Diseño y definición de controles informáticos para una arquitectura de seguridad en un centro alterno de operaciones -CAO-

Juan Carlos Espinosa Cordero, Gilberto Florez Gualacon,
y David Rodríguez Saavedra

Resumen - Las empresas que tienen como objetivo del negocio ofrecer servicios a un tercero, deben identificar la manera de mantener sus servicios siempre funcionales para no perder el costo de oportunidad frente a sus usuarios. Una de las formas en las que se pueden apoyar esta estrategia es por medio de un plan de continuidad en el negocio, que sea rentable para la empresa y que mantenga todas las condiciones de seguridad de la información como los que se tienen en la operación tecnológica principal. Para el desarrollo de este proyecto se identificaron cuatro posibles soluciones tecnológicas que podrían mejorar la solución actual del centro alterno de operaciones (CAO). Así mismo se plantearon tres metodologías de proyectos para desarrollar esta propuesta, donde la que mejor se adapta es la metodología TOGAF. En este artículo se desarrollarán las fases de esta metodología indicando los pasos a seguir para llevar a cabo el diseño de la solución tecnológica identificada.

I. INTRODUCCIÓN

La compañía es una empresa del sector financiero que presta servicios a sus clientes como comisionista de bolsa de valores con todo un portafolio de inversión bursátil. La empresa cuenta con alrededor de 700 colaboradores, 5.000 a nivel grupo en todo Colombia y unos 116.524 clientes. La Superintendencia Financiera de Colombia (SFC) es el organismo de control encargado de vigilar la compañía, por lo que se debe dar obligatorio cumplimiento a las diferentes circulares normativas que ellos emiten. Con base en eso, la empresa como uno de varios controles, dispone de un Centro de Operaciones Alterno (CAO), que cuenta con una capacidad operativa para 120 personas de las áreas críticas de la compañía (identificadas en el Análisis de impacto en el negocio; BIA), con el objetivo de centralizar, asegurar, y dar mayor confidencialidad de información, no obstante, solo se ha utilizado en tres ocasiones durante los últimos 10 años, lo que genera un detrimento económico y una subutilización de activos informáticos, adicionalmente, existe una alta probabilidad de ataques cibernéticos y pérdida de información crítica de la empresa.

II. PROBLEMÁTICA ACTUAL

En la circular básica jurídica de la SFC 029, capítulo IV: Sistema de control interno, numeral 4.2.6, indica que "Implementar, probar y mantener un proceso para administrar la continuidad de la operación de la entidad, que incluya elementos como: prevención y atención de emergencias, administración de crisis, planes de contingencia para responder a las fallas e interrupciones específicas de un sistema o proceso, y capacidad de retorno a la operación normal." Motivo por el cual la compañía decidió implementar un CAO y dar control al riesgo de interrupción de la operación, más cuando el mercado bursátil es tan dinámico.

La estrategia que se adoptó en su momento fue ideal para el tiempo en el que se generó el control, pero a medida que ha pasado el tiempo y con la llegada de nuevas tecnologías, se ha evidenciado la ausencia de una arquitectura de TI que dé cumplimiento a las buenas prácticas de seguridad de la información, generando vulnerabilidades a los procesos críticos de la organización, lo cual requiere un rediseño que esté alineado a la estrategia del plan de recuperación de desastres (DRP por sus siglas en inglés). Adicionalmente el costo de mantenimiento del CAO en la actualidad anualmente es de 1.000 millones de pesos, por lo que se debe replantear la estrategia del control o idear una nueva configuración al CAO existente.

Desde el área de seguridad de la información se ha informado a la organización que se debe pensar en una estrategia de rediseño del CAO teniendo en cuenta opciones como una actualización tecnológica o pensar en conceptos como la implementación de ambientes híbridos o en nube, teniendo en cuenta que para esta última opción se debe dar cumplimiento de manera adicional a la circular básica jurídica 005 "servicios de computación en la nube" y que de continuar con el CAO actual, se debería invertir en diferentes controles tecnológicos para poder asegurar los canales de comunicación, transporte de la información y el apetito de riesgo de la compañía.

III. METODOLOGÍA

A. *Planteamiento de la propuesta*

La compañía deberá realizar un nuevo estudio de Análisis de impacto en el negocio (BIA, por sus siglas en inglés), con el fin de validar la información, procesos y roles que actualmente están definidos como estratégicos y determinar si se mantienen o existen variaciones en el alcance actual del CAO y así poder dimensionar una estrategia que corresponda a las necesidades requeridas. Con base en ese análisis se realizará una propuesta para la implementación de un nuevo CAO que ofrezca el mismo servicio de una manera segura, buscando maximizar su uso y bajando los costos actuales de mantenimiento.

La propuesta a realizar deberá tener como uno de sus beneficios, el uso de los recursos tecnológicos del CAO para usos como el teletrabajo y así generar un valor agregado a este control.

La estrategia deberá analizar diferentes frentes como el costo beneficio para la compañía, en el que se pueda establecer un equilibrio dentro de lo funcional, que sea económicamente viable y donde la información de la empresa esté salvaguardada con los estándares definidos por la misma.

B. *Análisis de Diseño*

El alcance de seguridad de la información en el proyecto es apoyar la elección de la solución tecnológica para implementar una arquitectura de seguridad que mitigue riesgos cibernéticos identificados. Dentro del análisis realizado se identifican controles de seguridad en el perímetro y en los escritorios virtuales con el fin de proteger a la compañía de riesgos como ataques de ransomware, virus, fuga de información, movimientos laterales por un atacante, todo los anterior teniendo en cuenta el apetito de riesgo y la funcionalidad de la solución, llegando desde la definición e implementación de controles en la arquitectura en nube privada o pública y velando por el cumplimiento de las normativas de las entidades que vigilan a la empresa y a las mejores prácticas del sector para asegurar el perímetro y los repositorios que guardan y procesan información.

La ejecución de la implementación se realizará con base en la metodología propuesta.

1) *Fase A - Definición de la visión de la arquitectura*

De acuerdo con el marco de referencia seleccionado (TOGAF), en esta fase se coloca la arquitectura de seguridad a alto nivel, lo que, de acuerdo con lo esperado, sería de la siguiente manera (Figura 1):

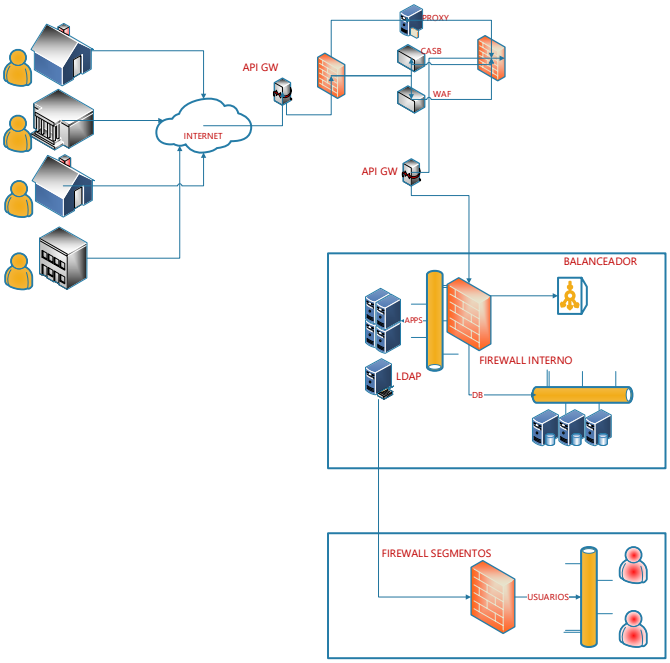

Fig 1. Diseño de arquitectura en nube. Fuente: Elaboración Propia

La arquitectura de seguridad estará alineada con la mitigación de riesgos identificados a nivel reputacional, de confidencialidad, integridad y disponibilidad, basados en un esquema de Software as a Service (SaaS) con el proveedor de servicios seleccionado, es decir que el soporte y administración está cubierta en el contrato. Con base en eso, se realizará un despliegue para virtualizar los escritorios (Desktop as a Service, DaaS) de los funcionarios críticos de la entidad donde tendrán enlaces punto a punto con proveedores relevantes para la compañía y con el centro de datos que se encuentra OnPremise (se consumen servicios in House).

El usuario se autentica contra el directorio activo (AD) local de la compañía, lo que implica que se tendrá un canal de comunicación dedicado entre la nube y la entidad para que el flujo siempre tenga que comparar el hash de la credencial con el que se tiene en el AD; una vez se compara, el AD OnPremise validará la respuesta, si es un 1, la credencial corresponde, si es 0 el portal le pedirá que vuelva a digitar la credencial.

La arquitectura contempla la migración de la información que se encuentra en los computadores físicos de la empresa, por lo que se realizará una gestión de cifrado de la data en horas no productivas para no afectar el rendimiento del canal y obtener una experiencia del usuario transparente.

2) Fase B - Evaluación de la arquitectura empresarial

La arquitectura empresarial es el proceso que busca llevar a la empresa a un cambio de su visión y estrategia mediante la mejora de procesos claves que conllevan a una mejora continua con el uso de la tecnología. En este caso se revisará el proceso de continuidad en el negocio haciendo énfasis en el procedimiento del centro alterno de operaciones y los controles de seguridad que se deben desarrollar para proteger la información de los procesos claves de la compañía.

Estrategia

La estrategia que se va a implementar en la arquitectura de seguridad en ambientes Cloud, será como DaaS (escritorio como servicio) lo que conlleva a una tercerización de la plataforma tecnológica donde los administradores de la compañía solo tendrán privilegios a la información y algunas reglas de monitoreo; El proveedor de servicios será el encargado de la administración de la tecnología, esto indica que este servicio incluye la gestión de vulnerabilidades, aplicación de parches, esquema de disponibilidad, actualizaciones y soporte. Este tipo de servicios ofrecen un indicador de cumplimiento del 99.99% valor que corresponde a la expectativa de disponibilidad que la compañía necesita en caso de requerir hacer uso del CAO.

Uno de los riesgos identificados en este esquema, es la dependencia generada con el tercero dado que todo el servicio estará en su infraestructura, reto que se deberá administrar por medio de cláusulas contractuales y cifrando la información con una llave privada, esto indica que ante un eventual fin de contrato se le daría muerte digital a la información que repose en el tercero porque no tienen acceso a ella.

Calidad

Una arquitectura en nube ofrece un esquema de servicio robusto puesto que los proveedores de servicio que ofrecen esta tecnología tienen un esquema maduro de implementación en data center con niveles de servicio con certificaciones SOC. Estos esquemas tienen altos esquemas de calidad porque continuamente están renovando su infraestructura tecnológica dado que este es el core de su negocio.

Organización

La compañía inicialmente dará uso al proyecto para los temas de cumplimiento y uso del CAO, pero en una segunda fase de adaptación se dará paso al esquema de teletrabajo haciendo uso de los escritorios virtuales y la facilidad para desplegar y asignar un activo a un empleado nuevo.

Esta modalidad de servicio le generará a la empresa una mejor calificación en la calidad de trabajo de los colaboradores de la compañía que se verá reflejado en la calidad de servicio a sus clientes finales, ofreciendo un esquema vanguardista de trabajo desde casa y con los mejores estándares de seguridad de la información para evitar la materialización de riesgos que afecten a la organización.

Procesos

Este proyecto está apoyando directamente el proceso de continuidad en el negocio de la compañía haciendo énfasis que no apoya la estrategia de disponibilidad de la información sino el proceso de acceso a la información generando espacios alternos a la sede principal con el fin que los procesos identificados en el BIA puedan seguir operando.

Las reglas de negocio para poder hacer uso de los escritorios virtuales en la primera fase de implementación son para uso exclusivo del proceso que activa el CAO, los usuarios que tendrán acceso a los escritorios son aquellos roles identificados como críticos y tendrán acceso controlado a la información, aplicaciones y navegación a internet igual a como los tiene definidos en la sede principal.

El CAO como servicio será activado cuando el árbol de llamadas del proceso de continuidad en el negocio se active y notifique a los roles críticos de la organización que debe trabajar en su escritorio virtual designado dado que se está presentando un evento no deseado en las instalaciones de la compañía.

Información

La información a la que puede acceder el usuario desde el CAO será la misma a la que tiene acceso desde la sede principal, es decir, los escritorios virtuales en nube estarán configurados para llegar al Data Center de la compañía y generar una experiencia transparente para el usuario, por lo que las labores que realizará desde el escritorio virtual serán las mismas que las que hace desde la sede principal de la empresa.

Los usuarios que utilizan la información que se aloja en el centro de datos de la empresa para generar informes y demás entregables y que posteriormente guardan en el PC virtual, no se tendrán que enviar a ningún repositorio externo para seguirlo trabajando desde la sede física de la empresa, puesto que los escritorios virtuales tendrán un agente de sincronización con el sharepoint de su proceso, es decir, la información queda replicada en la nube de la compañía y en el escritorio virtual.

Los escritorios virtuales cuentan con controles informáticos para que el usuario no pueda enviar información a cuentas propias, no permita descargas y tenga acceso a navegación controlada para que no se presenten casos de fugas de información.

Aplicaciones

Los sistemas de información a los que tendrá acceso el usuario se presentarán por medio de un portal similar a una tienda de aplicaciones, los usuarios están configurados en unidades organizaciones (OU) que definen los accesos permitidos, por lo que un usuario podrá revisar acceso a

aplicaciones ofimáticas, de negocio y de gestión.

Tecnología

El proyecto se implementará en ambientes cloud bajo modalidad de DaaS donde se generará un esquema de autenticación contra el directorio activo comparando el hash que se digita en el portal de acceso con el AD OnPremise, (cuando el usuario digita la clave en el portal se ejecuta una función que genera el hash de cifrado, envía la información por medio del canal configurado Firewall to Firewall, generando dos controles de seguridad, tanto en el túnel como enviando la información cifrada), si el hash de la credencial corresponde con el hash que se encuentra en el AD, se devuelve un 1 como respuesta y el usuario podrá acceder a su escritorio, si por el contrario el hash no corresponde, se devolverá un 0 como respuesta y un mensaje al usuario para que vuelva a digitar hasta por un máximo de tres veces (a la tercera vez el usuario se bloqueará).

Toda la infraestructura desplegada para la implementación de los escritorios la provee el proveedor de servicios, es decir que las capas de servidores, base de datos y el front es administrada y controlada por el tercero, del lado de la compañía se administrarán accesos, usuarios y reglas de negocio.

Las comunicaciones contra el Data Center OnPremise de la compañía y contra los terceros claves de negocio estarán implementados por canales redundantes, uno por medio de firewall to firewall y el otro por Ipsec, cada uno con un proveedor de servicios diferente.

El sistema operativo que se instalará en los escritorios virtuales será Windows 11, navegador de internet predeterminado Google Chrome, agentes de seguridad como data loss prevention (DLP), Endpoint detection and response (EDR) y Host intrusion prevention System (HIPS), sin ser estos los únicos.

3) Fase C - Desarrollo de arquitecturas de sistemas de información

Tal como se ha planteado, la propuesta definida en el proyecto es redefinir el CAO que se tiene actualmente y plantear una solución que mejore las características de seguridad, rendimiento y disponibilidad, en este orden de ideas, es posible asegurar que el flujo de información y el manejo de los datos se maneja de forma centralizada en el centro de datos de la organización, por lo tanto, la arquitectura de datos no se modifica. La arquitectura de aplicaciones se convierte en un reto importante debido a que el escenario de conexión que se plantea define el uso de aplicaciones específicas que le permitan al usuario tener una experiencia de escritorio remoto virtual desde cualquier ubicación que cuente con una conexión a internet. Este escritorio remoto virtual se genera en la nube del operador y realiza una conexión segura hacia todos los servicios que ofrece el centro de datos principal de la organización, de forma tal, que el usuario pueda consumir todos los servicios y aplicaciones de red que le permita su cuenta de usuario registrada en el directorio activo de la organización, sin la necesidad de que el escritorio remoto esté ubicado en la red corporativa de la organización, como se detalla en la Figura 2.

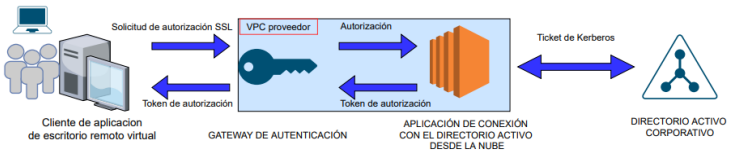

Fig. 2. Diagrama del proceso de autenticación del usuario con el CAO en nube. Fuente: Elaboración Propia

Proveedor de servicios de nube

Las diferentes soluciones de nube que se encuentran definidas en el mercado, indican que se pueden implementar opciones públicas y privadas, a continuación, se relacionan algunos términos:

Nube privada virtual (VPC): Tener la posibilidad de configurar una nube privada virtual con al menos dos segmentos de red.

- DHCP: Servicios de asignación dinámica de direcciones que permiten la conexión de red de los escritorios remotos virtuales.
- AD corporativo: Réplica de directorio activo corporativo.
- Gateway de autenticación: Ofrece la posibilidad de conectar la red corporativa con la nube a través de una VPN IPsec o las opciones que ofrezca el proveedor.
- Aplicación de administración del directorio activo desde la nube: Una aplicación de conexión ofrecida por el proveedor que enlace la réplica del directorio activo de la organización y permita la administración de los recursos.
- Aplicación de escritorio remoto virtual: Una aplicación ofrecida por el proveedor que se implemente en las mismas subredes privadas del conector AD, de esta forma se puede ofrecer una conexión de escritorio remoto virtual en la nube con las mismas características de una conexión directa en la red corporativa.

La organización Cliente

- Servicios de conectividad: permite crear la conexión entre el centro de datos corporativo y el proveedor de servicios en la nube.
- AD DS: servicios de directorio activo corporativo
- Dispositivos de usuario final: cualquier dispositivo que pueda conectarse a internet desde la red corporativa o desde cualquier ubicación remota.

Esta propuesta no genera dependencia de la conectividad

debido a que, si falla la conexión entre el centro de datos corporativo y la nube del proveedor, los escritorios remotos virtuales pueden seguir trabajando porque la autenticación se está procesando localmente con la colaboración de la aplicación de administración del directorio activo, también reduce la latencia de conexión y los costos de tráfico.

Es importante definir los grupos de usuarios que van a realizar la conexión por medio de los escritorios remotos virtuales en la nube del proveedor, la aplicación de administración de AD ofrecida por el proveedor da la posibilidad de generar las subredes privadas que alojan a los usuarios de cada uno de los grupos definidos.

También es un factor importante definir dos zonas de disponibilidad de los servicios en la nube, estas zonas de disponibilidad son ubicaciones físicas diferentes de la infraestructura del proveedor de servicios en la nube (diferentes centros de datos), este servicio ofrece características de DRP y garantiza la continuidad del negocio en caso de que una de las ubicaciones falle. Para determinar la ubicación de las zonas de disponibilidad, se deben tener en cuenta las recomendaciones del proveedor de servicios en la nube y los tiempos de respuesta de cada uno de los centros de datos del proveedor con respecto a la zona geográfica donde se van a conectar los usuarios que consumen los servicios, como se muestra en la Figura 3.

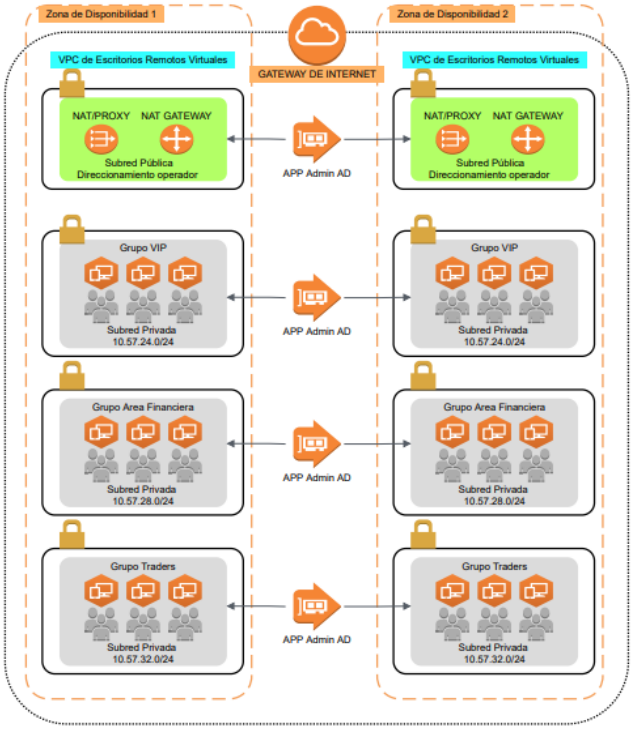

Fig. 3. Diseño de grupos de directorio activo y zonas de disponibilidad. Fuente: Elaboración Propia

4) Fase D - Descripción y desarrollo de la arquitectura tecnológica

– Arquitectura AS IS

La arquitectura actual del CAO cuenta con dos ubicaciones remotas, la primera es el centro de datos de la Organización, en esta ubicación se encuentra el directorio activo que administra los permisos de acceso de cada uno de los usuarios y los privilegios de administración de los usuarios especiales, este servicio se encuentra protegido por la red perimetral de la organización con sus políticas de filtrado y seguridad.

La segunda ubicación es el sitio arrendado donde se conectan los usuarios del CAO cuando en necesario, en esta ubicación se encuentran los equipos de cómputo conectados al router del arrendatario, estos equipos tienen una salida a internet que les permite realizar conexiones por VPN SSL con el centro de datos de la organización, cada uno de los usuarios se registra en el directorio activo de la organización y se conecta al escritorio remoto físico que se encuentra dentro de la red LAN de la organización para acceder a los servicios de conectividad con los privilegios que tiene su usuario de directorio activo, en la Figura 4, se muestra el diseño de la arquitectura actual.

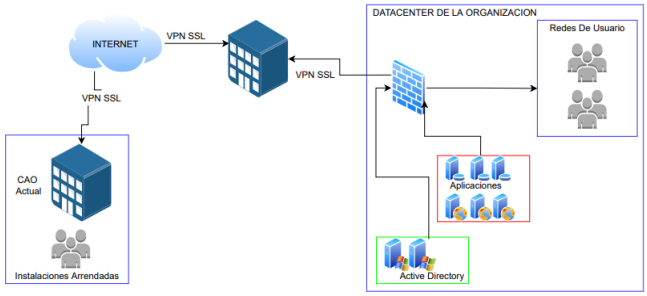

Figura 4. Diseño de la arquitectura actual (AS IS) del CAO. Fuente: Elaboración Propia

– Arquitectura TO BE

La arquitectura que se propone en el proyecto es flexible porque permite la conexión de usuarios autorizados desde cualquier ubicación, el usuario solamente necesita una conexión a internet. Otra característica es que el escritorio remoto ya no va a estar disponible únicamente dentro de la red LAN corporativa, sino que, se va a contar con escritorios remotos virtuales alojados en la nube del proveedor de servicios, para ofrecer servicios de autenticación y permisos de acceso a los recursos y aplicaciones de la organización. Es importante tener una aplicación de administración del directorio activo desde la nube, que se encarga de reemplazar el directorio activo corporativo para los escritorios remotos virtuales y otorgar los privilegios establecidos previamente a los diferentes usuarios autorizados que realicen conexiones al CAO.

A continuación, se muestra una arquitectura detallada de la solución que se plantea, en este escenario se muestran los

flujos de comunicación, los elementos más importantes y la ubicación de cada uno de los elementos.

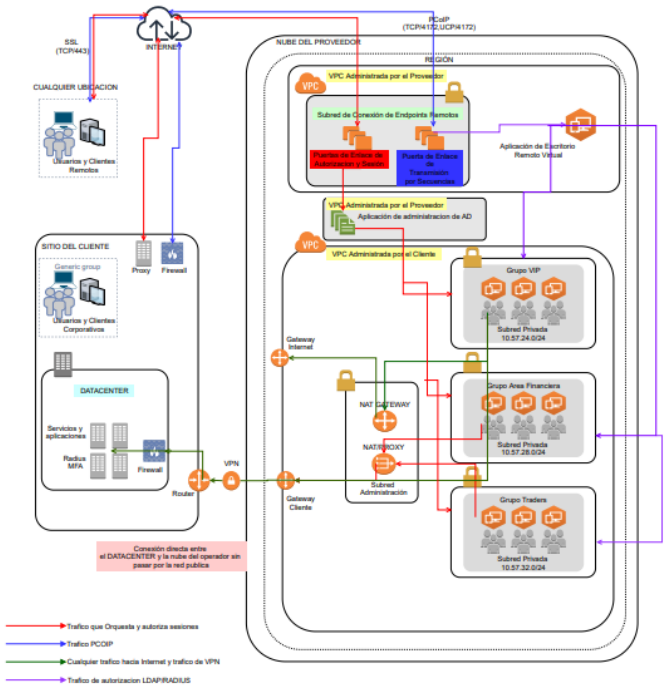

Fig. 5. Diseño de la arquitectura propuesta (TO BE) del CAO. Fuente: Elaboración Propia

En este escenario, la aplicación de administración del directorio activo desde la nube puede realizar tareas como la construcción de una topología de directorio altamente disponible, la monitorización de los controladores de dominio y la configuración de copias de seguridad y snapshots, estas funciones son realizadas por el proveedor de servicios de nube, el personal encargado de la administración del directorio activo corporativo únicamente tiene que desempeñar labores de supervisión, debido a que, la configuración que realiza el proveedor está basada en las directrices, características y recomendaciones del personal encargado de administrar el directorio activo corporativo, esta solución acompañada de la implementación de dos zonas de disponibilidad, ofrece acceso altamente disponible y de baja latencia a los servicios de AD DS (directorio activo, servicios de dominio) para los escritorios remotos virtuales, manteniendo las prácticas recomendadas de separación de roles y funciones del directorio activo corporativo.

5) Siguientes Fases

En las fases que se describen a continuación se indican los siguientes pasos que se deberán realizar pero que no están cubiertos en este proyecto dado que hacen parte de la implementación de la tecnología

Fase E - Identificación de oportunidades y soluciones

En esta fase se identifican oportunidades y busca las mejores soluciones para cualquier problema identificado en las fases anteriores o que surja en esta.

En esta fase se realiza el análisis de brechas, que es un mecanismo para seleccionar el camino más apropiado para pasar de un estado actual “AS-IS” a un estado objetivo “To-Be”. La transición entre la arquitectura de línea base y la arquitectura objetivo en un ejercicio de arquitectura consiste en establecer los elementos nuevos (New), los elementos que han sido modificados (Modify) y/o eliminados (Delete) y los elementos que permanecen (Keep) sin alteraciones.

El análisis de brechas se realiza en cada dominio de la arquitectura, y con dicho análisis se construye una hoja de ruta, soportado en los objetivos de negocio, que permita generar proyectos que lleven la organización de la arquitectura actual (AS-IS) a la arquitectura objetivo (To-Be).

TOGAF define la hoja de ruta de la arquitectura como una lista de componentes y módulos en una línea de tiempo. Cada componente o módulo identifica un grupo lógico de cambios o requerimientos necesarios para realizar la Arquitectura de destino.

Producto de esta se obtiene:

- Una versión inicial completa del roadmap de la arquitectura basado en las diferencias obtenidas a partir de las fases anteriores.
- Se determina si se requiere un enfoque incremental, o sea crear arquitecturas transitorias.
- Se crea una estrategia de migración.

A continuación, se muestra un esquema conceptual de cómo se construye esta fase (Figura 6)

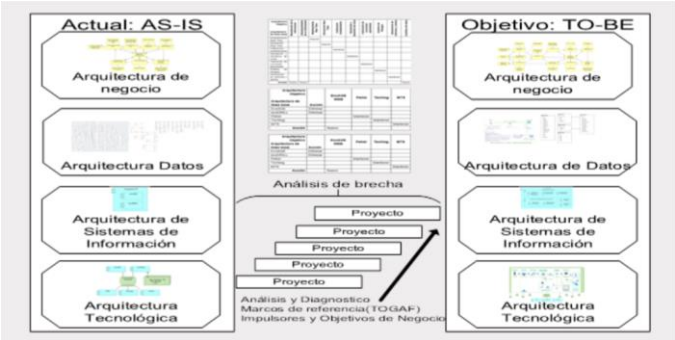

Figura 6. Esquema del proceso TOGAF Fuente: Elaboración Propia

Fase F - Creación de un plan de migración

En esta fase se gestiona el plan de migración en el caso que se requiera, usualmente es utilizado en la actualización de un sistema de información que esté soportado en tecnología obsoleta.

A continuación, se muestra (Figura 7) de manera esquemática el plan de migración, que básicamente consiste en migrar del sistema actual a un sistema SaaS en la nube. El CAO actual está concebido como una arquitectura OnPremises (AS-IS) y se desea llegar a una arquitectura CAO en la nube (TO-BE).

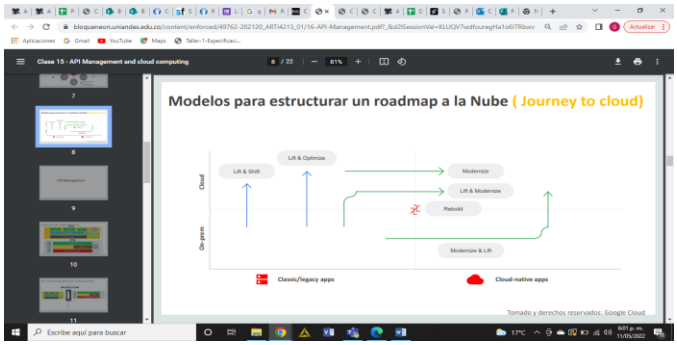

Fig. 7. Esquema de migración Fuente: Elaboración Propia

Fase G: Gobierno de implementación

La fase de gobierno de implementación es la encargada de ejecutar los cambios en la hoja de ruta del proyecto. Al ser una fase que va directamente relacionada con la ejecución, no entra dentro del alcance de este proyecto, más sin embargo se indica cuál es su finalidad.

Fase H: Administración de la gestión del cambio de arquitectura

La gestión de cambios de arquitectura es la fase encargada en que se logren los hitos esperados de acuerdo con las promesas de valor expuestas a los interesados. En esta fase se deberán realizar pruebas funcionales donde se demuestran las mejoras respecto a la solución que tenía y operaba antes la empresa.

El desarrollo de esta fase está por fuera del alcance de este proyecto, pero se indica la finalidad de esta.

IV. CONCLUSIONES

El diseño, la tecnología y la metodología, genera para la empresa una implementación en menores tiempos, ofreciendo servicios adicionales que se podrían desplegar a toda la compañía dando soporte a necesidades de trabajo como la virtualidad.

Como resultado del análisis utilizado se concluye que el mejor diseño del CAO es bajo un esquema en nube pública, dado que tiene los mejores indicadores financieros del proyecto VPN de US$883 y un ROI de 1.2 y no se identifican riesgos no controlables por la compañía.

La estrategia propuesta en este documento es la mejor opción costo-beneficio para la compañía dado que se mitigarán riesgos asociados a las vulnerabilidades encontradas en el CAO actual, se mejorará la seguridad de la información junto con los aspectos técnicos y económicos.

Los controles de seguridad deben estar integrados con un sistema de correlación de eventos con el fin de ser analizados por el centro de operaciones de seguridad (SOC) de la compañía y poder determinar cuándo se deben activar los procesos de vulnerabilidades, incidentes y accesos, que son los pilares de una operación de seguridad de la información.

Este análisis puede ser replicado a otro tipo de organizaciones, que pretendan realizar un diagnóstico, diseño y definición de controles informáticos para una arquitectura de seguridad en un CAO.

REFERENCES

[1] TOGAF. (S. F.). THE OPEN GROUP WEBSITE. RECUPERADO 12 DE MAYO DE 2022, DE HTTPS://WWW.OPENGROUP.ORG/TOGAF

[2] FASES MODELO DE ARQUITECTURA SEGURIDAD DE INFORMACIÓN SANS. (S. F.). EGNYTE. CONSULTADO 15 DE ABRIL DE 2022, DE HTTPS://SANSORG.EGNYTE.COM/DL/ZVJUPQZPRR

[3] CICLO PHVA PARA UNA ASI SEGÚN KILLMEYER. (S. F.). EGNYTE. CONSULTADO 22 DE ABRIL DE 2022, DE HTTPS://SANSORG.EGNYTE.COM/DL/ZVJUPQZPRR