relacionadas, con el fin de apoyar a los administradores de esta información y a reducir los impactos de los riesgos generados por fallas en la prestación de servicios internos.

1. Formulación Del Problema

La empresa Colombiana de Comercio Corbeta S.A de Colombia es una compañía a nivel nacional que cuenta con un amplio portafolio en producción de consumo masivo, electrodomésticos, productos de hogar, entre otros. Además, es la encargada de los procesos sistemáticos que se llevan a cabo en centros de atención al cliente como lo son Alkosto, Ktronix y otras tiendas de venta pertenecientes a la compañía.

Específicamente en el área de arquitectura de seguridad, su proceso de gestión de acceso frente a la creación, modificación y parametrización de los usuarios en los diferentes aplicativos se realiza mediante perfiles específicos, lo que significa que ciertos procesos se deben ejecutar con anterioridad y eficiencia. Dando, así como resultado que pueda realizar el proceso mediante un tiempo predeterminado de espera para la replicación desde el gestor de automatización (AUCA) o en ocasiones volver a reintentar este proceso.

Por otro lado, se realizan tareas constantes a los usuarios de la compañía, esto con el fin de llevar un registro y parametrización completos de los aplicativos automatizados y vinculados al gestor y otros que aún no se evidencia esta asociación, al momento de realizar la consulta esta debe garantizar accesos y credenciales para las labores de las personas creadas en diferentes aplicativos. Al llegar a este punto permite dar paso a resolver las novedades como activación, el retiro o inactivación de los aplicativos a los usuarios que se encuentran de vacaciones, ausentes o finalizan el tiempo de contrato laboral. Por ende, se remite

un previo aviso y entrega de credenciales a cada uno de los gestores o jefe a cargo.

Por consiguiente y debido a la magnitud de solicitudes realizadas para cambios o parametrización de los usuarios en los diferentes aplicativos, realizando procesos de creación, consultas, modificaciones, o añadiendo información; se genera un reproceso y atraso en los procesos ya que toman un mayor tiempo de lo habitual en cumplir los parámetros o validación esto hace que los usuarios se vean obligados a reconciliar o escalar a las áreas funcionales para evidenciar posibles fallas, y nuevamente retomar la tarea que se estaba realizando. Esto afecta la disponibilidad de los datos, el desarrollo y cumplimiento de labores.

La empresa colombiana de comercio corbeta S.A actualmente cuenta con una nómina de más de 15.000 mil empleados a nivel nacional, lo que hace que el volumen de solicitudes de gestión de accesos a los diferentes sistemas, aplicativos o herramientas aumente a medida que se solicite un nuevo ingreso, la eliminación de un usuario o la modificación de funciones dentro de la compañía para los usuarios que cambian de cargo y por ende cambian de perfil, es por esto que contar con un proceso adecuado en su gestión optimiza el tiempo de calidad y satisfacción para los usuarios lo cual se ve reflejado en cada uno de los clientes de la compañía.

2. Descripción Del Problema

Actualmente en la compañía Colombiana de Comercio Corbeta S.A la nómina de empleados internos es aproximadamente de 15.000 usuarios de los cuales se reciben solicitudes diarias para realizar nuevas parametrizaciones, modificaciones o creaciones frente a los permisos de cada uno, donde se evidencian diferentes problemas sobre el proceso que se maneja en el área Gestión de Accesos los cuales son descritos a continuación.

2.1 Base de Datos

La base de datos que se maneja actualmente el área de seguridad informática es Access la cual carece de una interfaz web no publica, la base de datos es una versión 2003 por lo que no está actualizada y presenta riesgos de ataques informáticos , Los usuarios que pueden manejar esta base de datos son aproximadamente unos 20 usuarios, donde la información presentada es aproximadamente de unos 15 mil usuarios, por lo que una consulta puede requerir bastante tiendo en la ejecución de la base de datos, adicionalmente a esteconflicto no se cuenta con una información detallada para los usuarios que necesitan visualizar los permisos, los jefes de área no pueden realizar consultas sobre los usuarios a cargo acerca de los roles, permisos y aplicativos a los cuales tienen acceso, también se evidencia que la base de datos carece de un botón de actualizaciones por lo que se genera un

re proceso a la hora de una consulta o una documentación, si una persona por error ingresa a trabajar sobre el archivo original de la base de datos automáticamente genera un ejecutable en el servidor principal lo cual genera que se dañen las bases copiadas en los diferentes servidores de quienes estén consultando o modificando en ese momento.

2.2 Perfilamiento de Usuarios.

En la empresa los puntos de venta se llaman Unidades de Negocio (UN) loscuales están distribuidos por todo el territorio colombiano, donde para cada UN cuenta con un perfil específico donde varían los tipos de roles en cada uno de los aplicativos a los cuales se les genera el acceso, en esta parametrización de perfiles se evidencio que no se tiene un análisis de riesgo para la apertura de nuevos perfiles con más tipos de accesos y tampoco se informan estos nuevos perfiles a las unidades de negocio, lo cual genera más proceso para los analistas yun menor rendimiento en las tareas diarias que se presentan.

2.3 Error Humano

Un factor muy influyente en el proceso diario de la gestión de accesos para los usuarios de la compañía es la mala praxis que se puede presentar por parte delos analistas o técnicos, ya que cuando ingresa una nueva persona al área no hay manuales para entender los diferentes aplicativos ni el

manejo que se debe dar sobre cada uno de ellos por lo que al no tener claridad sobre las diferentes funcionalidades que se tienen perjudica una posible solución para los incidentes que se presentan, esto perjudica el modo de trabajo ya que el error que se puede generar para las UN en sus accesos diarios se puede retrasar o incluso perder pordemasiado tiempo donde el impacto se refleja en el usuario final, el cliente.

2.4 Gestor de Identidades

Actualmente se Maneja el sistema de autogestión de usuarios (AUCA) el cual no gobierna totalmente los aplicativos que maneja la empresa por lo cual muchas creaciones, modificaciones o eliminaciones de permisos se deben desarrollar de manera manual, para replicar cada uno de los cambios aproximadamente tiene un tiempo de respuesta de 20 a 30 minutos lo cual genera retraso para la resolución de incidentes y muchas veces no replica completamentelos accesos a los usuarios por lo cual se considera muy deficiente al no tener integrados todos los aplicativos.

3. Alcance Y Limitación

El proyecto que se prevé tener es el análisis de una posible propuesta para la mejora de la parametrización de los usuarios registrados de la compañía, con ello el levantamiento de requerimientos y la creación de prototipos para tener una base fundamental del porque la solución quese plantea es viable y cuenta con suficiente información para pensar en la implementación de esta.

Alcances

- La propuesta de mejora en los procesos estará aplicada para el área de seguridad informática.
- Enfoque primordial para el gestor de automatización.
- Lineamientos de procesos RPA y parametrización de usuarios en los aplicativos.

Limitaciones

- Se contextualiza la propuesta para solo el área de gestión de accesos.
- La propuesta es plasmada en un prototipo
- Una implementación y desarrollo de esta propuesta afecta el conocimientode los clientes frente a el proceso

4. Justificación

Este proyecto se realiza con el fin de reducir los riesgos del gestor de automatización, y mitigar la pérdida información de la base de datos, de igual manera dar una comodidad al momento de generar solicitudes y la gestión accesos de estas, obteniendo un amplio procesamiento y correcta solución en un tiempo oportuno de ellas. Además, mitigamos las vulnerabilidades de ataques electrónicos e incluso cibernéticos en cuanto a la actualización del gestor de identidad.

La empresa Colombiana De Comercio maneja información muy robusta y altamente sensible que puede ser vulnerada como cualquier sistema de información por lo cual es de vital importancia también la mitigación de estos riesgos o vulnerabilidades a los cuales se está propenso día a día ya que son más de 15 mil empleados los cuales cuentan con diferentes accesos a este tipo de información.

Por consiguiente, el cronograma laboral se llevará a cabo con más eficiencia y el desarrollo de las labores, se realizará bajo amplios estándares y una mejor calidad de acceso a los aplicativos y su información para los empleados de la empresa corbeta. Además, se tiene un previo control de cada uno de los roles y/o permisos que otorgan a los usuarios asociados dando como prioridad mejorar el proceso de gestión de acceso de dichos usuarios frente a cada uno de los aplicativos, donde se pueden parametrizar de una manera más eficiente y con un menor factor de riesgos para la compañía, ya que la empresa maneja más de 80 aplicativos de las cuales algunas manejan información altamente sensible acerca de los movimientos financieros en la compañía por lo que un mal acceso puede llevar a causar una gran repercusión en la empresa.

5. Objetivos

5.1 Objetivo General

Plantear una propuesta de mejora en el proceso de parametrización de los usuarios frente a los aplicativos de la compañía Colombiana de Comercio Corbeta S.A, que permita minimizar los tiempos de gestión en cada uno de los procesos y mitigar las vulnerabilidades informáticas que se pueden presentar en el gestor de Identidades y las pérdidas de información.

5.2 Objetivo Específico

- Determinar los requerimientos del gestor de automatización para la intranet (AUCA)

- Detectar las falencias del gestor utilizado en la compañía Colombiana de Comercio Corbeta S.A y analizar una propuesta para el cambio de gestor de identidades.

- Analizar mediante estadísticas el comportamiento de la cantidad de peticiones o incidencias que pueden llegar a el área por medio de las diferentes Unidades de Negocio, para determinar la magnitud de solicitudes que se generan en un determinado tiempo y su cumplimiento de ANS.

- Establecer la propuesta de mejora sobre las falencias encontradas en la parametrización de los usuarios para los aplicativos de la compañía con el fin de dar una solución a las incidencias y requerimientos diarios que se presentan en el área.

6. Metodología

La metodología que se utilizara para el desarrollo del proyecto se basará en Six Sigma, ya que esta técnica es usada en la gestión de calidad de los proyectos en la cual se vincula con la mejora que queremos realizar, donde definiremos los procesos que se llevan a cabo dentro del área gestión de accesos para la empresa Colombiana de Comercio Corbeta S.A con el fin de determinar los alcances del proyecto, evaluar cómo se puede reducir el tiempo que lleva parametrizar cada uno de los usuarios que reporten en la compañía mejorando la productividad en el área y entregando soluciones con estándares de calidad más elevados.

Para comenzar con el desarrollo se determinará en cinco fases el proyecto, se iniciará con una investigación del proceso que se realiza en el área, tomando esta información para una revisión, evaluación y análisis de las posibles mejoras para el proceso y por último se podrá tener una propuesta concluyente resultado de este previo análisis de datos con el cual definiremos la probabilidad de éxito del proyecto.

Figura 1. Metodología, Six Sigma

Fuente: Autor Propio, diseñado en Lucidchart

6.1 Cronograma

Para el desarrollo del presente proyecto una vez culminada la pasantía en la empresa Colombiana de Comercio Corbeta S.A se presenta el siguiente cronograma de actividades elaborando el diagrama de Gantt en la herramienta ofimática Excel.

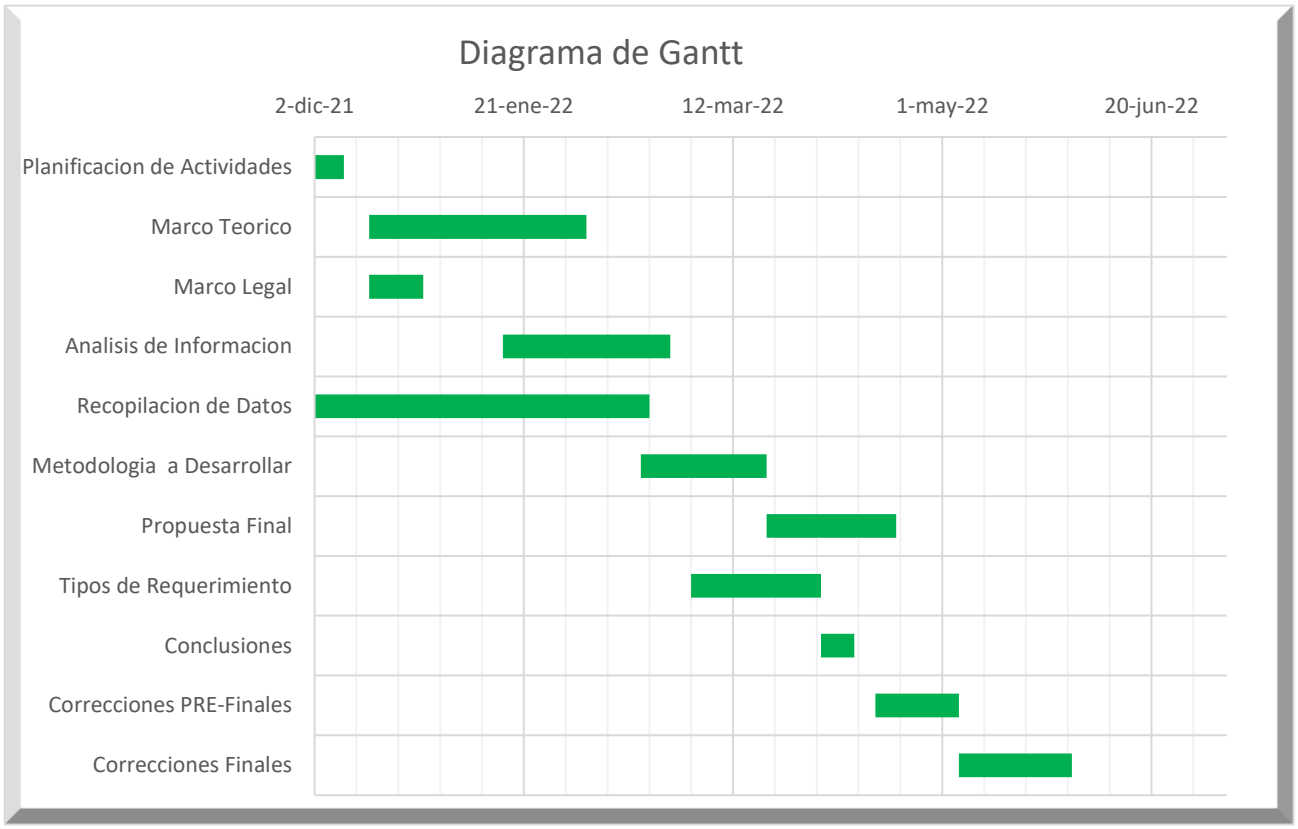
Tabla 1 Cronograma de Actividades.

CRONOGRAMA DE ACTIVIDADES					
FASE	ACTIVIDADES / ESTRATEGIAS	RESPONSABLE	Duracion (Dias)	FECHA	
				Inicio	Fin.
PLANEACIÓN	Planificacion de Actividades	Maria Paula Suarez	5	2/12/2021	7/12/2021
	Marco Teorico	Maria Paula Suarez	21	15/12/2021	5/01/2022
	Marco Legal	Maria Paula Suarez	6	22/12/2021	28/12/2021
	Analisis de Informacion	Maria Paula Suarez	40	16/01/2022	25/02/2022
	Recopilacion de Datos	Maria Paula Suarez	80	2/12/2021	20/02/2022
DIAGNÓSTICO	Metodologia a Desarrollar	Maria Paula Suarez	30	18/02/2022	20/03/2022
	Propuesta Final	Maria Paula Suarez	15	20/03/2022	4/04/2022
	Tipos de Requerimiento	Maria Paula Suarez	31	2/03/2022	2/04/2022
VALIDACION	Conclusiones	Maria Paula Suarez	8	2/04/2022	10/04/2022
	Correcciones PRE-Finales	Maria Paula Suarez	20	15/04/2022	5/05/2022
	Correcciones Finales	Maria Paula Suarez	27	5/05/2022	1/06/2022

Fuente: Autor Propio

6.2 Diagrama de Gantt

Figura 2 Diagrama de Gantt



Fuente: Autor Propio, Creado en Microsoft Excel 2019

7. Marco Teórico

Para dar inicio al desarrollo del proyecto primero se dará una breve descripción de los conceptos básicos que se comenzarán a trabajar en el documento con los cuales podremos encontrar una propuesta de mejora a los sistemas manejados en el área de seguridad informática específicamente en el área de gestión de accesos de la empresa Colombiana de Comercio Corbeta S.A

7.1 Gestor de Identidades

El gestor de identidades dentro de una compañía permite administrar las cuentas de los usuarios, los recursos de red corporativos, y los accesos para los diferentes aplicativos o sistemas, como función principal el poder administrar la identidad de los usuarios en la red garantizando la autenticación de cada uno de ellos.

Generalizando este concepto la administración de identidades le permite a la compañía saber que pueden hacer los usuarios de en los aplicativos o la red, en qué circunstancias y en qué dispositivos.

Dentro de un sistema, el ingreso de usuarios o identidad se convierte automáticamente en un atributo o dato el cual es almacenado en una base de datos, donde el gestor de identidades administra este atributo dentro del sistema y a su vez permite crear, modificar o eliminar estos datos o usuarios de la compañía,dando a cada uno de ellos un nivel de acceso a los aplicativos sobre los que gobierna.

En la empresa Colombiana de Comercio Corbeta S.A se maneja actualmente un gestor de identidades (AUCA) Gestor de Automatización donde sus funciones son:

- Aprovisionamiento Automático de cuentas de Usuario
- Autoservicio de Usuarios
- Manejo de credenciales de Acceso
- Control de acceso mediante roles
- Informe de Auditoría.

7.2 Base de Datos

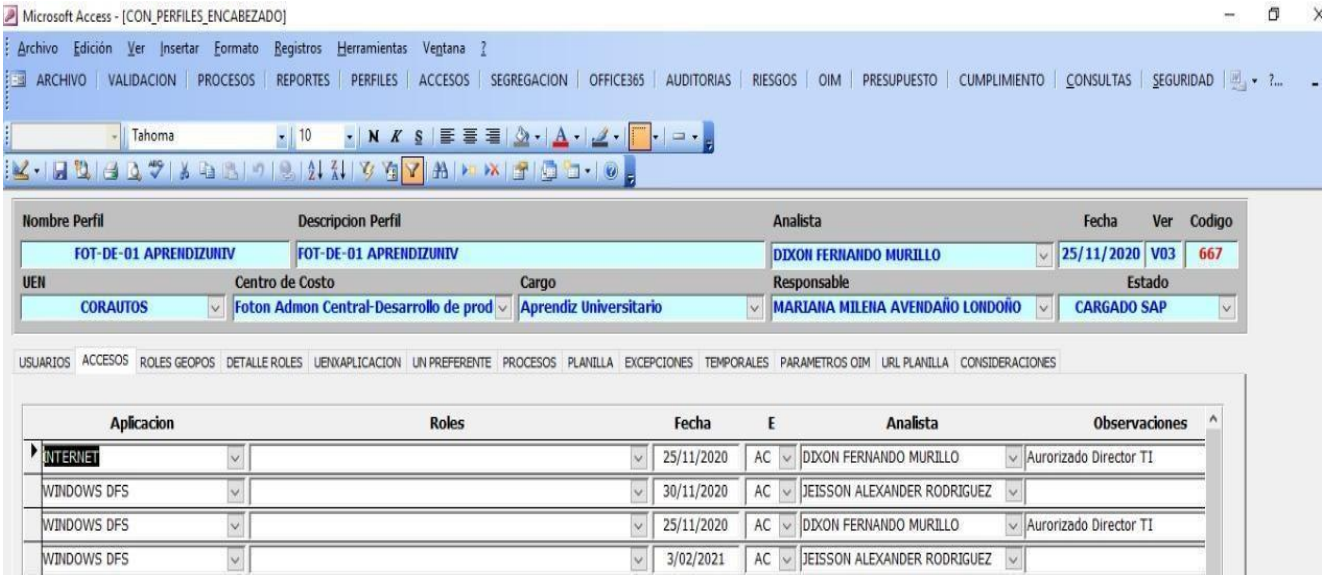
Las bases de datos facilitan la recopilación de información para su almacenamiento y procesamiento de datos, los cuales se pueden organizar o estructurar para una mejor búsqueda o manejo de ellos mediante un ordenador, también se pueden realizar análisis de los datos almacenados lo cual es de mucha utilidad para las empresas, actualmente existen diversos tipos de bases de datos como relacional, distribuida, orientada a objetos, NoSQL y gráficas (EKCIT, 2019).

La empresa Colombiana de comercio Corbeta S.A actualmente maneja una base de datos relacional MySQL la cual le permite hacer una recopilación de la información de los empleados internos y externos de la compañía con la cual se puede consultar, almacenar, modificar, extraer y analizar los datos de cada uno de los empleados todos estos datos son almacenados en tablas por separado que se componen en filas y columnas o atributos lo cual la hace más flexible , para realizar las opciones de consulta previamente descritas se hace por medio de un gestor de base de datos, actualmente el gestor de base de datos (DBMS) que utiliza la compañía es ACCESS de Microsoft (Hosting, 2019)

Database Management System (DBMS).

es un software con el cual se accede a la base de datos relacional de la compañía, en la empresa Colombiana de Comercio Corbeta S.A actualmente se maneja Microsoft Access versión 2013, donde por medio de esta aplicación se puede crear, administrar y depurar la información de la base de datos mediante la siguiente interfaz.

Figura 3. Gestor Base de Datos Access



Fuente: Colombiana de Comercio Corbeta S.A

7.3 RPA

La Automatización de Procesos Robóticos se define como el uso de robots de software para automatizar las tareas diarias y repetitivas que normalmente es realizado por los empleados de las organizaciones, mejorando el flujo de trabajo y reduciendo el riesgo de error un 10% de las áreas manuales, acelerando los procesos se mejora la productividad continua todo el día hasta 5 veces más rápido de lo que lo haría un empleado. Actualmente la compañía Corbeta S.A cuenta con seis Robots cada uno de ellos se encarga de realizar un reporte diario en unos aplicativos específicos donde indican el procedimiento que se debe hacer a cada uno de ellos ya sea bien activar, desactivar, crear o depurar.

El RPA nace de Business Process Management BPM en los años 90, donde se pretende administrar todos los procesos de una empresa en tondo a poder visualizarlos y transformar dichos procesos a medida que se fue implementando este modelo nació el Business Process Automation BPA, el cual se focaliza en automatizar el proceso de inicio a fin. Y finalmente surge el RPA para automatizar todo este proceso manual de los negocios propiamente a iniciosdel año 2000 actualmente puede trabajar esta automatización con plataformas como SAP, Oracle, Microsoft entre otras (IBM, 2020)

7.4 Seguridad de la Información

La seguridad de la información definida según ISO27001 habla de la confidencialidad y tratamiento de datos de la información importante dentro de una organización ya sean en formatos digitales, audios, videos o incluso en papel.

Hay 3 tipos de información con la cual trabajan todas las organizaciones porlo cual se debe tener en cuenta el nivel de confidencialidad.

Información Crítica.

La información crítica es indispensable en el correcto funcionamiento de las organizaciones, ya que estos datos establecen los beneficios a medio y largo plazo ya sea para ventas o atención al cliente por lo cual es de vital importancia establecer los protocolos de seguridad para este tipo de datos.

Información Valiosa.

Este tipo de información es vital para las organizaciones ya que tiene variantes subjetivas para un tipo de sector o mercado lo cual lo hace de tipo valiosa dependiendo de la actividad del sector o negocio por lo cual es importanteevaluar que tan importante puede ser la información o no para la organización.

Información Sensible.

Los datos o información de tipo sensible son los datos privados de los usuarios o clientes de las organizaciones, por lo cual es indispensable que solo tengan acceso a esta información las personas autorizadas al tratamiento de

dichos datos por lo cual los sistemas de seguridad de la información deben garantizar la protección de datos de los clientes.

8. Marco Legal

8.1 Antecedentes

Bajo la gran cantidad y evolución de los mercados y tendencias cambiantes las empresas optaron por incluir herramientas tecnológicas, las cuales permiten que el trabajo sea menos riguroso y rústico, mediante la automatización de los procesos reduciendo tiempo excesivo a tareas esto permite minimizar costos, aumenta la eficiencia y agilizar procesos complejos.

Con lo anterior se da cavidad a la transformación tecnológica describe la optimización de los procesos de un negocio impulsando la eficiencia, crear estándares útiles, ahorrando tiempo, dinero y recursos, favoreciendo a la compañía con tareas de alto volumen de manera organizada conduciendo mayores beneficios.

Tabla 2 Automatización

Posibles Problemas	¿Cómo puede ayudar la automatización?
Aspectos para considerar	La automatización de procesos le dará libertad a tu equipo de trabajo para que se enfoque en las tareas más complejas.
Algunas personas son culpadas por retrasar un proceso.	las empresas están propensas a fallas humanas, pero entendiendo que los procesos pueden sermecanizados podemos reducir el margen de error. Los tiempos de entrega se cumplirán siempre.
La falta de prioridades y gestión deprocesos causa mucho desperdicio de recursos y tiempo.	En el trajín diario es normal que las prioridades vayan cambiando de acuerdo con las necesidades de lasempresas. Sin embargo, con la automatización todos los procesos seguirán siendo realizados, independientemente de las situaciones. El tiempo y los recursos no serán desperdiciados para cubrir baches
Correr contra el tiempo para entregar resultados es parte de la rutina de la empresa	Uno de los bienes más preciosos es el tiempo. Nadie lo puede recuperar. La automatización de procesos evitará que los empleados inicien una carreracontra el reloj, dejando de lado sus actividades para entregar las tediosas tareas manuales.
Algunas actividades quedan pausadas durante mucho tiempo y no sesabe por qué no continúan.	Las actividades menos importantes quedaránrelegadas hasta que alguien les dé prioridad. Ciertamente, con la automatización de procesos noserían pausadas y no se retrasarían.

Nota: Mediante la tabla 2 se puede plasmar la idea para mejorar en aspectos según la ley del consejo de Colombia (EL CONGRESO DE COLOMBIA, 2020).

Ley 2052 del 25 de agosto de 2020

Artículo 5. AUTOMATIZACIÓN Y DIGITALIZACIÓN DE LOS TRÁMITES.

Nos plantea la necesidad de automatizar y que sea un proceso digital por gestión interna, esto expedido por el departamento administrativo de la función pública y el ministerio de tecnología de la información, para que dichos procesos se digitalicen sin que se genere un cobro ni que se establezca una tarifa dando así a cumplir con la ley para evadir su correspondiente sanción.

8.2 Normatividad

"El presente documento se basa en las buenas prácticas, leyes y normas relacionadas con la seguridad de la información: Ley 1273 de 2009 — De La Protección de la Información y de los datos, ISO/IEC 27001:2013 — Sistemas de Gestión de Seguridad de la Información (SGSI), ISO/IEC 17799 -2 :2005 — Código Para la Práctica de la Gestión de la Seguridad de la Información, ISO 22301:2012" (Política de respaldo, custodia y recuperación de la, 2019). La norma puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades interorganizacionales.

8.3 Prerrequisitos

➢ Todas las copias de información crítica deben almacenarse en un área adecuada y con control de acceso (Política de respaldo, custodia y recuperación de la, 2019). Las copias de respaldo se mantendrán con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y/o por requerimiento legal.

➢ Los administradores de los servidores de Backus realizarán periódicamente pruebas de restauración de la información mediante la rotación de los medios y en un ambiente de pruebas controlado (Política de respaldo, custodia y recuperación de la, 2019), con el objetivo de garantizar que los medios se encuentran funcionando adecuadamente.

➢ Para la gestión de archivos compartidos de los usuarios, DPA, Documental creó carpetas para la copia que se realizan a la información que puede ser vulnerable, siguiendo una nomenclatura de tablas de retención documental generadas por dicho grupo.

➢ Los Analistas de la base de datos de Colombiana de comercio S.A. adoptará planes de recuperación de emergencia para todas las aplicaciones que manejen información crítica. Dichos planes se actualizarán periódicamente, y serán probados y revisados.

➢ El personal encargado, mantendrá al menos una copia de la información

en un servidor de archivos y A su vez, realizará periódicamente pruebas de funcionamiento y ejecución de los procesos de Backus (Política de respaldo, custodia y recuperación de la, 2019). La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario.

9. Análisis De Información

La presente investigación se realizó con el fin de identificar la frecuencia de las solicitudes de los usuarios para la gestión y manipulación de los aplicativos, por medio de la herramienta POWERBI, haciendo una recopilación de datos en cuanto a peticiones tales como modificación, eliminación y/o creación en cada uno de los aplicativos bajo el grupo en gestión de accesos y los técnicos de operación de identidades quienes son los que día a día parametrizan estos usuarios.

Esta información es tomada de un previo análisis que se realiza en cuanto criterios y títulos de las solicitudes, basadas en tiempos estimados, buscando así llegar a evaluar las peticiones realizadas en diferentes aplicativos de los negocios de la compañía, a partir de ello se realiza la validación y gestión en cuanto parametrización del perfil asociado dando así los accesos pertinentes según la asignación de perfil por el gestor de usuario. Estas solicitudes se realizan basadas en Consultas de los atributos de informe y a través de solicitudes para obtener información precisa dando su mayor gestión e investigación acerca de la atención de peticiones e incidentes y los casos que reportan diariamente.

En la figura 4. Análisis de Incidencias podemos observar la cantidad de incidencias que llegan al área en un mes desde el 01 de enero al 01 de febrero para los 3 técnicos que actualmente se dedican a la resolución de estos incidentes provenientes de las diferentes unidades de negocio con un total de 275 casos cumpliendo los ANS establecidos en un 90.18%.

Figura 4. Análisis de Incidencias

Fuente: Herramienta PowerBI-Colombiana de Comercio Corbeta S.A

En la figura 5. Análisis de Peticiones podemos observar la cantidad de solicitudes que llegan al área en un mes desde enero a febrero para los 3 técnicos que actualmente se dedican a la resolución de estas peticiones provenientes de las diferentes unidades de negocio con un total de 1.002 casos en los cuales se ve la dificultad de cumplir los ANS requeridos por la empresa ya que son demasiadas solicitudes para el recurso humano que tiene actualmente.

Figura 5. Análisis de Peticiones

Fuente: Colombiana de Comercio Corbeta S.A.

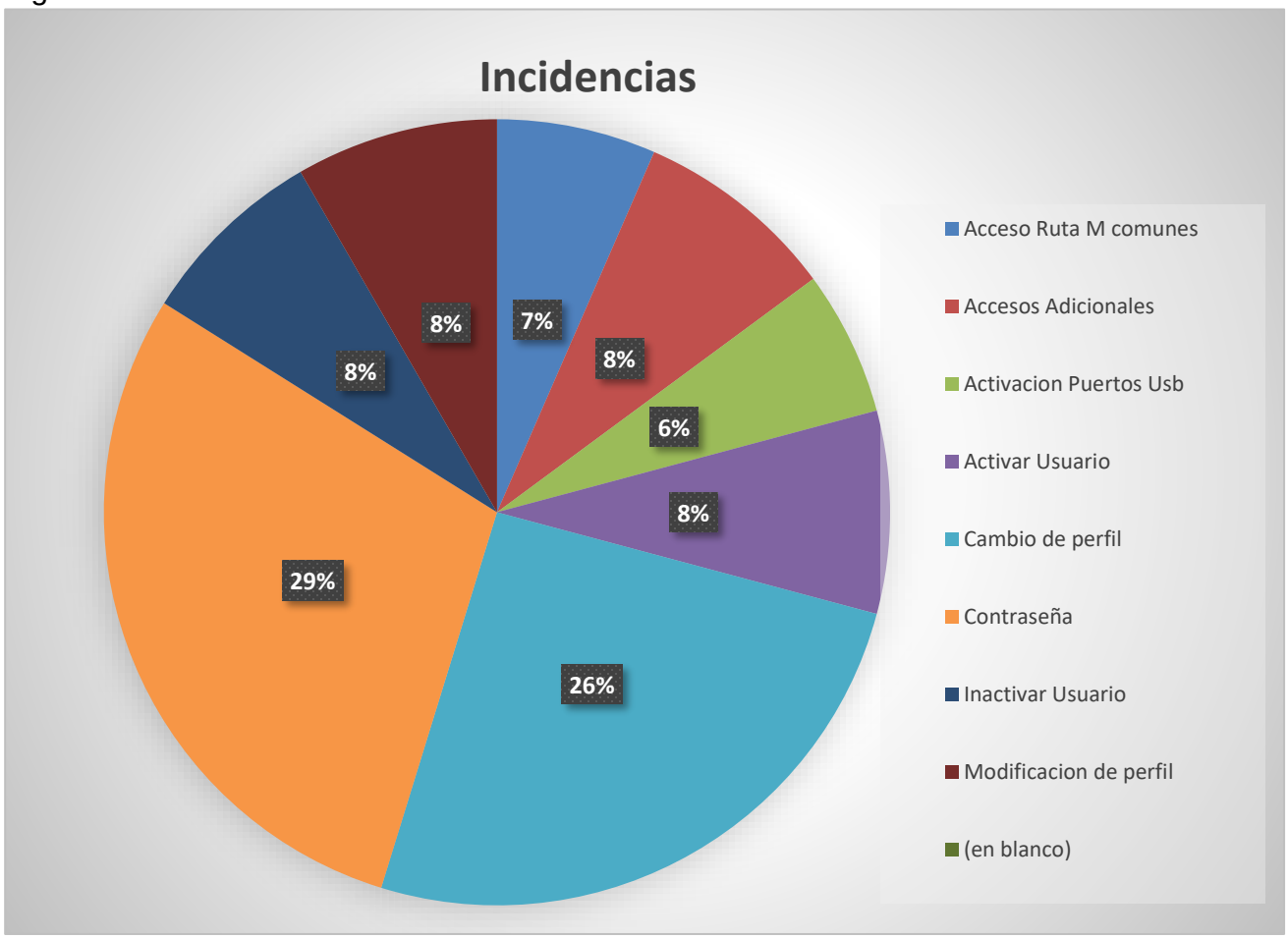
En la siguiente tabla dinámica se observan las cantidades de peticiones en el mes de Abril donde observamos la clasificación de los incidentes que pueden llegar como lo son de accesos no funcionales, configuración de aplicaciones, error de aplicación, gestión de accesos y de tipo información o datos en columnas y segmentado por las categorías que se manejan actualmente con un total de 210 incidencias en las cuales según el grafico de incidencias el 26% son cambio de perfil y el 29% son contraseñas donde se observa que son un gran numero de

credenciales que gestionar teniendo un gestor de identidades que permite su autogestión de credenciales lo cual evidencia su deficiencia.

Tabla 3. Solicitud de Incidencias

Cuenta de Categoría	Etiquetas de co					
Etiquetas de fila	Acceso no Funcional	Configuración Aplicacion	Error de Aplicacion	GESTION DE ACCESOS	Informacion o Datos	Total general
Incidencia	**168**	**2**	**36**	**1**	**3**	**210**
Acceso Ruta M comunes	11					11
Accesos Adicionales	14	1	5			20
Activacion Puertos Usb	10		5		2	17
Activar Usuario	14					14
Cambio de perfil	43		13		1	57
Contraseña	49	1	12			62
Inactivar Usuario	13					13
Modificacion de perfil	14		1	1		16
Total						
(en blanco)						
Total general	**168**	**2**	**36**	**1**	**3**	**210**

Figura 6. Gráfico Incidencias



En la tabla 4. Observamos en el mes de abril las solicitudes que llegaron fueron un total de 887 de las cuales a nivel de peticiones se tienen diferentes categorizaciones entra las que los cambios de credenciales siguen siendo muy altas, así como la validación de accesos con un 55% en accesos y un 18% de contraseñas esto indica la demanda que hay frente al área para el cambio y realización de accesos en un corto tiempo.

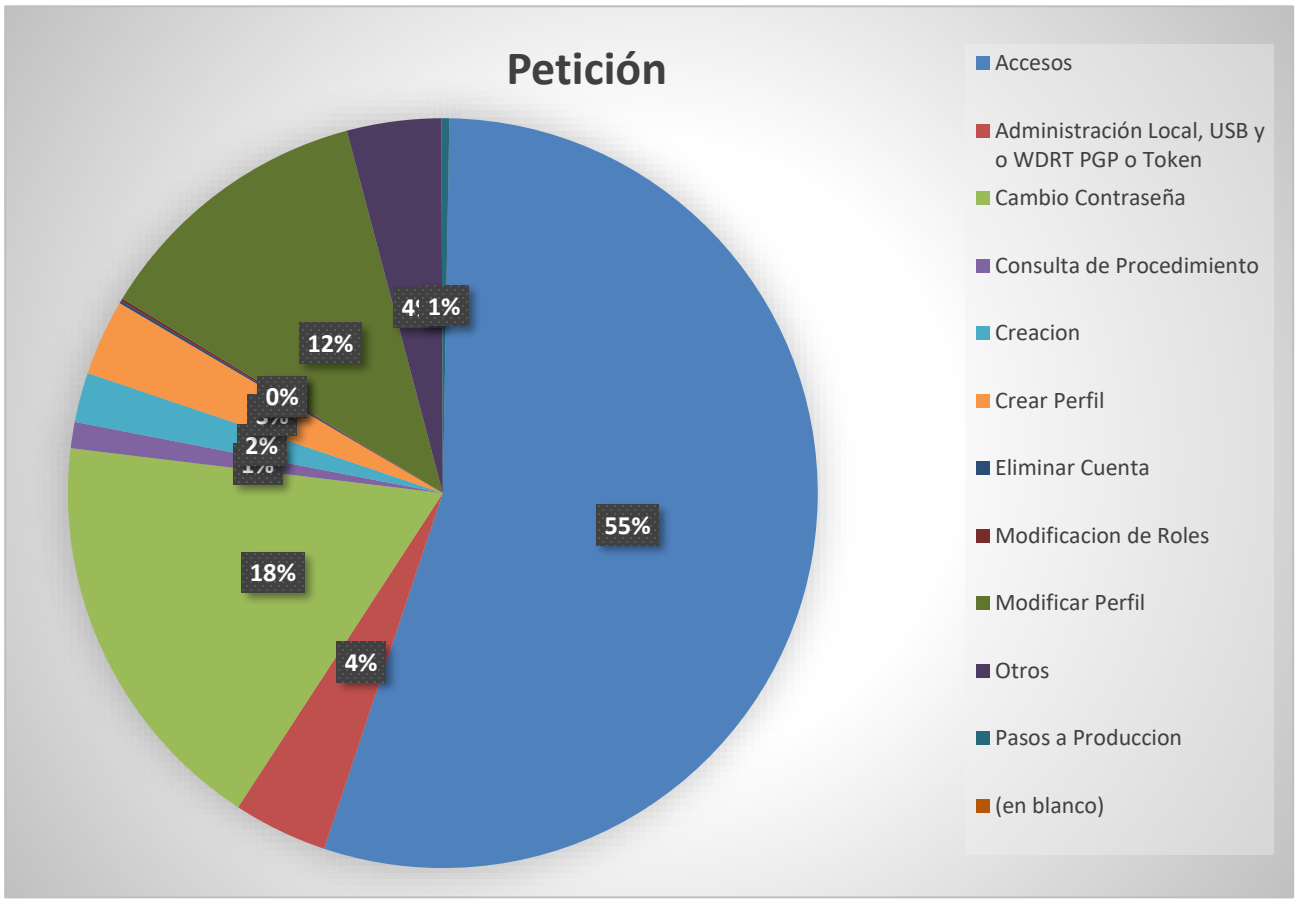
Tabla 4. Solicitud de Peticiones

Cuenta de Tipo de caso	Etiquetas de columna		
Etiquetas de fila	Petición	Total	Total general
Accesos	486		486
Administración Local, USB y o WDRT PGP o Token	36		36
Cambio Contraseña	157		157
Consulta de Procedimiento	10		10
Creacion	19		19
Crear Perfil	29		29
Eliminar Cuenta	1		1
Modificacion de Roles	1		1
Modificar Perfil	108		108
Otros	36		36
Pasos a Produccion	3		3
(en blanco)		1	1
Total general	**886**	**1**	**887**

&

Fuente: Autor Propio - Herramienta Excel

Figura 7. Gráfico de Peticiones



Fuente: Autor Propio - Herramienta Excel

Requerimientos Funcionales

Tabla 5. Requerimiento funcional 01

Identificación del requerimiento:	RF01
Nombre del Requerimiento:	Ingresar al PC con un nombre de usuario y contraseña.
Características:	El usuario ingresa con credenciales que le fueron asignadas.
Descripción del requerimiento:	El usuario administrador hace el registro de todos los usuarios que tendrán acceso al sistema y lesasigna una clave y usuario con el que podrán ingresar.
Prioridad del requerimiento: Alta	

Nota; Mediante la tabla evidenciamos la calificación de los requerimientos funcionales para las pautas a tener en cuenta en el proceso de gestión de accesos y la debida parametrización de los usuarios, esta clasificación se adoptódel documento Especificación de requisitos de software, (SISCOOP, 2010).

Tabla 6. Requerimiento funcional 02

Identificación del requerimiento:	RF02
Nombre del Requerimiento:	Ingresar a la base de datos
Características:	Posee un usuario autorizado para poderacceder a la base de datos
Descripción del requerimiento:	Ingresa a la base de datos validando el usuario y elmodo en que manipula la DPA
Prioridad del requerimiento: Alta	

Nota; Mediante la tabla evidenciamos la calificación de que los requerimientos funcionales para el desarrollo de la automatización, esta clasificación se adoptó del documento Especificación de requisitos de software, (SISCOOP, 2010).

Tabla 7. Requerimiento funcional 03

Identificación del requerimiento:	RF03
Nombre del Requerimiento:	Ingresar al servidor S: para validar cada uno de los planos
Características:	Identificar errores de los planos y percibir los que nose ejecutaron
Descripción del requerimiento:	Valida la causante del error, la confiabilidad de los datos obtenidos para posterior a ello actualizar las tablasde la base de datos.
Prioridad del requerimiento: Alta	

Tabla 8. Requerimiento funcional 04.

Identificación del requerimiento:	RF04
Nombre del Requerimiento:	Comparativo de los parámetros de los planos y lacopia de seguridad
Características:	Mediante procesos se verifican los datos actualizados.
Descripción del requerimiento:	Al contar con todos los planos actualizados y corregidos de acuerdo con la causa de error, se procede averificar los parámetros con la copia de seguridad para certificar la confiabilidad de los datos.

Prioridad del requerimiento: Alta

Tabla 9. Requerimiento funcional 05

Identificación del requerimiento:	RF05
Nombre del Requerimiento:	Actualizar las Tablas para ejecutar la base de datos.
Características:	Como prioridad, para la actualización de la DPA
Descripción del requerimiento:	Se debe ejecutar en primera instancia las tablascon la información de los empleados de la compañía para acceder a la información actualizada de la DPA.
Prioridad del requerimiento: Alta	

Tabla 10. Requerimiento funcional 06

Identificación del requerimiento:	RF06
Nombre del Requerimiento:	Genera los planos para poder obtener las novedades
Características:	Dado el caso final se genera los reportes de estadode los usuarios
Descripción del requerimiento:	Mediante la actualización de cada una de las tablasa través de los planos, se generan novedades acerca del estado de los usuarios en los diferentes aplicativos

	no conectados a Auca
Prioridad del requerimiento: Alta	

Tabla 11. Requerimiento funcional 07

Identificación del requerimiento:	RF07
Nombre del Requerimiento:	Guardamos en el repositorio de las novedades
Características:	Se gestionan de acuerdo con lo indicado
Descripción del requerimiento:	Al realizar la consulta de las novedadesnos genera acciones que debemos tomar en cuanto al estado del usuario, es decir, está ausente, retirado o activo para poder gestionarlos enciertos aplicativos
Prioridad del requerimiento: Alta	

Tabla 12. Requerimiento funcional 08

Identificación del requerimiento:	RF08
Nombre del Requerimiento:	Compactamos y reparamos la base de datos
Características:	Se genera esto con el fin de guardar todos los cambios y que se actualice

Descripción del requerimiento:	Una vez se culmine con la ejecución de cada uno de los planos y las novedades se procede a compactar y reparar, esto con el fin de que se repliquen las modificaciones y actualice el procesorealizado
Prioridad del requerimiento: Alta	

Tabla 13. Requerimiento funcional 09

Identificación del requerimiento:	RF09
Nombre del Requerimiento:	Agregamos la base de datos a el servidor S:
Características:	Copia y pegamos la DPA en este servidor para eluso de los demás funcionales del área
Descripción del requerimiento:	Al finalizar y a verse generado los cambios y actualizaciones de la base, sin problemas y aviándola copiado en el repositorio se realiza unacopia de seguridad
Prioridad del requerimiento: Alta	

Tabla 14. Requerimiento funcional 10

Identificación del requerimiento:	RF10
Nombre del Requerimiento:	Notificación a el área encargada

Características:	Se comunica que ya se encuentra la DPA actualizadapara que pueda continuar las labores con datos recientes
Descripción del requerimiento:	Al momento de copiarla en el repositorio y realizar la copia de seguridad se notifica a toda el área para que esta puedaser copiada y replicada en los repositorios de cada funcional del área.
Prioridad del requerimiento: Alta	

Tabla 15. Requerimiento funcional 11

Identificación del requerimiento:	RF11
Nombre del Requerimiento:	Tareas diarias
Características:	Una vez actualiza la base de datos se asignan tareas
Descripción del requerimiento:	Cuando realizamos laactualización y generamos los planos, se generan tareas las cuales derivan de tablas con elementos vacíos, de cambios o retiros en diferentes aplicativos
Prioridad del requerimiento: Alta	

Tabla 16. Requerimiento funcional 12

Identificación del requerimiento:	RF12

Nombre del Requerimiento:	Accesos temporales
Características:	Un registro de datos donde se documenta los roles oacceso por un periodo de tiempo a un usuario
Descripción del requerimiento:	Cada uno de los administradores de los negocios asignan por petición de los jefes de las tiendas, accesos a sus usuarios por periodos de tiempo haciendo que cuandoculmine, estos datos se dirigen a la consulta de accesos temporales la cual se envía una notificación, para que esta sea marcada como solucionado
Prioridad del requerimiento: Alta	

Tabla 17. Requerimiento funcional 13

Identificación del requerimiento:	RF13
Nombre del Requerimiento:	Gestión de las demás tareas
Características:	Para llevar a cabo el proceso y desarrollo de lastareas diaria
Descripción del requerimiento:	Se da una gestión a diario de estas tareas realizando la búsqueda los responsables e identificandoel nombre de usuarios de muchos otros, esto atreves de consultas en otras tablaso por peticiones en el correo o ya asignados en Auca.
Prioridad del requerimiento: Alta	

Tabla 18. Requerimiento funcional 14

Identificación del requerimiento:	RF14
Nombre del Requerimiento:	Informe semanal
Características:	Se genera un informe semanal para evidenciar elproceso de estas tareas
Descripción del requerimiento:	Semanalmente se genera la revisión de las tareas en cada una de las tablas, tomando valores numéricos para plasmar y registrar el avance semanal y bajo qué criterios se pueden resolver en ocasiones
Prioridad del requerimiento: Alta	

Nota; Mediante la tabla evidenciamos la calificación de los requerimientos funcionales para las pautas a tener en cuenta en el proceso de gestión de accesos y la debida parametrización de los usuarios, esta clasificación se adoptódel documento Especificación de requisitos de software, (SISCOOP, 2010).

Requerimientos No Funcionales.

Tabla 19. Requerimiento NO funcional 01

Identificación del requerimiento:	RNF01
Nombre del Requerimiento:	Verificar el modo en que se va a usar la base de datos
Características:	Garantiza que se le sea permitido ejecutar los planos y actualizar la base de datos
Descripción del requerimiento:	Realización de distintas pruebas a realizar alsistema para verificar el correcto funcionamiento
Prioridad del requerimiento: Alta	

Nota; Mediante la tabla evidenciamos la calificación de los requerimientos NO funcionales para el desarrollo de mejora en el proceso de gestión de accesos y la debida parametrización de los usuarios, esta clasificación se adoptó del documento Especificación de requisitos de software, (SISCOOP, 2010)

Tabla 20. Requerimiento NO funcional 02

Identificación del requerimiento:	RNF02

Nombre del Requerimiento:	Control de acceso a la base de datos y únicamentea los usuarios autorizados
Características:	Garantiza que solo los usuarios autorizados tengan acceso a la base de datos
Descripción del requerimiento:	Mediante controles y políticas garantiza que solo los usuarios autorizados tengan acceso a la base de datos
Prioridad del requerimiento: Alta	

Tabla 21. Requerimiento NO funcional 03

Identificación del requerimiento:	RNF03
Nombre del Requerimiento:	Los permisos de acceso al sistema podrán ser cambiados solamente por el administrador de acceso a datos
Características:	Solo el usuario con mayor poder en el sistema puede realizar cambios
Descripción del requerimiento:	Especifica que solo el usuario con mayor rango en el sistema tiene el permiso para cambiar algún tipo de acceso al sistema por parte otro usuario.
Prioridad del requerimiento: Alta	

Tabla 22. Requerimiento NO funcional 04

Identificación del requerimiento:	RNF04
Nombre del Requerimiento:	El sistema debe tener un respaldo de la base de datos
Características:	El sistema realiza respaldos mediante copias para asegurar los datos contra pérdidas o daños
Descripción del requerimiento:	Al momento de la actualización se deja en el repositorio una copia de seguridad a la cual se le asigna un nombre diferente para que no sea distinguida de la base original
Prioridad del requerimiento: Alta	

Tabla 23. Requerimiento NO funcional 05

Identificación del requerimiento:	RNF05
Nombre del Requerimiento:	Tener presente el tiempo de la ejecución de las tablas
Características:	En momentos ciertos planos tardan más en la actualización de las tablas
Descripción del requerimiento:	Llevar tiempo ejecutar el plano que está actualizando en la tabla de la DPA, en ocasiones nos indica que no responde, pero es parte de la ejecución
Prioridad del requerimiento: Alta	

Tabla 24. Requerimiento NO funcional 06

Identificación del requerimiento:	RNF06
Nombre del Requerimiento:	El tiempo para iniciar o reiniciar el sistema no podrá ser mayor a 3 minutos
Características:	Mediante distintos componentes asegura que el sistema no tardará más de 3 minutos en iniciar para que el sistema funcione.
Descripción del requerimiento:	El sistema tardara un máximo de 3 min para estar completamente en funcionamiento y accesible a los usuarios
Prioridad del requerimiento: Alta	

Tabla 25. Requerimiento NO funcional 07

Identificación del requerimiento:	RNF07
Nombre del Requerimiento:	El promedio de duración de fallas no podrá ser mayor a 5 minutos
Características:	Si se produce una falla tendrá queresponder en menos de 5 minutos
Descripción del requerimiento:	El sistema deberá realizar alguna acción predeterminada para que responda en un lapso de 5 minutos en caso de alguna falla o deberá reiniciarse
Prioridad del requerimiento: Alta	

Tabla 26. Requerimiento NO funcional 08

Identificación del requerimiento:	RNF08
Nombre del Requerimiento:	Para compactar la base datos
Características:	Al momento de tener todas las tablas actualizadas y las novedades en el repositorio
Descripción del requerimiento:	Se procese de compactar la DPA y que genere los cambios pertinentes de cada uno de los usuarios suestado y aplicaciones a la que pertenece
Prioridad del requerimiento: Alta	

Tabla 27. Requerimiento NO funcional 09

Identificación del requerimiento:	RNF09
Nombre del Requerimiento:	No se debe manipular la base del servidor
Características:	No utilizar la DPA del servidor, debido a que se crea un ejecutable y no permite que sea copiadapor los demás
Descripción del requerimiento:	No se debe manipular la base de datos estando enservidor, debido a que crea un ejecutable el cual no permite que sea copiada en otros servidores y afecta las labores de los demás
Prioridad del requerimiento: Alta	

Tabla 28. Requerimiento NO funcional 10

Identificación del requerimiento:	RNF10
Nombre del Requerimiento:	Los registros se mantienen en una base de dato
Características:	Se mantienen los datos de los usuarios enlos planos para tener un registro y control
Descripción del requerimiento:	Los datos se mantienen en la base de datosdesignada para realizar el debido tratamiento a los datos con los cuales se parametrizan los usuarios.
Prioridad del requerimiento: Alta	

Tabla 29. Requerimiento NO funcional 11

Identificación del requerimiento:	RNF11
Nombre del Requerimiento:	El administrador es capaz de recuperar datos del usuario y administrarlos, mediante la introducción de un ido nombre
Características:	Por el identificador único se puede consultar
Descripción del requerimiento:	Permite buscar un dato o recuperarlo a través del identificador único que se le dio al ingresar a la base de datos
Prioridad del requerimiento: Alta	

Nota; Mediante la tabla evidenciamos la calificación de los requerimientos NO funcionales para el desarrollo de mejora en el proceso de gestión de accesos y la debida parametrización de los usuarios, esta clasificación se adoptó del documento Especificación de requisitos de software, (SISCOOP, 2010)

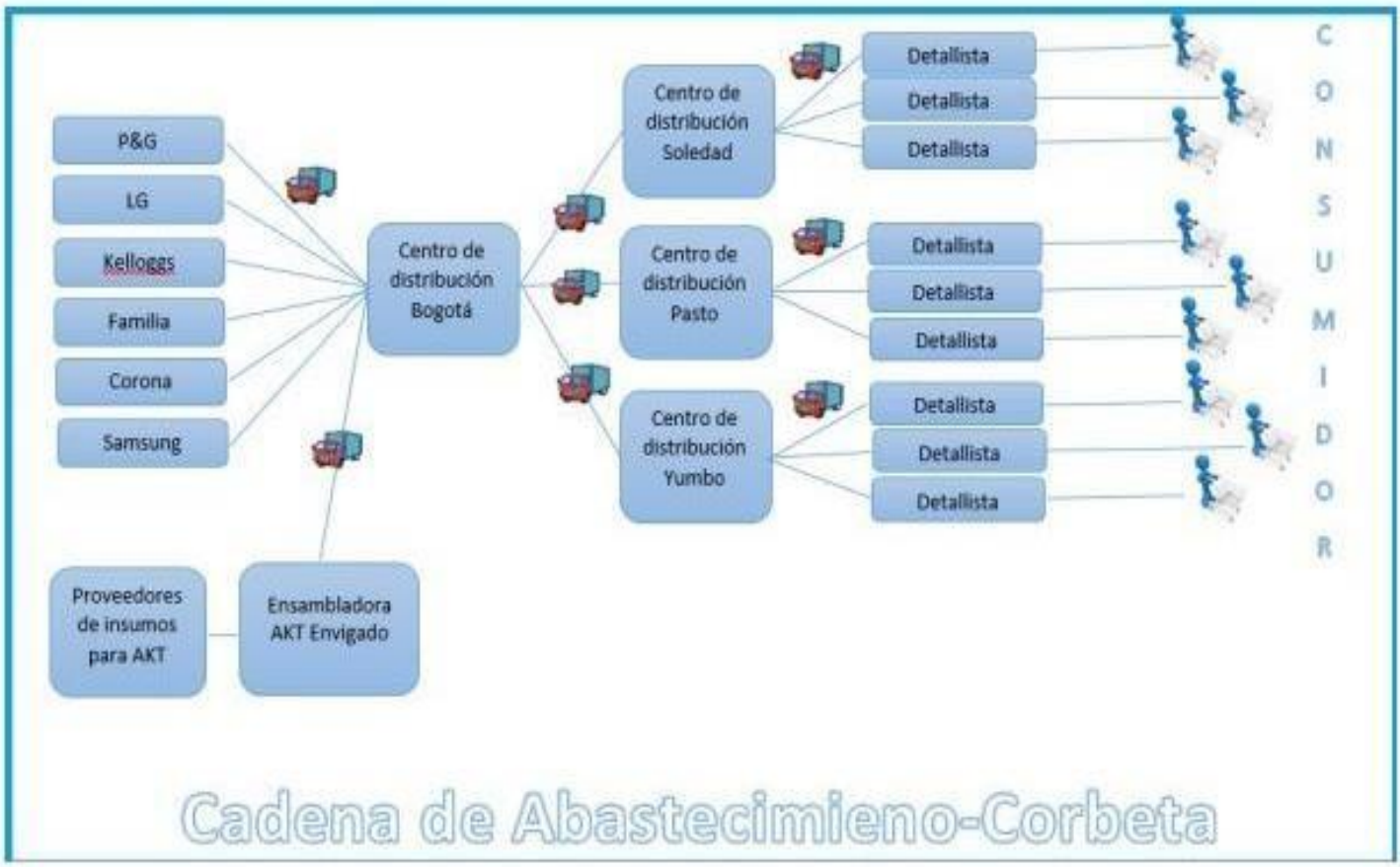
10. Descripción de la Propuesta

Para abarcar la propuesta de mejora comenzaremos por explicar un poco el proceso de gestión de acceso para los usuarios de la compañía Colombiana de Comercio Corbeta S.A y como está dividida el área de seguridad informática para entender cada una de las funciones que se realizan dentro de la compañía y como esto se ve reflejado en el proceso final para la prestación de servicios y venta de productos.

10.1 Cadena De Abastecimiento- Corbeta

Para que se pueda realizar la cadena de abastecimiento de la empresa Colombiana de Comercio Corbeta S.A hacia sus diferentes puntos de ventas y las diferentes Unidades de Negocio (UEN), se debe contar con un buen proceso interno en la compañía al momento de darle acceso a los principales usuarios los clientes ya sea para el despacho, la compra y la venta de los productos que manejan, como para los créditos, las cajas, y la dirección que hace posible el funcionamiento de toda esta cadena de abastecimiento en Colombia.

Figura 8. Cadena de Abastecimiento Colombiana de Comercio Corbeta S.A



Autor: Colombia de Comercio Corbeta S.A

10.2 organigrama de la subdirección de Planeación y Arquitectura

El área de la Subdirección de Planeación y arquitectura se despliega en el área de seguridad informática el cual se divide en tres subáreas:

10.2.1 Gestión de Accesos.

Dentro de la subárea de gestión de acceso se tiene un líder, los analistas de seguridad informática y los aprendices actualmente tres.

10.2.2 Gobierno de Identidades.

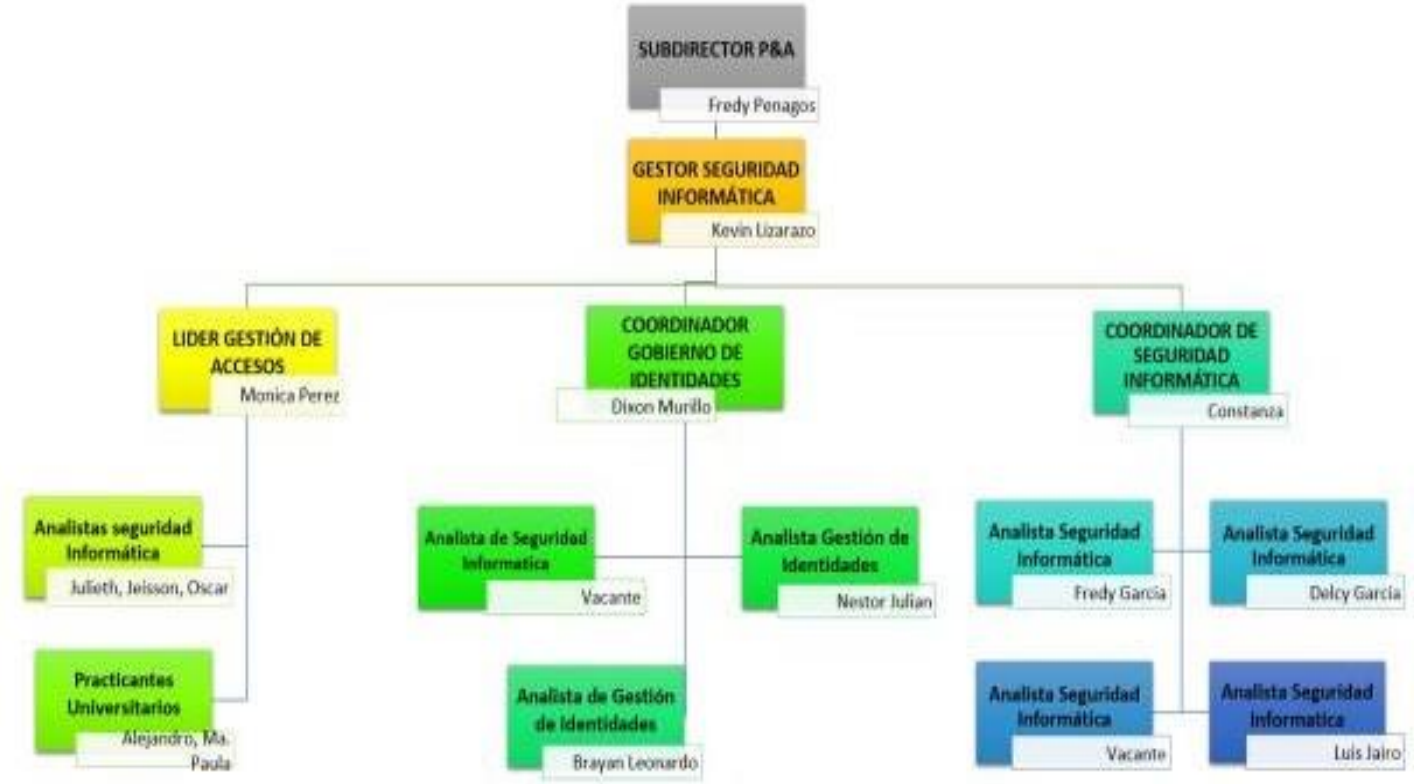
Cuenta con un coordinador de gobierno de identidades, un analista de seguridad informática y dos analistas de gestión de identidades.

10.2.3 Seguridad Informática.

La Subárea de Seguridad Informática, cuenta con un coordinador de seguridad informática y cuatro analistas de seguridad informática.

El equipo de trabajo previamente descrito es el gestor de todo el proceso de seguridad en los diferentes aplicativos, en el tratamiento de la información, y el cual es un factor importante en la parametrización de los más de 15.000 empleados internos de la compañía quienes hacen posible la anterior cadena de distribución previamente mostrada.

Figura 9. Organigrama Jerárquico Área de Seguridad Informática Corbeta S.A



Autor: Colombiana de Comercio Corbeta S.A

10.3 Proceso de Gestión de accesos.

En el siguiente diagrama se encuentra el proceso que se realiza dentro del área de gestión de accesos para los usuarios que ingresan en la compañía en el cual se les asigna una posición desde nomina al momento de la contratación donde nos indican el perfil que requiere este empleado, el siguiente paso es consultar si existe este perfil o si se debe crear uno nuevo, en caso de que no exista se pasa el caso a gobierno de identidades quien evalúa una posible apertura de perfil y su documentación dentro del directorio de perfiles esto volviendo al punto de partida de si existe el perfil, una vez creado o si ya existía se pasa el caso al grupo de gestión de accesos el cual parametriza el usuario dando los accesos correspondientes al perfil indicado por nómina.

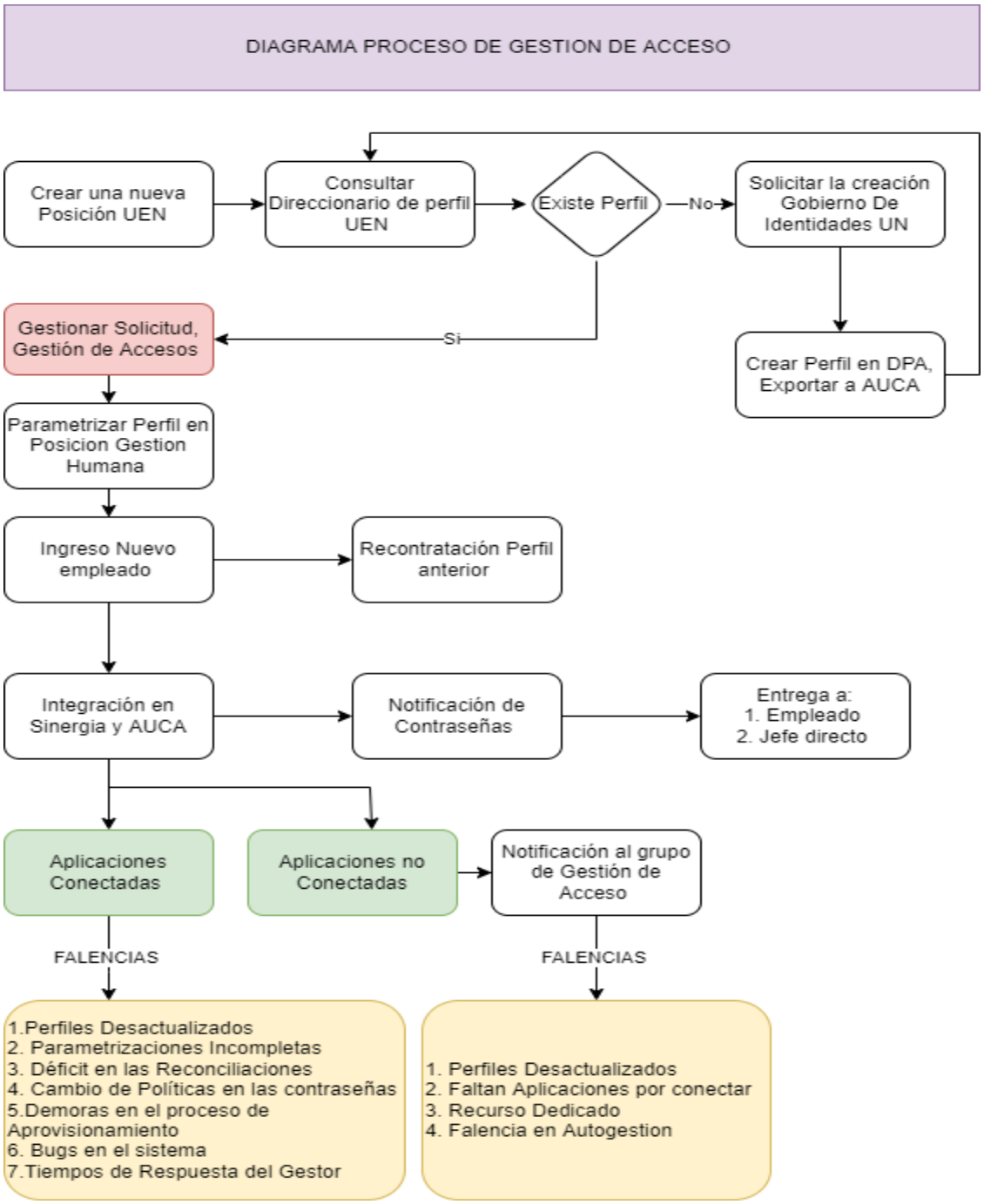
Si es un usuario que yahabía sido creado dentro del sistema simplemente se activa y se hace entrega de las credenciales de acceso, en caso de ser nuevo en la compañía se parametriza y se entregan las credenciales de los aplicativos conectados y no conectados de laempresa. las entregas de estas credenciales se envían a el jefe directo o el usuario en cuestión para el ingreso a los diferentes sistemas de la compañía.

Los Usuarios que ingresan a la compañía se encasillan en perfiles estructurados de la siguiente manera:

- Unidad de Negocio - División de Área - Departamento

Los perfiles indican el número de aplicativos, el nivel de acceso a los aplicativos o el rol que corresponde a cada departamento, por lo cual tener los perfiles actualizados es la mayor utilidad en la gestión de acceso.

Figura 10. Diagrama del proceso de Gestión de Acceso.



Fuente: Autor Propio, diseñado en Lucidchart

10.4 Falencia en el proceso de Gestión de Accesos

Al momento de realizar el proceso de gestión de acceso se cuenta con varios incidentes o fallas en el mecanismo de la parametrización de los usuarios respecto a los aplicativos conectados y no conectados:

10.4.1 Aplicativos Conectados.

El gestor de Identidades (AUCA) cuenta aproximadamente con una administración del 50% de los aplicativos conectados entre los cuales se detallaron las siguientes falencias:

1. El gestor de Identidades no está actualizado con los perfiles existentes enla base de datos.
2. No se cumple con las parametrizaciones completas ya que el Gestor tiene un déficit en la información de los perfiles por lo cual no crea los usuarios con los roles en los aplicativos conectados.
3. El gestor de identidades AUCA no crea los usuarios de forma adecuada por lo que se debe hacer un reproceso en la creación o reconciliación de los usuarios entre el gestor administrativo y el aplicativo esto se realiza mediante la base de datos de Oracle.
4. Cuando hay cambio de políticas de contraseñas en los aplicativos, al crear un usuario nuevo no se crea en los aplicativos ya que no se ha actualizado esta nueva política en el gestor.
5. El proceso de aprovisionamiento entre el gestor de identidades

(AUCA) y los aplicativos toma más de 20 minutos.

6. Los bugs en el sistema se han convertido en un problema casi constante ya que no replican los accesos y no se parametrizan los usuarios correctamente

7. El tiempo de respuesta del gestor tarda entre unos 10- 20 minutos para replicar los accesos en los diferentes aplicativos.

10.2.4 Aplicativos No Conectados.

1. La desactualización de los perfiles respecto a los roles que se deben asignar a los usuarios retrocede la entrega de los accesos y la parametrización de los usuarios.

2. El 50% de los aplicativos se encuentra no conectado al gestor de identidades por lo que la administración, creación, permisos se debe hacer manual.

3. Se necesita dedicar tiempo extra en la creación de usuario por usuario de forma manual en estos aplicativos por lo cual se invierte un recurso dedicado como lo es la mano de obra, perdiendo este recurso en un gran porcentaje de tiempo.

4. Al ser no conectada no se cuenta con la Autogestión de contraseñas de los usuarios en los aplicativos lo que conlleva a más trabajo para el grupo de gestión de accesos.

10.5 Modelo de Operación Gestión de Acceso

Las herramientas de trabajo para realizar la gestión a las solicitudes de peticiones para los diferentes aplicativos sobre los cuales se tiene la administración se realiza por medio del gestor de identidades (AUCA) desde el cual crea los casos a la plataforma de ProactivaNet el cual es un aplicativo que genera incidentes o peticiones a los técnicos y analistas de seguridad informáticay las demás áreas.

Dentro de sus funciones se encuentra:

- Asignar accesos en aplicaciones no conectadas
- Creación de Usuarios Externos y Genéricos
- Peticiones sobre los accesos
- la asignación de accesos temporales
- Resolver todo tipo de incidentes sobre los accesos
- Cambio de Credenciales en los aplicativos

Figura 11. Modelo de Operación.

Fuente: Colombiana De Comercio Corbeta S.A

11 Propuesta final en el área de Gestión de Accesos

A continuación, se encuentra la propuesta final con la cual se busca concluir que procesos, software o herramientas se deben cambiar para poder tener una mejora en el proceso de gestión de accesos al momento de solucionar un requisito o un incidente que requiera alguna parametrización de usuario.

11.1 Cambio de Gestor de Identidades

Muchos de los reprocesos que se realizan en el área de Gestión de accesos se debe a la deficiencia del gestor de identidades actualmente llamado (AUCA) por

la compañía, el proveedor de este software es Oracle donde su plataforma se denomina Oracle Identity Management, se ha evidenciado una serie de carencias o fallos al momento de parametrizar los usuarios por medio de este software como los descritos a continuación.

- No hay gobernanza total en todos los aplicativos que maneja el área de gestión de accesos
- No funciona la autogestión de credenciales para los aplicativos en el gestor AUCA.
- El tiempo de aprovisionamiento de los usuarios en los aplicativos toman más de 20 minutos.
- Error en la creación o parametrización de los usuarios en los aplicativos conectados al gestor AUCA.
- Carece de Integración con los demás aplicativos.
- Genera cargas laborales para los analistas lo cual repercute en el área al tener que gastar un recurso dedicado.
- Desactualización de datos en el gestor de identidades lo cual detiene el proceso de parametrización.

Figura 12. Cuadro Comparativo de Gestores.

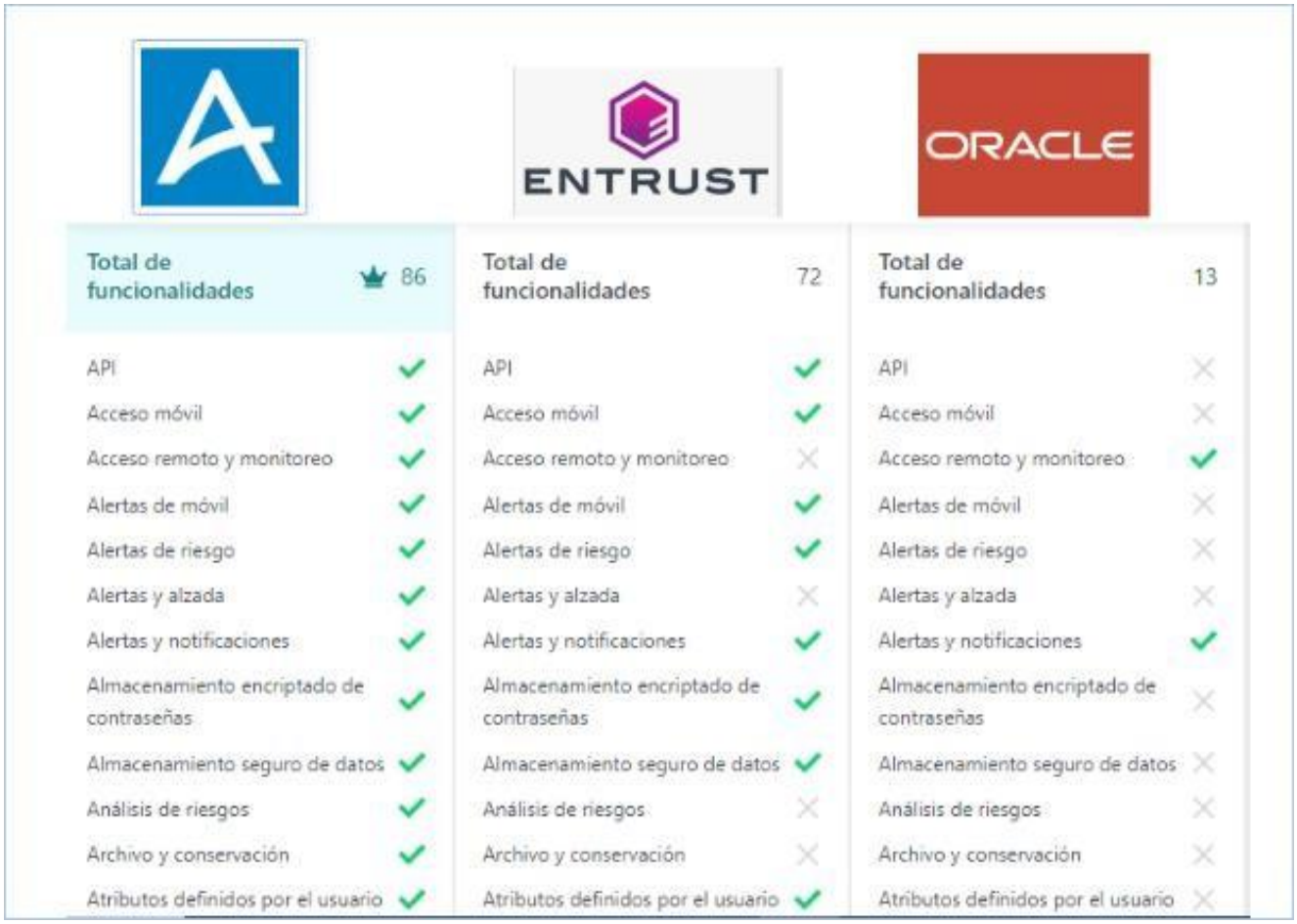
Fuente: Autor Propio

Respecto al cuadro comparativo se encuentran las siguientes diferencias considerable para un cambio de gestor de identidades con el cual se logre mitigar los errores previamente descritos a la hora de realizar la parametrización de los usuarios.

Figura 13. Comparativo compatibilidad y asistencia.

Fuente: GetApp Recomendadores de Software

Figura 14. Comparativo entre funcionalidades.



Fuente: GetApp Recomendadores de Software

Como se evidencia en los anteriores cuadros comparativos el gestor de identidades de Oracle (OIM) carece de funcionalidades, de integraciones con diferentes Softwares o sistemas y un limitado número de plataformas compatibles lo que nos conlleva a realizar un análisis de la deficiencia que tiene frente a otros Gestores de Identidades y Accesos (eBusiness, 2022).

Al analizar esta información como principal propuesta se debe migrar a otro gestor de identidades ya que al comparar el actual se evidencia que no tiene

suficientes funcionalidades compatibilidad y asistencia frente a otros por lo cual se propone implementar el gestor de identidades Avatier Identity Anywhere, este gestor proporciona como uno de sus objetivos primarios el acceso fácil y seguro a los aplicativos, activos y demás elementos de la empresa al requerir menos inicios de sesión mediante tecnologías como contenedores Docker o identidad como contenedor (IDaac) permite implementar este sistema rápidamente, es un sistema que se mantendrá en la nube (IDaaS) con mayor control del repositorio de identidad, mejor seguridad y flexibilidad con menores costos, por lo cual seria una mejora para el proceso de control de los accesos de los usuarios además que es implementable en un tiempo optimo como lo es 14 días (Avatier, 2022).

Esta empresa ofrece soluciones alojadas en las instalaciones o en la nube haciendo más versátil la idea de negocio y el acople a las empresas a su gusto, como uno de sus puntos a favor cuenta con diseño de respuesta sobre la gestión de identidad móvil para brindar soporte desde cualquier lugar, cualquier dispositivo las horas.

11.2 Análisis gestor Base de Datos.

La base de datos que utiliza la compañía actualmente es de tipo relacional de MySQL donde se accede mediante el gestor de Base de Datos Access versión 2013. La base de datos que está sobre el gestor de Access 2013 se denomina DPA que significa Documentación de Perfiles de Acceso, a esta base de datos

acceden con diferentes roles o permisos como lo son de tipo, diseñador, administrador y consultor.

El coordinador de Gobierno de identidades es el actual administrador de la base de datos DPA, los analistas de gestión de acceso, los analistas de seguridad informática y los aprendices pueden ingresar de modo consultor, pero también pueden realizar modificaciones sobre la información que se almacena de los perfiles, usuarios y roles.

La información que se maneja en la base datos es de alta sensibilidad por lo cual solo 17 personas pueden acceder a ella ya sea para consulta, modificación, depuración o creación de usuarios en el sistema, para la parametrización de los usuarios, las Unidades de Negocio como Alkomprar, Alkosto- Ktronix, Distribuciones, Corautos hacen la solicitud al grupo de gestión de accesos ya sea para actualizar, modificar o cambiar a los usuarios de perfil y los tipos de permiso que estos tienen por lo cual ellos deben informarse de los perfiles existentes dentro de la base de datos lo cual no se hace diariamente y como repercusión se ve un doble proceso y una suma de casos para los analistas y técnicos de gestión de accesos.

11.2.1 Interfaz Web no pública.

En el proceso de Gestión de accesos no se cuenta con una interfaz web pública de la base de datos DPA lo cual causa un gran retraso en las actividades diarias del área, ya que toda esta información que se almacena en la base de Datos DPA no está visible para las unidades de negocio, esta pérdida de información y de

recursos se podría mitigar al crear una Interfaz Web Pública conectada con la base de Datos donde los usuarios de la compañía tales como directores, líderes, coordinadores y supervisores accedieron a esta información para consultar los accesos, tipos de accesos y permisos de los empleados a su cargo, esto provocaría un menor índice de casos para el proceso de gestión de accesos y un mejor perfilamiento a la hora de los ingresos de los nuevos usuariosasignados a los perfiles solicitados por los usuarios descritos anteriormente.

11.2.2 Compatibilidad y recursividad del sistema Operativo.

La base de datos de MySQL tiene un bajo costo en requerimientos, un buen rendimiento y velocidad al realizar las operaciones, el cual soporta casi el 100% de los sistemas operativos ya que tiene flexibilidad con todas las versiones de Linux, Unix y Windows, es un sistema seguro dentro de los servidores en torno a la seguridad y encriptación de datos.

Este tipo de Software al ser de uso libre presenta desventajas como las soluciones para las deficiencias de software no estén documentadas ni sean de tipo oficial y la mayor desventaja es que no es eficaz en aplicaciones que requieran de una constante modificación de escritura en la Base de Datos.

Esta Base de datos de MySql al estar conectada con el Gestor Access 2013. da como resultado una mitigación en los sistemas operativos ya que solo acepta a Windows como el sistema operativo funcional, otro problema es que la información registrada en la base de datos se guarda en un solo archivo por lo cual realizar múltiples consultas ralentiza el proceso y su rendimiento se va debilitando, la

interfaz de Access no cuenta con un botón de actualización por lo que realizar consultas en la DPA se vuelve un proceso más largo y menos eficiente al cargar los datos de la base de datos, corriendo el riesgo que la información mostrada no sea la correcta.

Por lo anterior descrito se muestra el comparativo de los diferentes gestores de base de datos el cual se puede ajustar al proceso que requiere la compañía Colombiana de Comercio Corbeta S.A donde Oracle actualmente se posiciona como uno de los mejores en el mercado y es el recomendado para este cambio ya que es gestor multiplataforma, dispone de su propio lenguaje y es hecho para grandes compañías que requieran el acceso, modificación, almacenamiento y creación de muchos datos.

Figura 15. Comparativo Sistemas de Gestores Base de Datos.

SGBD	Características	Ventajas	Inconvenientes
ACCESS	Perteneciente a Microsoft. Es muy gráfico. Métodos simples y directos, con formularios, para trabajar con la información.	Asequible para personas con poco manejo con las bases de datos. Crea varias vistas para una misma información.	No es multiplataforma. No funciona con bases de datos grandes, tanto para registros como para usuarios.
SQLite	Los tipos de datos se asignan a valores individuales y no a la columna como la mayoría de los SGBD.	Multiplataforma. No requiere configuración. Acceso muy rápido. No requiere servidor.	El dinamismo de los datos hace que no se portable a otras bases de datos. Falta de clave foráneas.
SQL SERVER	Software propietario. El lenguaje es TSQL.	Multiplataforma, aunque pertenezca a Microsoft. Transacciones.	Utiliza mucha RAM. Tamaño de página fijo y pequeño. Relación calidad/precio inferior a Oracle.
MYSQL	Pertenece a Oracle. Licencia GPL/Licencia comercial.	Agrupación de transacciones. Distintos motores de almacenamiento. Instalación sencilla.	No tiene soporte. Capacidad limitada.
POSTGRESQL	Tiene la extensión POSTGIS para bases de datos espaciales.	Código abierto y gratuito, multiplataforma. Gran volumen de datos. Transacciones, disparadores y afirmaciones.	Respuesta lenta. Requiere hardware. No es intuitivo.
ORACLE	Dispone de su propio lenguaje PL/SQL. Soporta bases de datos de gran tamaño.	Es el más usado a nivel mundial. Multiplataforma. Es intuitiva y fácil de usar.	Precio muy elevado. Elevado coste de la información, tratado por trabajadores formados por Oracle.

Fuente: Grupo TYC GIS - Asesoría Técnica de Softwares.

11.2.3 Migración de BD local a la Nube.

Una Base de Datos en la nube a diferencia de una local es que la BD en la nube no se almacena en un equipo o sistema local, su ejecución se realiza por medio de una infraestructura de los actuales proveedores de servicios en la nube.

Hay dos formas de tener una base de datos en la nube o también llamada DBaaS (DataBase as a Service) la primera es gestionar la información almacenada por medio de un proveedor de servicios de infraestructura física, la segunda es donde el proveedor ofrece la infraestructura física, la base de datos y la gestión integral del contenido almacenado.

Las ventajas que se obtendrían al Migrar la Base de Datos a la Nube es la escalabilidad ya que se pueden aumentar los recursos y el almacenamiento de los datos ya que la empresa requiere una gran cantidad de almacenamiento de información, al estar migrado a la nube la integridad de los datos se puede mantener ya que la réplica de información es instantánea por ende se visualizan los cambios de manera más segura, el ahorro de espacio físico también es una ventaja de tener la base de datos en la nube.

Uno de los fallos más comunes que ocurren en la compañía es la conexión a escritorios remotos lo cual nos hace imposible acceder a la base de datos, con la base de datos en la nube se puede acceder desde cualquier dispositivo solo con la conexión a internet y las credenciales de acceso lo cual ofrecería una opción muy viable para esta falencia y tener una optimización de trabajo aún mayor.

11.3 Implementación de Buenas Prácticas de seguridad

Primordialmente se debe unificar las políticas de contraseña ya que hay algunas que no aceptan caracteres especiales, ni letras solo números lo cual hace más vulnerable el acceso de estas credenciales, una buena contraseña debe tener las siguientes recomendaciones:

- Contar con al menos 12 caracteres
- Tener mayúsculas y minúsculas, números y símbolos.
- No admitir lugares ni nombres propios,
- No admitir nombres de equipos de futbol
- Contener al menos 2 Mayúsculas, 2 minúsculas, 2 caracteres y 2 números.
- No ser mayor a 16 caracteres
- No tener números consecutivos como 1234.

Actualmente no se cuenta con un generador de contraseñas lo cual hace más difícil la entrega de más de 40 credenciales diarias por lo cual muchas veces se repiten las mismas credenciales no cumpliendo con las buenas prácticas de seguridad, pero a grandes rasgos comenzar por contraseñas privilegiadas y centralizadas sería la mejor opción.

Se deberían dar cursos de buen manejo de las credenciales como también enseñar las vulnerabilidades o ataques más comunes como lo son La ingeniería

Social, el Phishing y spear phishing como obligación a cada uno de los usuarios ya que estos son la principal fuente de vulnerabilidad.

Gestionar que cada uno de los usuarios tenga restricciones a páginas web que puedan contener virus, o malwares que afecten la integridad de los activos de la compañía esto se realiza con los proxys y los niveles de internet para cada uno de los usuarios.

Tener un gestor de contraseñas significa tener las credenciales bajo gestión lo cual mitiga el almacenamiento en el cache del navegador y así mismo el auto rellenó de las credenciales en los aplicativos, ya que esta es una vulnerabilidad del Top 10 de las afectaciones a la seguridad de la información.

12 Mitigación de vulnerabilidades y perdida de información

En la investigación realizada a continuación describiremos las 10 vulnerabilidades que toda empresa debe tener presente ya que son las más populares actualmente utilizadas por los hackers, Tener buenas políticas de seguridad, antivirus, redes seguras ayudan a mitigar estos riesgos de seguridad informática así mismo como promover el buen uso de los aplicativos o recursos de la empresa son parte de las buenas prácticas, que como usuarios se deben seguir para evitar este tipo de vulnerabilidades, los cuales pueden ser de gran afectación para cualquier empresa ya que hablando a grandes rasgos la perdida de información altamente sensible, la corrupción de información por parte de terceros

entre otros (OWASP, 2017)

12.1 inyección

La primera vulnerabilidad o agente de amenaza es la Inyección la cual puede utilizar cualquier fuente de datos como un vector de datos hostiles, estas inyecciones aplicadas a consultas SQL, LDAP, XPATH Y NoSQL, comandos de sistema operativo, consultas ORM entre otras, este tipo de afectación causa perdidas de información, perdidas de acceso o adquisición completa al host por terceros (OWASP, 2017).

Es muy importante el acceso a los aplicativos ya que son la principal fuente de ataque en una compañía siempre hay 3 tipos de escenarios el primero es un nuevo aplicativo, el segundo un aplicativo de código abierto y el tercero un aplicativo de código cerrado. La mayoría de los aplicativos de la empresa se encuentran conectados con el LDAP el cual se encarga de dar acceso mediante las mismas credenciales que otorga la compañía una vez ingresa al sistema en este caso el directorio activo con el cual se ve evidenciada la primera vulnerabilidad frente a este tipo de acceso.

La compañía Colombiana de Comercio Corbeta S.A.S implementa dentro de sus policitas de seguridad como prevención un escaneo de vulnerabilidades mediante Acunetix la cual es una herramienta de prueba de seguridad de aplicaciones dinámicas con la cual se mitigan estos riesgos a nivel web.

12.2. Autenticación Rota

Como su nombre lo indica hablamos de un ataque a la confirmación de identidad de usuario, autenticación y administración de sesión en los diferentes activos de la compañía, Una de sus principales formas de ataque es cuando los aplicativos permiten el relleno de credenciales automáticamente, tipos de contraseñas predeterminadas, recuperación de credenciales débiles basadas en respuestas de conocimiento. Actualmente la mayoría de los aplicativos maneja una sola credencial la cual se autentica con LDAP y está conectada al directorio activo de la compañía, muchas de las páginas web permiten el auto relleno de información, su autogestión y son contraseñas débiles ya que acepta lugares, nombres predecibles de los usuarios, y no cuenta actualmente con una autenticación multifunción la cual brinda una mitigación de vulnerabilidad al robo de identidad o suplantación (OWASP, 2017).

La mayoría de las empresas utilizan actualmente este método de autenticación doble o multifunción a través de un correo de verificación, mensaje de texto, código de verificación en los celulares o llamadas de identificación como por ejemplo las de Microsoft, por lo cual se debería autenticar los usuarios de la compañía con este nuevo sistema para mitigar este tipo de vulnerabilidad presente en la empresa como también el cierre de sesión después de inactividad y el bloqueo de usuario después de tres intentos son las primeras medidas que debería tomar la compañía en el área de seguridad informática.

12.3 Exposición de datos confidenciales

Esta vulnerabilidad hace referencia a información disponible altamente sensible para el uso de uno o más interesados a través de un sitio web o un recurso de red, esta exposición ocurre cuando se envían los datos a través del correo electrónico lo cual podría asegurar un robo de identidad , en la compañía Corbeta S.A.S se realiza la solicitud de credenciales mediante correo lo cual es inseguro y está expuesto a este tipo de vulnerabilidad, además de lo mencionado anteriormente se pueden guardar las credenciales en el navegador y esto puede ser expuesto ya que muchas de las aplicaciones funcionan sin necesidad de estar conectado a la VPN lo que hace que se expongan más este tipo de información (OWASP, 2017).

Como primera medida la Compañía debería mejorar las políticas de contraseñas como un generador de contraseñas altamente seguro para los usuarios que reciben sus primeras credenciales de acceso por parte de los técnicos de Gestión de Acceso, los aplicativos no deberían almacenar este tipo de contraseñas y no deberían permitir el auto relleno, Los usuarios que manejan distintos accesos a los aplicativos deberían contar con un gestor de contraseñas proporcionado por la compañía lo cual mitigue el riesgo de guardar esta información en el cache, también los aplicativos web no deberían estar expuestos ni funcionar sin la autenticación de las credenciales en la VPN, y utilizar un doble autenticador.

12.4 Entidades Externas XML

También llamadas Inyección de entidad externa este tipo de vulnerabilidad se trata de un ataque contra un aplicativo que analiza la entrada XML llamada entidad externa y se utiliza para acceder a contenido local o remoto con una URL el cual apunta a modificar el código en un sistema de archivo local y remplazar cualquier referencia en el documento con un contenido, aparte de leer archivos del sistema, los atacantes inician escaneo de puertos cambiando la URL de otra entidad con la finalidad de encontrar máquinas o servicios vulnerables.

La compañía Colombiana de Comercio Corbeta S.A.S cuenta con dos analistas de seguridad informática en la sede de Bogotá donde ellos realizan el escaneo de vulnerabilidades y son los encargados del parchado de sistema operativo de toda la compañía, donde realizan alrededor de dos escaneos por año, en donde son más de 20mil tipos de vulnerabilidades que deben remediar por lo cual el recurso es muy poco y muchas veces no alcanzan a parchar los sistemas ni a remediar las vulnerabilidades ya que no cuentan con un sistema de remediación en caso de fallas de servidores esto hace que sea más propenso a estas vulnerabilidades previamente descritas.

12.5 Control de Acceso Roto

Esta vulnerabilidad trata del tipo de acceso que tienen los usuarios en los activos de la compañía, estos accesos incluyen la modificación de URL, el acceso a información y divulgación no autorizado, modificación y destrucción de datos, actuar como administrador ingresando como con permisos de usuario a los aplicativos, forzar el acceso a páginas web autenticadas como usuarios no autenticados.

A diferencia de ACUNETIX, Una de las plataformas que mitiga este riesgo es Tenable o Nessus que son herramientas de escaneo de vulnerabilidades y los cuales abordan el riesgo en el directorio activo quien es la mayor fuente de información de toda la compañía Corbeta S.A.S la cual interrumpe las rutas de atacantes, estas plataformas las manejan diferentes empresas que se dedican a la remediación de vulnerabilidades, Hardening de sistemas operativos y bases de datos, y remediación de vulnerabilidades como por ejemplo IT SECURITY SERVICE esta empresa cuenta con un SOC de remediación y un gran plan de trabajo para los servidores que maneje cualquier empresa ya sea de cualquier sistema operativo.

12.6 Configuración Incorrecta de seguridad

Esta vulnerabilidad se ve reflejada cuando hay fallas en los parches de seguridad o acceder a cuentas predeterminadas, páginas web no utilizadas, archivos y directorios desprotegidos con el fin de obtener acceso no autorizado o conocimiento del sistema. La configuración incorrecta puede vulnerar cualquier nivel depila de los aplicativos. Como se ha descrito en las vulnerabilidades el no parchar un sistema operativo deja expuesto a muchos tipos de vulnerabilidades y este es uno de ellos, el área de Seguridad informática no está lo suficientemente formado como para tener prevención de estos ataques a los activos de la compañía una gran solución sería contar con un externo que este altamente calificado para la remediación de vulnerabilidades y ataques informáticos, como bien sabemos no hay un sistema totalmente seguro pero si se puede lograr un sistema altamente fortificado.

12.7 Secuencias de comandos entre sitios.

Tener herramientas automatizadas pueden detectar y explotar las tres formas de vulnerabilidad la primera XSS reflejado la cual incluye entradas no validas de los usuarios sin escape como parte de la salida HTML la vulnerabilidad

consiste en un ataque ejecutable de HTML y JavaScript al navegador mediante sitios maliciosos, XSS almacenado es otra forma en la cual la aplicación almacena la entrada del usuario que otra persona puede ver más tarde, y el ultimo Dom XSS los cuales son el robo de sesión, apropiarse de cuentas, suplantación, software malicioso, registro de claves entre otros.

En la compañía deberían implementar para la mitigación de estas vulnerabilidades los cursos interactivos de adaptación de los posibles ataques informáticos ya sea como no descargar ejecutables de correos ya que pueden traer un virus malicioso, detectar el phishing y no caer en esta modalidad, como el robo de credenciales las cuales deben entregársele al usuario de manera que entienda la gravedad de compartirlas o dejarlas visibles a los compañeros o en sitios no autorizados de la compañía, al igual que no guardar credenciales en el navegador, por otro lado la compañía no debería permitir el uso de usuarios genéricos con el cual varios usuarios accedan por medio de unas credenciales a una cuenta compartida.

12.8 Deserialización Insegura

Es la vulnerabilidad de tipo industrial donde buscan deserializar los objetos hostiles o manipular las estructuras de datos y logra ejecutar un código remoto arbitrario, otro ataque es hacia el control de acceso en los que se cambian los contenidos esta serialización utiliza comunicación remota y entre procesos, protocolos de conexión, almacenamiento de cache, base de datos y cookies, como

parte de la parametrización de usuarios en aplicativos las medidas que se tienen en cuenta son la certificaciones de las páginas web, la asociación al directorio activo lo cual asegura o mitiga estas vulnerabilidades por parte del usuario ya que los inactiva en los periodos de vacaciones, o al terminar contrato para no permitir el acceso no autorizado pero como se ha descrito anteriormente muchas aplicaciones web no están conectadas al gestor de identidades lo cual genera mas vulnerabilidades en los accesos de los usuarios. Por lo cual es importante que todos los aplicativos estén conectados a este directorio para mejorar el acceso y tener la información de forma más segura, un punto a favor que tiene la compañía es el monitoreo de la conectividad de red ya que solo soporte puede configurar las VPN en ciertos equipos.

12.9 Uso de componentes con vulnerabilidades conocidas

Estas vulnerabilidades son la sumatoria de varios componentes como lo son los activos por parte del cliente con el cual pueden acceder a los sistemas de la compañía, un software vulnerable no actualizado, el gestor de base de datos, y todos los componentes que hagan parte de los activos de la compañía, no realizar escaneos de vulnerabilidades, no tener aseguramiento de sistemas operativos o bases de datos, todos estos problemas de seguridad se deben remediar y es posible su aseguramiento con un escaneo mensual o trimestral que se realice sobre todos los servidores, firewalls, aplicativos, bases de datos, así mismo como la depuración de información y administración de parches y utilizar solo componentes de fuentes oficiales para esto es importante las restricciones a la hora de

parametrizar un usuario ya que no se deben tener acceso a otro tipo de aplicativos que no correspondan a los certificados por la compañía.

12.10 Registro y monitoreo insuficientes

Explotar un riesgo latente y la supervisión insuficiente es la base de casi todos los incidentes importantes, un ataque exitoso comienza con un escaneo de vulnerabilidades donde les permita de varias formas el acceso ya sea a los activos, al host, a los servidores, a la información crítica o confidenciales y al robo de identidad, teniendo una explotación exitosa mediante este sondeo.

Tener alertas de inicios de sesión donde se verifiquen el número de intentos, ubicación y red son importantes a la hora de prevenir estos riesgos ya que un buen monitoreo conlleva a una buena práctica de seguridad, por lo cual después de describir cada una de estas vulnerabilidades se concluye que la cantidad de vulnerabilidades es inmensa y que una empresa que no preste atención a la parte de seguridad informática está en riesgo de explotación por parte de los hackers, como se describió en varias ocasiones la empresa Colombiana de Comercio Corbeta S.A.S no cuenta con el suficiente personal para remediar las vulnerabilidades que se presentan en todo el año en los diferentes activos, son más de 80 aplicaciones y softwares que remediar y dos escaneos al año no son suficiente por lo cual la compañía debería contratar personal altamente calificado para el aseguramiento y remediación de vulnerabilidades del sistema operativo y bases de datos.

Conclusiones

En definitiva y de acuerdo con las prácticas empresariales realizadas en la empresa Corbeta de Colombia S.A. se logra enriquecer el proceso formativo adquirido aportando conocimientos, destrezas y habilidades.

La propuesta de una mejora en la parametrización de usuarios frente a los accesos en los diferentes aplicativos que son manipulados por más de 14 mil empleados ayudan como parte funcional y primordial en el sector empresarial, destacando solicitudes constantes que realiza un usuario en su labor, como caso puntual en el área de seguridad informática, en el cargo de analista y la interacción que se tiene con el gestor de automatización para la parametrización de usuarios donde se presentan solicitudes y/o casos constantes que se hacen extensos e incrementar el tiempo y afectaba la disponibilidad de los datos y el cronograma laboral.

Esta investigación frente a la automatización de estos procesos diarios se evidencia que generaría una menor carga operativa para los analistas y mejora en cuanto a la integridad de los datos y disponibilidad frente a la parametrización de los usuarios, la excesiva acumulación de tareas y novedades, lo errores de creaciones masivas de perfiles y usuarios asignados a estos, el tiempo de espera frente a la documentación y consultas, entre otras muchas.

Por consiguiente, con base en la estadística y analizando los datos de prioridad se evidencia que la cantidad de solicitudes de cualquier tipo para su validación y gestión de una solicitud se debe realizar en un tiempo muy corto con el cual se logre cumplir los ANS que exige la compañía esto genera que no se realicen las validaciones pertinentes a la hora de dar un acceso a cualquier activo de la empresa por ende sin buenas prácticas de seguridad se estará propenso a vulnerabilidades.

Se concluye que sin un área que remedie las diferentes vulnerabilidades la afectación podría ser de tipo critica tanto para la compañía como clientes ya que la información que suministran las bases de datos de la compañía tiene datos con los cuales se puede realizar suplantación de clientes o empleados lo cual puede concluir en robos para la empresa o clientes.

Recomendaciones

Como ente de recomendaciones a posibles usuarios que continúen esta propuesta en el proceso de parametrización, frente a disponibilidad de los usuarios en las herramientas y aplicativos de la compañía aportando al mejoramiento continuo de los procesos, para que se ejecuten con eficiencia y eficacia. Por consiguiente, brindar una capacitación oportuna de los clientes solicitantes, para entender su función. Además, entregar el prototipo ingenieril y de esta manera exigir el desarrollo o reestructuración del gestor mitigando pérdida de información y disponibilidad en los accesos de los aplicativos.

Bibliografía

Download. (24 de sep de 2017). EasyFit 5.0. Obtenido de EasyFit 5.0: https://www.download3k.es/Negocios-y-Finanzas/Calculadoras-y-conversores/Download-EasyFit.html#page

eBusiness, N. (15 de ENERO de 2022). getapp. Obtenido de getapp: https://www.getapp.com.co/compare/114195/121159/avatier-identity-anywhere/vs/intellitrust?vs[]=121190#

EKCIT. (07 de Septiembre de 2019). Obtenido de Tic.Portal: https://www.ticportal.es/glosario-tic/base-datos-database

EL CONGRESO DE COLOMBIA . (25 de 08 de 2020). LEY 2052 DEL 25 DE AGOSTO DE 2020. Obtenido de LEY 2052 DEL 25 DE AGOSTO DE 2020: https://dapre.presidencia.gov.co/normativa/normativa/LEY%202052%20DEL%2025%20DE%20AGOSTO%20DE%202020.pdf

Hammer, M. (2001). REENGINEERING THE CORPORATION. New York : HarperCollins.

Hosting. (24 de Enero de 2019). hostingpedia. Obtenido de hostingpedia: https://hostingpedia.net/mysql.html

https://hostingpedia.net/mysql.html. (s.f.). https://hostingpedia.net/mysql.html. Obtenido de https://hostingpedia.net/mysql.html

IBM. (2020). Obtenido de IBM : https://www.ibm.com/downloads/cas/EAPLKO96 Instituto Tecnologico De Pachuca. (12 de Marzo de 2010). Numeros Pseudoaleatorios. Obtenido de Numeros Pseudoaleatorios: https://es.slideshare.net/iorifoar/numeros-pseudoaleatorios

MEDISAN. (07 de 2019). Mi SciELO. Obtenido de Mi SciELO: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1029-30192019000300534#:~:text=Las%20t%C3%A9cnicas%20estad%C3%ADsticas%20constituyen%20las,hist%C3%B3rica%20de%20las%20t%C3%A9cnicas%20y

Métodos de Análisis Estadístico. (12 de 09 de 2018). Proyectos en Gestión del Conocimiento. Obtenido de Proyectos en Gestión del Conocimiento: https://www.pgconocimiento.com/metodos-de-analisis-estadistico/

Pérez Porto, J., & Merino, M. (2021). Definiciones. Obtenido de Definiciones: https://definicion.de/grafico/

Política de respaldo, custodia y recuperación de la informacion. (17 de 05 de 2019). Proceso Tecnologías de la Información . Obtenido de Proceso Tecnologías de la Información: https://www.funcionpublica.gov.co/documents/34645357/34703081/Politicas_respaldo_custodia_informacion.pdf/cdadd3ea-31f5-4154-be6a-f8227b3cc47e?t=1544198825391

Avatier. (2022). identity & access management (IAM) solutions. Obtenido de identity & access management (IAM) solutions: https://www.avatier.com/products/identity-management/

OWASP. (2017). OWASP. Obtenido de OWASP: https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring

SISCOOP. (12 de 04 de 2010). Especificación de requisitos de software. Obtenido de Especificación de requisitos de software: http://dspace.espoch.edu.ec/bitstream/123456789/188/1/EspecificacionRequerimientosSoftware.pdf