

UNIVERSIDAD NACIONAL
Escuela de Informática
Licenciatura

**ELABORACIÓN DE UN PROTOTIPO FUNCIONAL DE ESCRITORIOS VIRTUALES PARA LA AUDITORÍA
INTERNA DEL BANCO DE COSTA RICA**

Para optar por el grado de Licenciatura en **ÉNFASIS EN SISTEMAS DE INFORMACIÓN**

Por: **CRISTIAN SOLANO CHACÓN**

FEBRERO, 2021

A Dios.

Por darme la paciencia y sabiduría para entender y superar los obstáculos para concluir con este trabajo y claridad mental para continuar a pesar de las dificultades en el camino y lograr mis objetivos, aunque no fueron cuando yo lo quería, se dieron en el mejor momento porque así él lo quiso.

A mis padres.

Por los ejemplos de superación y constancia que me enseñaron, por el valor de las cosas cuando se logran con sacrificio, por referirse a mi como capaz, inteligente y por darme la mejor educación posible para poder llegar a este punto, por transmitirme la fe en un Dios todo poderoso que me guiará y me abrirá puertas.

A mi Amor, Esposa y Compañera de Vida, Magaly.

Por haberme impulsado a concluir con mis estudios superiores después de tanto tiempo, por su paciencia, apoyo, consejos y el ánimo que siempre me dio para seguir adelante y poder concluir este proyecto.

A mi hija, Valentina

Por ser el motor que me impulsa a mejorar, superarme y motivarme para ser un ejemplo para ella, también por soportarme en momento de frustración por los inconvenientes para concluir mi Licenciatura.

A la subdirectora, Carmen Cordero, por su orientación y apoyo para la culminación del trabajo de graduación de Licenciatura.

A mi tutor Randall Artavia, por su guía, acompañamiento y asesoría durante toda la elaboración de este trabajo de graduación en Licenciatura.

TABLA DE CONTENIDOS

CAPÍTULO I: INTRODUCCIÓN	8
1. Antecedentes	8
2. Planteamiento del problema	9
3. Justificación	11
4. Objetivos del Proyecto	14
4.1 <i>Objetivo general</i>	14
4.2 <i>Objetivos específicos</i>	15
CAPÍTULO II: MARCO TEÓRICO	17
CAPÍTULO III: METODOLOGÍA	31
1. Tipo de investigación	31
2. Población y muestra	32
3. Descripción de instrumentos	33
4. Procedimientos para analizar la información del diagnóstico	34
CAPÍTULO IV: PROPUESTA DE SOLUCIÓN	38
1. Diagnóstico	38
1.1 Situación actual:	38
1.1.1 Requerimientos de usuarios	38
1.1.2 Requerimientos de seguridad	40
1.1.3 Requerimientos de conexión	41
1.1.4 Documentación para la gestión de Escritorios Virtuales	41
1.1.5 Recursos disponibles	41
2. Propuesta de solución	45
2.1 Requerimientos de usuarios	47
2.1.1 Herramientas de trabajo	47
2.1.2 Situaciones no previstas	51
3. Validación de la propuesta	53
3.1 Conexión y validación del usuario	54
3.2 Visualización de Escritorio Virtual	54
3.3 Carga de configuración específica para Lotus Notes	55
3.4 Sitio de SGA y GEA	55
3.5 Sitio de SOMOS BCR	55
3.6 Recursos de Información	56
3.7 Recursos para Administración Infraestructura	56

3.8 Editores de archivos de Office	56
3.9 Sistemas CORE	57
3.10 Administración de infraestructura	57
3.11 Conocimiento adquirido para asesorar	57
CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES	61
1. Conclusiones	61
2. Limitaciones	64
3. Recomendaciones	65
4. Trabajos futuros	66
REFERENCIAS	69
Anexo 1 - Entrevistas a usuarios expertos	72
Anexo 2 - Matriz Requerimientos – Propuesta – Implementado	85

ÍNDICE DE TABLAS

TABLA 1. Matriz de soporte por parte del proveedor	41
TABLA 2. Reducción de gastos de la Auditoría Interna del Banco de Costa Rica con el teletrabajo.....	63

ÍNDICE DE FIGURAS

FIGURA 1. Propuesta de acceso a los recursos tecnológicos de la Auditoría Interna y del Banco	12
FIGURA 2. Organigrama Organizacional.....	25
FIGURA 3. Fases y elementos a considerar en el desarrollo del prototipo.....	34
FIGURA 4. Cronograma de actividades para la ejecución del proyecto.....	35
FIGURA 5. Características de cada Host del clúster en el CPP y CAP.....	42
FIGURA 6. Infraestructura vSphere y vSAN en el CPP y CAP.....	43
FIGURA 7. Acceso a los recursos informáticos antes de la propuesta.....	44
FIGURA 8. Acceso por Escritorio Virtual Remoto a los recursos informáticos.....	58
FIGURA 9. Distribución de teletrabajadores en total del BCR.....	62

CAPÍTULO I
INTRODUCCIÓN

CAPÍTULO I: INTRODUCCIÓN

1. Antecedentes

En Costa Rica, el uso de Infraestructura de Escritorios Virtuales (VDI) por sus siglas en inglés, ya forma parte del esquema de trabajo y negocio de algunas empresas importantes, por mencionar algunas de ellas tenemos la empresa HUAWEI que ofrece el servicio de Escritorio Virtual en la nube tanto para pymes como empresas grandes en el 2015; la Comisión de la Jurisdicción Civil implementa Escritorios Virtuales en diferentes despachos del país publicado en el la página del Poder Judicial en 2016; RACSA ofrece servicio de conversión de escritorios físicos a virtuales en el 2019; Kölbi Negocios ofrece el servicio de Escritorios Virtuales desde dispositivos fijos o móviles hoy día.

En la actualidad, el Banco de Costa Rica utiliza la Infraestructura de Escritorios Virtuales, para que sus proveedores de software tengan un recurso tecnológico dentro del Banco con el cual dar soporte y desarrollar desde sus empresas, siempre en conexión con los ambientes de Desarrollo-Pruebas-Producción del Banco permitiendo movilidad y acceso a distancia.

Esta decisión se tomó en el 2017 con 250 escritorios virtuales, con el fin de reducir los costos en que se incurrían al tener proveedores dentro de las instalaciones del Banco, como por ejemplo: espacio físico, equipo de cómputo, personal para supervisión en sitio y horarios especiales para atender al proveedor según necesidades. Dado el éxito que esta tecnología tuvo en el BCR, se hizo necesario el incremento de almacenamiento y servidores físicos para aumentar en 3000 Escritorios Virtuales en el 2018, aun cuando no se requería inmediatamente se consideró esta capacidad para un futuro crecimiento.

La Auditoría Interna en instituciones como el Banco de Costa Rica, es una figura que apoya a la administración para validar la aplicación y eficiencia de los controles definidos para salvaguardar los recursos económicos y de bienes muebles e inmuebles que administran, incluyendo la información de los clientes y del negocio, por lo que requiere de una movilidad y acceso en todo momento a la información del Banco.

La plataforma de VDI, podría proveer a la Auditoría Interna del Banco de Costa Rica de Escritorios Virtuales y remotos como un medio para conectarse y tener acceso a los sistemas de información que fiscaliza y utiliza para su labor diaria desde cualquier lugar geográficamente hablando, proveyendo de una movilidad para los trabajos de campo.

Hoy día esta Auditoría, accede sistemas de información y herramientas del Banco y de la Auditoría misma desde las oficinas centrales en San José, sin embargo, en otras ubicaciones geográficas de trabajo existen limitaciones de acceso, dado la ausencia de controles de seguridad para la concentración de información y sistemas a acceder como en la oficina.

La solución que se persigue con el uso de la VDI permitirá implementar Escritorios Virtuales para cada uno de los funcionarios de la Auditoría Interna del BCR, proveyendo una movilidad y acceso total de sistemas e información, manteniendo los mismos estándares de seguridad, calidad e integridad de la información que fiscaliza y procesa, definidos por y para el Banco de Costa Rica. Además, esta plataforma permite utilizarse para el Teletrabajo y en otras situaciones de emergencia institucional o nacional, como en los casos de contingencia o desastres naturales.

2. Planteamiento del problema

Actualmente los funcionarios de la Auditoría Interna del Banco de Costa Rica necesitan de movilizarse a las oficinas del Banco en diferentes ubicaciones geográficas en todo el territorio nacional y realiza sus estudios de auditoría y demás actividades o labores de valoración y fiscalización que fortalecen el control interno de la institución.

La verificación en sitio es una de las necesidades primordiales para ser oportunos y efectivos en sus trabajos de campo, lo cual incluye tener acceso a todos los sistemas de información del Banco, entes externos que norman los procesos internos del negocio bancario.

Por otro lado, la Auditoría Interna del Banco de Costa Rica cuenta con su propia infraestructura de Red, Servidores y estaciones de trabajo, los cuales administra de forma independiente del área de Tecnología del Banco y cuentan con funcionarios para administrar estos recursos de forma autónoma e independiente, mismos que dan soporte y administración en todo momento a los funcionarios y sistemas propios de la Auditoría.

La labor de una auditoría en instituciones públicas cubre tanto a las oficinas centrales como a las distribuidas en todo el territorio nacional, para estas últimas, es necesario que los funcionarios de Auditoría se desplacen a realizar trabajo de campo en coordinación con otros funcionarios que se mantienen en la sede central, requiriendo comunicación en línea para tareas colaborativas y de acceso a información sensible que por la seguridad que requiere se almacena de forma centralizada.

Por lo anterior, la información que se requiera acceder fuera de la red principal del Banco debe de mantener las características de confidencial, integridad y de acceso restringido, pero manteniendo

por parte de los Auditores una independencia para su consulta, en su totalidad y con acceso oportuno.

Actualmente, el trabajo de campo en la Auditoría Interna del Banco de Costa Rica se encuentra con una limitación de acceso a sistemas e información tanto del Banco como de la misma Auditoría, recursos necesarios para consultas, investigación y de procesamiento de información en los sistemas. Las restricciones se dan, debido al esquema de seguridad implementados para acceder a la red principal del Banco en donde se encuentran los equipos y sistemas CORE, desde puntos externos a esta red, que por política institucional y por recomendación del área de seguridad en Tecnología, solo se habilitan para acceder desde su sede central, forzando a realizar la mayor parte del trabajo de auditoría desde esta sede, limitando el trabajo a realizar dado el no acceso en los sitios de investigación y objeto de Auditorías, provocando reproceso, inoportunos en el acceso a la información, imposibilidad de ejecutar un flujo de trabajo normal con los colaboradores de un mismo estudio.

La implementación de Escritorios Virtuales permitiría que los funcionarios de la Auditoría Interna realicen las actividades diarias en coordinación y oportunidad al contar con todas las herramientas e información en tiempo real desde cualquier oficina del Banco, permitiendo la movilidad, potenciando el alcance del auditor a todos los puntos geográficos de negocio del Banco como una extensión del trabajo de las oficinas centrales.

3. Justificación

Para los funcionarios de la Auditoría Interna del Banco de Costa Rica, tener acceso a los datos en la plataforma tecnológica de la institución como fuente de información y de herramientas de procesamiento para los estudios de auditoría en todo momento, permitiría brindar un servicio de fiscalizador y asesor oportunamente, y cumplir con su misión de “Contribuir al logro de los

objetivos del Banco mediante los servicios preventivos y de auditoría que ayuden al mejoramiento de la efectividad de la gestión del riesgo y el control, y la optimización de los procesos y recursos.”

Utilizando la tecnología de los Escritorios Virtuales de forma remota, se tendría acceso desde cualquier ubicación geográfica que cuente con una red, a los recursos tecnológicos del Banco que son necesarios para las labores de auditoría, contempladas en el marco regulatorio que debe de cumplir.

Con la presente propuesta, se prevé igualar las condiciones de trabajo fuera de la sede central en cuanto al acceso de información en todo momento y de las herramientas definidas para el trabajo de auditoría. También, se podrá continuar con el flujo de trabajo con todos los funcionarios de la Auditoría independientemente de donde estén laborando para la coordinación, discusión, aprobación y comunicación de resultados.

En otras palabras, no habrá diferencia de realizar estudios de auditoría en las áreas de negocio que se encuentren descentralizadas, dado que la ampliación y cobertura de las herramientas tecnológicas para la auditoría será total a todas las oficinas del negocio.

Se proveerá de una movilidad al funcionario de la auditoría con el acceso remoto a los recursos tecnológicos que se acceden desde la sede central, esto sin comprometer la seguridad e integridad de la información accedida y procesada.

La implementación de movilidad y acceso remoto son necesarias para minimizar el impacto de las limitaciones de acceso a los recursos de información y procesamiento para los estudios de

Auditoría en sitios descentralizados, disminuyendo el riesgo de detección de auditoría al contar con la capacidad de analizar y procesarla en sitio.

El trabajo en cuestión, generará un diseño, lineamientos de configuración, gestión e implementación para un prototipo funcional de los Escritorios Virtuales con acceso remoto para la Auditoría Interna del BCR, con las características específicas de trabajo y acceso para cada una de sus áreas de fiscalización que la componen, que independientemente de donde se desarrolle el trabajo de Auditoría se mantendrá centralizado tanto la información fuente como la generada con las calidades de integridad y veracidad de la información actualizada en línea.

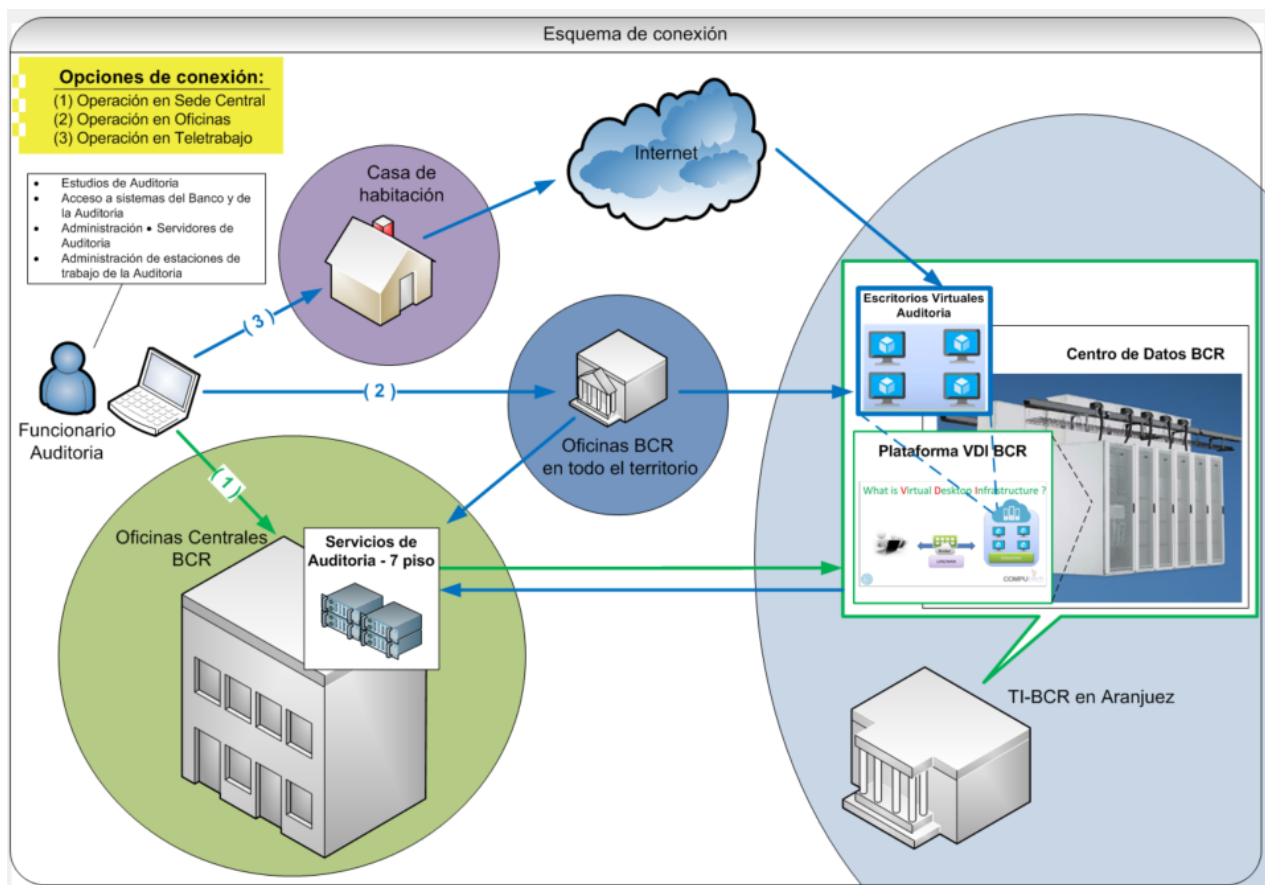


Figura 1. Propuesta de acceso a los recursos tecnológicos de la Auditoría Interna y del Banco por el Auditor desde diferentes ubicaciones geográficas. Elaboración propia.

Dicha propuesta, proveerá los mecanismos de control de acceso y validación necesarios para cumplir con el marco regulatorios y sanas prácticas de seguridad de la información, establecidos a lo interno y externo del Banco de Costa Rica como sanas prácticas.

Atender la necesidad operativa de contar con acceso en todo momento e irrestricto de información y herramientas de trabajo para las labores de auditoría, indistintamente de la ubicación geográfica en donde se realicen las labores de un auditor, permitiría que la Auditoría Interna del Banco de Costa Rica pueda ser eficiente y eficaz en su labor, oportuno en la comunicación de resultados y por ende una pronta atención de las debilidades para el beneficio de la institución a la cual se debe.

Cabe destacar, que la Auditoría Interna debe de cumplir con el plan de labores anual que comunica a la Contraloría General de la República, el cual presenta riesgos que pueden afectar en tiempo y alcance dicho plan, por las limitaciones que se han mencionado anteriormente y que, dependiendo del tema evaluado, el riesgo de incumplimiento aumenta su probabilidad.

Por otro lado, proveer a la Auditoría de herramientas como Escritorios Virtuales remotamente para estar alineados con la actualización tecnológica de hoy día como VDI, permitirá que a futuro la adopción de nuevas tecnologías de comunicación y trabajo, tendrán las bases sólidas y un nivel de madurez para un proceso de cambio necesario en la forma de trabajar del auditor.

La tendencia que se identifica hoy día, como por ejemplo el enfoque de “Trae tu propio dispositivo” (BYOD) por sus siglas en inglés y el uso de Cloud como medio de almacenamiento y acceso a Escritorios Virtuales, son elementos para una flexibilidad de lugares de trabajo en las organizaciones, lo que sugiere una movilidad y uso de dispositivos fuera de la oficina.

4. Objetivos del Proyecto

4.1 Objetivo general

Diseñar un prototipo funcional de Escritorios Virtuales con acceso remoto para conectarse a la red de la Auditoría Interna y del Banco de Costa Rica desde cualquier punto geográfico por medio de un computador, conforme a las políticas de seguridad e integridad de los datos.

4.2 Objetivos específicos

1. Definir una plantilla Master en la plataforma VDI del BCR que contenga el software configurado, permisos y accesos para las actividades diarias de la Auditoría Interna del Banco de Costa Rica.
2. Elaborar la documentación técnica de apoyo para la administración, configuración y operación de los Escritorios Virtuales para la Auditoría Interna del Banco de Costa Rica, así como las estrategias de respaldos.
3. Implementar un prototipo funcional de Escritorio Virtual para la Auditoría Interna del Banco de Costa Rica, desde la red privada del Banco y la red pública (Internet) para el uso diario en las labores de la auditoría.

CAPÍTULO II
MARCO TEÓRICO

CAPÍTULO II: MARCO TEÓRICO

Dentro del ámbito del diseño de una solución de Escritorios Virtuales (VDI) se deben abarcar previamente algunos conceptos relacionados con las tecnologías de infraestructura virtualizada que permitan dilucidar los aspectos involucrados para tal efecto y que se irán introduciendo a continuación.

- **Teletrabajo**

El teletrabajo consiste en el trabajo que hace una persona para una empresa desde un lugar distante de la sede de esta, y que se realiza utilizando las TIC's (tecnologías de información y comunicación). Se realiza a distancia y con la colaboración de las modernas tecnologías de la comunicación, o si se quiere precisar un poco más, es aquella forma de trabajo que se realiza en un lugar alejado de las oficinas centrales o centros de trabajo habituales, y que implica la utilización de equipos informáticos y de telecomunicaciones como herramientas primordiales para el cumplimiento de las actividades (Buirra, 2012)

- **Hardware y Software**

El hardware son todos los componentes materiales y físicos de un dispositivo, es decir aquellos que se pueden ver y tocar. El monitor, el ratón, el CPU, etc.

El Software es la parte digital de un dispositivo, es decir, el conjunto de instrucciones, programas y reglas informáticas que el dispositivo requiere para funcionar. No tiene por consiguiente una existencia física, sino que es intangible e inmaterial. (Heredero, 2004).

- **Computadora**

Una computadora es una máquina electrónica conformada por hardware y software que recibe, almacena y procesa datos, para luego convertirlos en información conveniente y útil para los usuarios.

- **Red de computadoras**

Una red de computadoras o red informática es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Las redes son un conjunto de equipos (computadoras y/o dispositivos) vinculados por medio de cables, señales, ondas o cualquier otra técnica de transporte de datos, que distribuyen información (archivos), recursos (discos, impresoras, etc.) y servicios (acceso a internet, correo electrónico, chat, juegos), entre otros (Cedano Olvera, Cedano Rodríguez, Rubio González, & Vega Gutiérrez, 2014).

- **Seguridad informática**

La seguridad informática, también conocida como seguridad de tecnologías de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras y todo lo que la organización valore y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encargan de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta (Urbina, 2016).

- **Cifrado de la información**

El cifrado es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que solo pueda leerlo la persona que cuente con la clave de cifrado adecuada para decodificarlo.

- **Certificado Digital**

Es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. El titular del certificado debe mantener bajo su poder la clave privada, ya que, si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red.

- **VPN**

Una red privada virtual o Virtual Private Network (VPN) por sus siglas en inglés, es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas, como si

fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

- **BYOD**

Por sus siglas en inglés Bring Your Own Device, cuya traducción sería “trae tu propio dispositivo”, una tendencia en el ámbito empresarial, en la cual los empleados tienen la posibilidad de llevar y utilizar sus propios dispositivos (ordenadores portátiles, smartphones y tabletas) para acceder a los recursos de su compañía.

- **VDI**

El término Infraestructura de Escritorios Virtuales (VDI) hace referencia al uso de máquinas virtuales para proporcionar y gestionar escritorios virtuales. La VDI aloja entornos de escritorio en un servidor centralizado y los distribuye a los usuarios finales según las necesidades.

- **Virtualización**

En Informática, virtualización es la creación a través de software de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

La virtualización es la técnica de abstracción de hardware que permite emular varios sistemas con características físicas similares (limitados por la arquitectura del procesador físico); de forma tal, que permita ejecutar varios recursos computacionales, llamadas máquinas virtuales (PACIO, 2014).

- **Virtualización de Sistemas Operativos**

Consiste en ejecutar varios sistemas operativos (invitados) sobre un sistema operativo real (anfitrión) que se ejecuta sobre una máquina física. Para ello se utiliza un software de virtualización (gestor de máquina virtual) que se encarga de interpretar el conjunto de instrucciones de la máquina, ese programa se le conoce como Hipervisor de tipo 2. Un inconveniente es que consume recursos que necesita el sistema operativo real

- **Escritorios Virtuales**

La virtualización de escritorio es un término relativamente nuevo, introducido en la década de los 90, que describe el proceso de separación entre el escritorio, que engloba los datos y programas que utilizan los usuarios para trabajar, de la máquina física. El escritorio "virtualizado" es almacenado remotamente en un servidor central en lugar de en el disco duro del ordenador personal. Esto significa que cuando los usuarios trabajan en su escritorio desde su portátil u ordenador personal, todos sus programas, aplicaciones, procesos y datos se almacenan y ejecutan centralmente, permitiendo a los usuarios acceder remotamente a sus escritorios desde cualquier dispositivo capaz de conectarse remotamente al escritorio, tales como un portátil, computadora (PC), tableta, teléfono inteligente o cliente ligero.

- **Gestión de Procesos de Auditoría (GPA)**

Se refiere a la aplicación para el control de todo el proceso de auditoría. A través de una plataforma única integrada, la solución gestiona todas las etapas, desde la planificación de la auditoría, preparación, definición de cronogramas, desarrollo de planes y listas de verificación, hasta la ejecución, registro de resultados, emisión de informes y seguimiento.

- **Auditorías**

La actividad de auditar consiste en realizar un examen de los procesos y de la actividad económica de una organización para confirmar si se ajustan a lo fijado por las leyes o los buenos criterios.

- **CORE**

Es una palabra en inglés que significa núcleo o centro por ejemplo un **sistema** de préstamos sería un componente del CORE Bancario.

- **Servidor**

Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente.

- **Código Fuente**

El código fuente de un programa informático (o software) es un conjunto de líneas de texto con los pasos que debe seguir la computadora para ejecutar un programa.

- **Capa de Presentación- Aplicación- Base de Datos**

Distribución de funciones primordiales de una aplicación informática, las cuales son accedidas en el siguiente orden: Presentación, Aplicación, Base de Datos.

- **Respaldo**

Se refiere al resguardo que se realiza de ciertos datos de una aplicación o base de datos, ya sea datos de configuración o información.

- **Plantilla Master**

Se refiere a la configuración de un sistema operativo que es replicada en nodos para presentarse al usuario final en un escritorio virtual dentro de la plataforma VDI de VMWare.

- **Permisos y privilegios**

Los permisos suelen estar asociados al poder que se otorga a los usuarios y grupos de usuarios sobre los archivos, carpetas, directorios, etc. Los privilegios se refieren a las acciones que se pueden realizar sobre estos objetos.

- **Firewall**

Es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- **Palo Alto Networks**

Marca de equipos Firewall que ofrece una visibilidad integral del tráfico de red basado en aplicaciones, usuarios y contenido, al tiempo que le permite adoptar y abordar sus necesidades comerciales.

- **Puertos de red**

Número identificador en un protocolo de red utilizado por una aplicación para establecer comunicación.

- **PKI**

Es una infraestructura de clave pública (en inglés: Public Key Infrastructure –**PKI**–) es una combinación de hardware, software, y políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas, como el cifrado, la firma digital, y el no repudio de transacciones electrónicas.

- **VMWare Horizon**

Es una solución que simplifica la gestión y distribución de escritorios y aplicaciones virtuales en las instalaciones, en la nube o en una configuración híbrida o multinube a través de una sola plataforma para los usuarios finales. Horizon ayuda a los departamentos de TI a controlar, gestionar y proteger todos los recursos de Windows que los usuarios finales desean, a la velocidad que esperan y con la eficacia que la empresa exige, ya que aprovecha la gestión completa de entornos de área de trabajo y está optimizado para el centro de datos definido por software.

- **Active Directory**

Su traducción es Directorio Activo (DA) son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos, principalmente LDAP, DNS, DHCP y Kerberos.

- **ADFS**

Por sus siglas en inglés es Active Directory Federator System.

- **Dominio**

Es el nombre con el que se conoce a una empresa en Internet. En el dominio se definen los usuario y grupos de usuario que pueden acceder a la organización relaciona.

- **Centro de procesamiento de datos**

Es el espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

- **Almacenamiento en la nube**

El almacenamiento en la nube es un modelo de almacenamiento de datos basado en redes de computadoras, ideado en los años 1960 donde los datos están alojados en espacios de almacenamiento virtualizados, por lo general aportados por terceros.

Las compañías de alojamiento operan enormes centros de procesamiento de datos. Los usuarios que requieren estos servicios compran, alquilan o contratan la capacidad de almacenamiento necesaria. Los operadores de los centros de procesamiento de datos, a nivel servicio, virtualizan los recursos según los requerimientos del cliente. Solo exhiben los entornos con los recursos requeridos. Los clientes administran el almacenamiento y el funcionamiento de los archivos, datos o aplicaciones. Los recursos pueden estar repartidos en múltiples servidores físicos.

- **Recompose**

Proceso por medio del cual se actualizan todos los clones enlazados a una plantilla Master.

- **Hipervisor**

Hipervisor o Virtual Machine Monitor (VMM) es una tecnología que está compuesta por una capa de software que permite utilizar, al mismo tiempo, diferentes sistemas operativos o máquinas virtuales (sin modificar o modificados en el caso de para-virtualización) en una misma computadora central. Es decir, es la parte principal de una máquina virtual que

se encarga de manejar los recursos del sistema principal exportándolos a la máquina virtual.

- **vSAN**

Es la solución de hyperconvergencia para el almacenamiento que VMware sacó al mercado con la versión de vSphere 5.5. Este almacenamiento está definido por Software (Storage Defined Software o SDS) y permite abstraerse del hardware de almacenamiento.

- **vMotion**

Es una tecnología que permite la migración “en caliente” de una MV desde un host a otro, sin un impacto apreciable por el usuario final.

- **¿Qué es infraestructura virtual?**

Una infraestructura virtual es una infraestructura de Tecnología basada en software alojada en otra infraestructura física y destinada a ser distribuida como un servicio, tal como en el modelo de entrega de Infraestructura como Servicio (IaaS) de computación en la nube.

Este tipo de servicios en la nube son cada vez más utilizados por las organizaciones, particularmente las más pequeñas, que no pueden permitirse construir su propia infraestructura física, permitiéndoles el acceso a tecnologías de grado empresarial, tales como servidores y aplicaciones de alto rendimiento, alta disponibilidad y continuidad del servicio. La distribución de dichos servicios a menudo se hace a través de la nube, es decir, a través de grandes redes como Internet.

La Auditoría Corporativa del Banco de Costa Rica cuenta actualmente con nueve áreas de Auditoría, las cuales están relacionados con Procesos, Finanzas, Banca Personas, Banca Corporativa, Riesgos, Apoyo, Operaciones, General, Legal y de Tecnologías, también existen cuatro Sociedades Anónimas del Conglomerado BCR, cada una con su respectiva área de Auditoría.

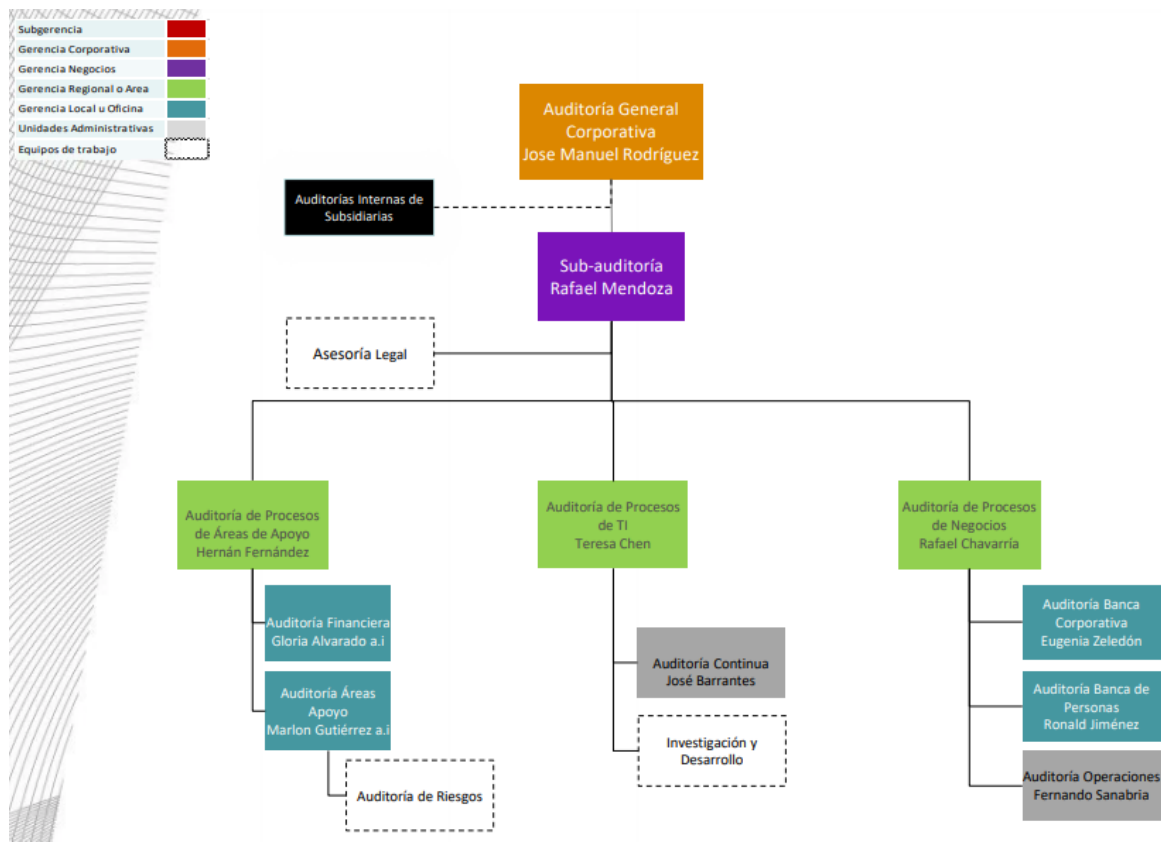


Figura 2. Organigrama Organizacional de la Auditoría Interna vigente desde junio del 2020. Tomado de SOMOS.bancobcr.com, sitio oficial interno del Banco de Costa Rica.

Dentro de las labores diarias que los auditores ejecutan, se tienen el desarrollo de Estudios de Auditoría, Seguimientos de Auditoría, Estudios Especiales o cualquier otra actividad dentro de

las responsabilidades de la labor de auditoría, los cuales se gestionan y documentan a través de un sistema denominado GPA (Gestión de Proceso de Auditoría), el cual es la aplicación principal de la Auditoría Interna cuya información residen en dos servidores administrados por esta.

Existen también desarrollos internos para el análisis de riesgos, intranet de Auditoría, publicación de indicadores para el negocio y almacenamiento de información propia de auditoría. Todo esto reside y se administra en servidores y sistemas desarrollados a lo interno por y para la Auditoría.

Las actividades y herramientas mencionadas se deben ejecutar y acceder tanto dentro de las instalaciones centrales del Banco, como en las oficinas ubicadas en todo el territorio nacional, recopilando, accediendo y analizando información, los cuales deben de validarse con la normativa interna, externa y datos de sistemas en su versión más actualizada o en línea.

Por su rango de acción, los funcionarios de la Auditoría Interna deben de tener acceso irrestricto, en línea y sin intervención de los dueños de los datos para mantener la interdependencia e integridad de la información de los sistemas de Crédito, Financieros y de Procesos del Banco objeto de estudio, así como Proyectos, Estrategias y de Tecnología implementados y de uso diario para el negocio, esto abarca información de los funcionarios y de los clientes del BCR.

Actualmente se tiene la limitación de acceso total y en línea a información y sistemas, cuando se ejecutan los trabajos de auditoría denominado de Campo, los mismos se desarrollan fuera de las oficinas de la Auditoría e incluso del BCR, en donde el acceso a los recursos tecnológicos que custodian datos está limitado por un tema de seguridad, no habilitada en estos espacios.

Ante estas limitaciones de consulta y validación de información y colaboración en línea con los funcionarios de Auditoría que participan en los estudios, los trabajos se realizan parcialmente en sitio y de forma aislada, contando con reproceso de trabajo y reiteradas visitas a la misma oficina una vez que se refresquen los datos.

Dentro del Banco no se cuenta con posibilidades de realizar la modalidad de *Teletrabajo* con el mismo acceso a los sistemas, datos, información y colaboración línea con la oficina de la Auditoría Interna, con el fin de obtener los beneficios de un tiempo de calidad para la preparación de análisis de información e informes finales, y en el caso de tener que dar un soporte a los servidores de (Base de datos-Aplicación-Presentación-Respaldos) y sistemas internos, no es posible fuera de las instalaciones centrales.

En el caso de que un administrador de la infraestructura de la Auditoría Interna requiera restablecer la operativa normal de la oficina en situaciones o eventos que provocan un mal funcionamiento en algún punto de la infraestructura y que los administradores no estén dentro de las instalaciones del Banco, la recuperación de la operativa normal de sistemas, equipos o incluso la administración de usuarios, permisos y accesos que se otorgan a solicitud dentro de la Auditoría Interna, no sería posible de inmediato y solo estando en sitio.

En resumen, la Auditoría Interna del BCR mantienen una total independencia en la administración de la red, servidores y equipos portátiles del resto del Banco, con un mayor acceso a la información y sistemas.

Existen tecnologías como VPN, con la cual se crea una extensión de una red privada como la del Banco por medio del Internet, esto permitiría la comunicación segura y encriptado a la VDI del BCR desde las computadoras de los auditores.

El diseño de Escritorio Virtual para el auditor contemplara la instalación de los clientes aplicativos, herramientas de administración para servidores, apertura de puertos y acceso desde el ambiente VDI a sistemas y equipos servidores que utiliza a diario los funcionarios de la auditoría, homologando el ambiente de trabajo tecnológico como en la oficina.

Contar con la posibilidad de aislarse del entorno de las oficinas y sus distractores, permitiendo una mejor concentración y disposición para los trabajos de análisis y documentación de informes que lo requieren por su importancia y urgencia, esto sin perder la disponibilidad como recurso y participación en el flujo de trabajo de la oficina, aunado a mejorar la condición de ánimo del funcionario por evitar trasladarse de la casa al trabajo y viceversa. Todo lo anterior, utilizando la tecnología que permite un acceso remoto, en línea y colaborativa, serían los beneficios que se lograrían desarrollando un protocolo, plataforma, configuración y accesos para realizar tareas en línea de forma remota hacia los recursos de información y tecnológicos del Banco y Auditoría Interna con esta propuesta.

Desarrollar y configurar las condiciones para contar con una movilidad y acceso desde cualquier punto geográfico sin desmejorar o atentar contra la seguridad de acceso y validación establecidas por la institución, que aseguran la integridad de la información de los funcionarios y clientes, conforman los logros de esta propuesta, que permitiría una forma de trabajo a distancia con el mismo acceso, independencia y atención a las actividades diarias, con mejores y oportunos resultados.

CAPÍTULO III METODOLOGÍA

CAPÍTULO III: METODOLOGÍA

1. Tipo de investigación

La metodología a utilizar para la recopilación de la información del proyecto de propuesta de implementación de Escritorios Virtuales en la Auditoría Interna del Banco de Costa Rica, es del tipo descriptivo ya que tiene como fin describir, determinar las necesidades, las características técnicas y de recursos necesarias para el diseño de una solución de Escritorios Virtuales que permitan a los usuarios de la organización desempeñar sus funciones sin importar donde se encuentren, esto apoyado en lo que dice (Moguel, 2005):

La investigación descriptiva comprende la descripción, registro, análisis e interpretación de la naturaleza actual, composición o procesos de los fenómenos.

El enfoque se hace sobre conclusiones dominantes, o sobre cómo una persona, grupo o cosa, se conduce o funciona en el presente. La investigación descriptiva trabaja sobre realidades y su característica fundamental es la de presentarnos una interpretación correcta.

El enfoque de este estudio es de carácter cualitativo, debido a que se quiere analizar elementos como de infraestructura de tecnológica existente, el centro de datos, los requerimientos de seguridad y de redes de comunicación actual del Banco de Costa Rica, para elaborar un diseño de una solución para el uso de Escritorios Virtuales; y para ello se utiliza la recolección de datos sin medición numérica, para descubrir o afinar preguntas de investigación en el proceso de interpretación (Hernández Sampieri, Fernández Collado, & Batista Lucio, 2010).

Los sujetos de información son las entidades que serán beneficiadas con el desarrollo de la investigación. En este caso se encuentran representados por los funcionarios de la Auditoría

Interna del Banco de Costa Rica, Auditorías de las Subsidiarias del Conglomerado, el Auditor General y el Sub Auditor de la Gerencia de Auditoría, estos últimos son los encargados de tomar las decisiones gerenciales importantes para la Gerencia de Auditoría Interna en general.

Las fuentes de información de la investigación que se utilizarán serán las fuentes primarias que hacen referencia a información no abreviada ni traducida, tales como libros, entrevista a usuarios, informes técnicos y documentación técnica y en cuanto a las fuentes secundarias serán toda la información escrita que sirve de apoyo tales como: Tesis, artículos científicos, sitios Web y proyectos similares.

Se considerarán las variables de acuerdo con los objetivos específicos de la investigación, que según (Salkind, 2012), La palabra variable tiene varios sinónimos, como cambiante o inestable. Nuestro conjunto de reglas nos dice que una variable es un sustantivo, no un adjetivo, y representa una clase de resultados que pueden asumir más de un valor.

También, como dice (Icart Isern, Pulpón Segura, Garrido Aguilar, & Delgado Hito, 2012); las variables son propiedades o construcciones hipotéticas que pueden adquirir distintos valores; propiedad es la variabilidad y afecta a casi todos los fenómenos relacionados con la vida. Las variables se pueden clasificar según diferentes criterios, que no son excluyentes.

2. Población y muestra

La población a la que beneficiadas con el desarrollo del proyecto de Escritorios Virtuales son los señores auditores funcionarios de Auditoría Interna del Banco.

El Auditor General y el Sub Auditor son las cabezas de las diferentes Gerencias de Auditoría Interna, y constituyen las figuras que conocen a fondo las necesidades de información en cada

una de una de las Gerencias de Auditoría, estos apoyados por sus mandos medios como los Gerentes y Jefes de departamentos.

El tipo de muestreo a utilizar es el no probabilístico debido a que la muestra está sujeta a las características de la investigación y no por probabilidad. Consiste en entrevistas a los usuarios expertos y encargados de los diferentes departamentos involucrados.

Ya que según (Salkind, 2012), el muestreo no probabilístico comprende aquellas en las que se desconoce la probabilidad de escoger un solo individuo. En este caso, hay que suponer que los miembros en potencia de la muestra no tienen una probabilidad igual e independiente de ser seleccionados.

Además, el muestreo también es por conveniencia ya que dicha muestra está supeditada a las características que mejor se adapten a la investigación, ya que según (Salkind, 2012), El muestreo de conveniencia es justo lo que indica su nombre. Un entrenador de fútbol da a cada miembro de su equipo un cuestionario.

3. Descripción de instrumentos

Los instrumentos que se utilizarán para la recopilación de datos e información será la *entrevista*, que implica dirigir preguntas a los beneficiados ya sea individualmente o por grupos.

La entrevista se utilizará como instrumento principal para la recopilación de las necesidades de los usuarios, para la recopilación de información acerca del estado de la infraestructura del Banco en general, así como de las características de seguridad necesarias.

4. Procedimientos para analizar la información del diagnóstico

Después de haberse aplicados los instrumentos de recolección de datos, para el tratamiento de la información se clasificará de manera que permita tener un panorama de las necesidades y del problema a resolver.

Posteriormente, se generará una lista de requerimientos técnicos necesarios y relacionados con las diferentes áreas de la Auditoría Interna y se clasificarán de acuerdo con sus correspondientes interrelaciones.

Una vez identificadas las interrelaciones, los requerimientos técnicos, infraestructura y seguridad se procederán a realizar una matriz en donde plasme de manera ordenada los requerimientos para el diseño e implementación de un piloto.

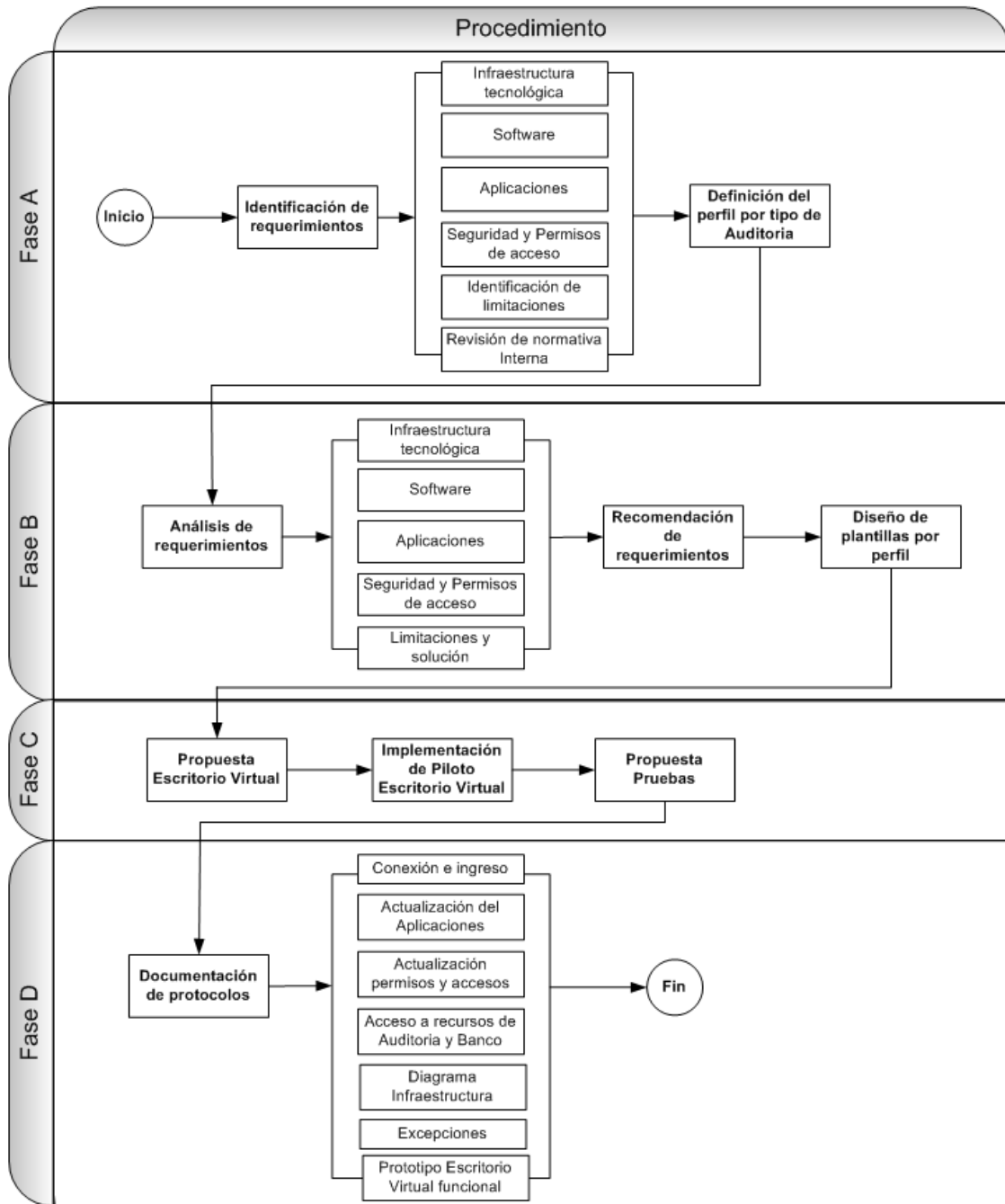


Figura 3. Fases y elementos a considerar en el desarrollo del prototipo de Escritorios Virtuales para la Auditoría Interna del Banco de Costa Rica. Elaboración propia.

Para el desarrollo de dicho proyecto, se estiman 98 días, contando con el apoyo de la Gerencia de Auditoría de Tecnología de Información, con los recursos de tiempo y humano para el desarrollo de las actividades propuestas a continuación:
















	 Nombre de tarea	Duración	Comienzo	Fin	Predecesora	Nombres de los recursos
1	 Proyecto - Escritorio Remoto	98 días	lun 3/8/20	mié 16/12/20		Cristian Solano Chacón
2	 FASE A- Requerimientos de la Auditoria	30 días?	lun 3/8/20	vie 11/9/20		
3	  Reunión inicial con Patrocinador	1 día?	lun 3/8/20	lun 3/8/20		Cristian Solano Chacón
4	 Recursos tecnológicos	4 días	mar 4/8/20	vie 7/8/20		
5	 Identificación y creación de los recursos en la plataforma virtual del Banco	1 día	mar 4/8/20	mar 4/8/20	3	Cristian Solano Chacón
6	 Identificación de la infraestructura de Red y Servidores de la Auditoria	2 días	mié 5/8/20	jue 6/8/20	5	Cristian Solano Chacón
7	 Documentación configuración de escritorio remoto	1 día	vie 7/8/20	vie 7/8/20	6	Cristian Solano Chacón
8	 Identificación de requerimientos de software y hardware para uso de la Auditoria	25 días	lun 10/8/20	vie 11/9/20		
9	 Entrevistas con funcionarios Administradores de la Red de la Auditoria	1 día	lun 10/8/20	lun 10/8/20	7	Cristian Solano Chacón
10	 Entrevistas con funcionarios de la Auditoria de Tecnología	1 día	mar 11/8/20	mar 11/8/20	9	Cristian Solano Chacón
11	 Entrevistas con funcionarios de la Auditoria Financiera	1 día	mié 12/8/20	mié 12/8/20	10	Cristian Solano Chacón
12	 Entrevistas con funcionarios de la Auditoria de Areas de Apoyo	1 día	jue 13/8/20	jue 13/8/20	11	Cristian Solano Chacón
13	 Entrevistas con funcionarios de la Auditoria de Operaciones	1 día	vie 14/8/20	vie 14/8/20	12	Cristian Solano Chacón
14	 Entrevistas con funcionarios de la Auditoria Banca Corporativa	1 día	lun 17/8/20	lun 17/8/20	13	Cristian Solano Chacón
15	 Entrevistas con funcionarios de Auditoria Banca de Personas	1 día	mar 18/8/20	mar 18/8/20	14	Cristian Solano Chacón
16	 Entrevistas con funcionarios de la Auditoria Continua	1 día	mié 19/8/20	mié 19/8/20	15	Cristian Solano Chacón
17	 Entrevistas con funcionarios de la Auditoria General	1 día	jue 20/8/20	jue 20/8/20	16	Cristian Solano Chacón
18	 Documentación de lista de requerimientos	2 días	vie 21/8/20	lun 24/8/20	9;10;11;12;13;14	Cristian Solano Chacón
19	 Entrevistas con funcionarios administradores de la Infraestructura Virtual del Banco	1 día	mar 25/8/20	mar 25/8/20	18	Cristian Solano Chacón
20	 Entrevistas con funcionarios administradores de la Seguridad de TI del Banco	1 día	mié 26/8/20	mié 26/8/20	19	Cristian Solano Chacón
21	 Revisión de normativa del Banco y Auditoria	7 días	jue 27/8/20	vie 4/9/20		
22	 Infraestructura Virtual y Física	3 días	jue 27/8/20	lun 31/8/20	20	Cristian Solano Chacón
23	 Seguridad	3 días	mar 1/9/20	jue 3/9/20	22	Cristian Solano Chacón
24	 VDI	1 día	vie 4/9/20	vie 4/9/20	23	Cristian Solano Chacón
25	 Inventarios	3 días	lun 7/9/20	mié 9/9/20		
26	 Funcionarios por perfil	1 día	lun 7/9/20	lun 7/9/20	24	Cristian Solano Chacón
27	 Software por perfil (Banco-Auditoria)	1 día	mar 8/9/20	mar 8/9/20	26	Cristian Solano Chacón
28	 Aplicaciones por perfil (Banco-Auditoria)	1 día	mié 9/9/20	mié 9/9/20	27	Cristian Solano Chacón
29	 Documentación Análisis de requerimientos versus lo posible	2 días	jue 10/9/20	vie 11/9/20	28	Cristian Solano Chacón
30	 FASE B - Diseño	18 días	lun 14/9/20	mié 7/10/20		
31	 Análisis y recomendación de hardware requerido para escritorio virtual	2 días	lun 14/9/20	mar 15/9/20	29	Cristian Solano Chacón
32	 Análisis y recomendación de software requerido para escritorio virtual	2 días	mié 16/9/20	jue 17/9/20	31	Cristian Solano Chacón
33	 Análisis y recomendación de acceso y navegación permitida desde escritorio virtual	2 días	vie 18/9/20	lun 21/9/20	32	Cristian Solano Chacón
34	 Análisis de limitaciones del escritorio virtual vs escritorio normal	2 días	mar 22/9/20	mié 23/9/20	33	Cristian Solano Chacón
35	 Análisis y recomendación de solicitud de permisos según la normativa	2 días	jue 24/9/20	vie 25/9/20	34	Cristian Solano Chacón
36	 Análisis y recomendación de infraestructura para administración del escritorio remoto	2 días	lun 28/9/20	mar 29/9/20	35	Cristian Solano Chacón
37	 Análisis y recomendación de herramientas de conexión e ingreso a la VDI y escritorio remoto	1 día	mié 30/9/20	mié 30/9/20	36	Cristian Solano Chacón
38	 Análisis y recomendación de herramientas de seguridad para validación y conexión	1 día	jue 1/10/20	jue 1/10/20	37	Cristian Solano Chacón
39	 Diseño general de la conexión-navegación-acceso a recursos del Banco-Auditoria	4 días	vie 2/10/20	mié 7/10/20	38	Cristian Solano Chacón
40	 FASE C - Propuesta de Implementación	11,5 días	jue 8/10/20	vie 23/10/20		
41	 Escritorio Virtual en el Banco	6 días	jue 8/10/20	jue 15/10/20		
42	 Desarrollo de escritorio master para la Auditoria	1 día	jue 8/10/20	jue 8/10/20	39	Cristian Solano Chacón
43	 Instalación de software del Banco y de la Auditoria	2 días	vie 9/10/20	lun 12/10/20	42	Cristian Solano Chacón
44	 Instalación de aplicaciones del Banco y de la Auditoria	2 días	mar 13/10/20	mié 14/10/20	43	Cristian Solano Chacón
45	 Solicitud de permisos de acceso requeridos	1 día	jue 15/10/20	jue 15/10/20	44	Cristian Solano Chacón
46	 Estación de trabajo física en la Auditoria	2 días	vie 16/10/20	lun 19/10/20		
47	 Solicitud e instalación de herramientas y componentes de seguridad para el usuario	2 días	vie 16/10/20	lun 19/10/20	45	Cristian Solano Chacón
48	 Pruebas Escritorio Remoto	3,5 días	mar 20/10/20	vie 23/10/20		
49	 Ingreso a herramientas de comunicación y acceso a la VDI	0,5 días	mar 20/10/20	mar 20/10/20	47	Cristian Solano Chacón
50	 Ingreso al escritorio virtual y validación	0,5 días	mar 20/10/20	mar 20/10/20	49	Cristian Solano Chacón
51	 Navegación en la red del Banco y de la Auditoria	0,5 días	mié 21/10/20	mié 21/10/20	50	Cristian Solano Chacón
52	 Ingreso a recursos compartidos del Banco y Auditoria	1 día	mié 21/10/20	jue 22/10/20	51	Cristian Solano Chacón
53	 Ingreso a las aplicaciones	1 día	jue 22/10/20	vie 23/10/20	52	Cristian Solano Chacón
54	 FASE D - Documentación	8 días	vie 23/10/20	mié 4/11/20		
55	 Protocolo de conexión-ingreso-cierre en el escritorio remoto	1 día	vie 23/10/20	lun 26/10/20	53	Cristian Solano Chacón
56	 Protocolo de actualización de permisos	1 día	lun 26/10/20	mar 27/10/20	55	Cristian Solano Chacón
57	 Protocolo de mantenimiento y actualización de software-aplicaciones	2 días	mar 27/10/20	jue 29/10/20	56	Cristian Solano Chacón
58	 Protocolo de acceso recursos compartidos	2 días	jue 29/10/20	lun 2/11/20	57	Cristian Solano Chacón
59	 Protocolo para limitaciones	2 días	lun 2/11/20	mié 4/11/20	58	Cristian Solano Chacón
60	 Finalización y entrega del proyecto	30 días	mié 4/11/20	mié 16/12/20	59	Cristian Solano Chacón
61	Documentación del Proyecto para la Universidad	30 días	mié 4/11/20	mié 16/12/20	59	Cristian Solano Chacón

Figura 4. Cronograma de actividades para la ejecución del proyecto. Elaboración propia.

CAPÍTULO IV
PROPUESTA DE SOLUCIÓN

CAPÍTULO IV: PROPUESTA DE SOLUCIÓN

1. Diagnóstico

En este capítulo se presenta el resultado de los registros de datos obtenidos de las entrevistas realizadas a los usuarios expertos, tanto de las áreas de Virtualización de Infraestructura en TI, Seguridad de la Información y de Telecomunicaciones del BCR, así como de los Administradores de la infraestructura de la Auditoría y sus funcionarios.

1.1 Situación actual:

De las entrevistas realizadas a usuarios expertos de las áreas de tecnología antes mencionadas y sesión de trabajo con los administradores de la infraestructura de la Auditoría Interna del Banco de Costa Rica documentadas en el **Anexo N° 01** se determinó como situación actual lo siguientes:

1.1.1 Requerimientos de usuarios

Los funcionarios de la Auditoría requieren de una serie de herramientas, aplicaciones y fuentes de datos sin excepción para sus labores diarias, y otras herramientas y aplicaciones exclusivos según el área dentro del departamento de Auditoría Interna en el que trabajan o estudios de Auditoría que realicen. Lo anterior incluye el acceso a Internet, intranet del BCR y de la Auditoría.

La Auditoría Interna se divide organizacionalmente en varias áreas, dependiendo de las áreas de negocio y soporte del Banco, por lo que esto puede variar a través de los años, sin embargo, las herramientas, aplicaciones y fuentes de datos principales no cambian.

El Conglomerado Financiero BCR, además de contar con su departamento de Auditoría Interna, cuenta con Sociedades Anónimas que tienen su propio departamento de Auditoría Interna, con las mismas y particulares necesidades de acceso a información, aplicaciones y herramientas.

Los requerimientos de estaciones de trabajo para el desarrollo de sus funciones son actualmente de equipos portátiles configurados con 8GB de memoria RAM, 250GB de disco duro, 4 procesadores Intel Core i7 (8 núcleos) y conexión inalámbrica.

Se requiere mantener en todo momento las actualizaciones del sistema operativo de las estaciones de trabajo, así como el antivirus, los cuales se actualizan cuando están conectadas a una red del BCR.

La Auditoría Interna del BCR, provee a sus funcionarios y otros departamentos del Banco, información consolidada y procesada por el mismo departamento. Esta información se provee por medio de bases de datos, sistemas desarrollados a lo interno de la Auditoría. Esto implica que la Auditoría Interna mantiene y administra sus propios equipos servidores tanto físicos como virtuales, así como el soporte de aplicaciones, herramientas y estaciones de trabajo, incluyendo el acceso y la seguridad de estos elementos. Lo anterior basado en la independencia funcional y tecnológica que requieren para hacer su trabajo y adquirir conocimiento con laboratorios propios.

Lo anterior, conlleva todo el tema de administración de seguridad, obsolescencia, monitoreo y gestión de recursos tecnológicos.

Las labores de la auditoría, requieren que sus funcionarios se desplacen a las oficinas del Banco en todo el territorio nacional, con el mismo acceso y comunicación que tienen en las oficinas de la Auditoría Interna.

Cabe destacar que los funcionarios de las Auditorías Internas de cada Sociedad Anónima del Conglomerado BCR, actualmente utilizan algunos de los servicios que la Auditoría Interna usa y administra.

1.1.2 Requerimientos de seguridad

El área de Seguridad de TI del BCR, exige que todo sistema o dispositivo que se integre consuma servicios internos o se conecte a la red del Banco debe hacerlo utilizando protocolos seguros y con conexiones cifradas; esta última debe utilizar algoritmos de cifrado vigentes y que no hayan sido vulnerados. Además, toda autenticación de usuarios se debe hacer por medio del servicio de ADFS del Banco.

Los sistemas que se utilicen desde la red del Banco deben contar con roles definidos según sea necesario y dependiendo de la naturaleza del sistema; No se deben utilizar usuarios locales para la administración de los sistemas, es decir, los usuarios que conforman los respectivos roles de cada sistema deben ser los dispuestos en el Directorio Activo del Banco o en cualquier otro sistema autorizado por la Gerencia de Seguridad de TI.

En cuanto a la seguridad lógica interna y externa, se deben de solicitar los permisos de firewalls necesarios y de navegación que no atenten contra la normativa interna de seguridad del BCR.

No se permite bajo ninguna circunstancia acceder información desde un ambiente virtual y trasladarla a un ambiente físico o medio de almacenamiento externo y viceversa. Esta restricción permitirá evitar y minimizar el riesgo de que se comprometa información sensible al trasladarse de un ambiente a otro, por otro lado, evitar infección de ambientes virtuales desde ambientes físicos.

1.1.3 Requerimientos de conexión

Solo se permitirá conectarse desde una red externa al Banco por medio de una VPN implementada con herramientas adquiridas por el Banco, que permitan una comunicación cifrada y segura, lo cual es proveído para este caso por el Firewall Palo Alto.

Deben utilizarse mecanismos de validación y encriptación de datos durante la validación de la conexión, como certificados digitales. La conexión a recursos virtuales como los Escritorios se hará por medio de los clientes para aprovisionamiento de escritorios, para este caso VMWare Horizon Client.

1.1.4 Documentación para la gestión de Escritorios Virtuales

Para la administración sana de recursos tecnológicos, es recomendable la elaboración de la documentación respectiva para la instalación y configuración de herramientas y sistemas, así como de guías para los usuarios, con las instrucciones de ingreso, utilización de solución de los Escritorios Virtuales, y en el caso de los administradores, las instrucciones para la configuración de estos ambientes.

Lo anterior, está consolidado en el **Anexo N° 02 - Matriz Requerimientos – Propuesta - Implementado**, en donde se listaron los requerimientos de sistemas, herramientas, plataformas y documentación requeridos para la implementación, gestión y mantenimiento de los Escritorios Virtuales para la Auditoría Interna y Auditorías de las Sociedades Anónimas del Conglomerado Financiero del BCR.

1.1.5 Recursos disponibles

El Banco de Costa Rica, tiene implementada una solución de virtualización en los Centros de Datos, con la plataforma VMWare que proporciona software de virtualización que corre tanto en Windows, Linux y macOS, en donde se tienen los ambientes de desarrollo, pruebas y producción de los sistemas del Banco, con la capacidad de brindar servicios de escritorios virtuales.

Tabla 1.

Matriz de soporte por parte del proveedor

Producto	Disponibilidad General	Fin Soporte General	Fin Orientacion Tecnica
Vmware Horizon View 7.7	22/03/2016	22/03/2021	22/03/2023
Vmware vSphere 6.5 U2	15/11/2016	15/11/2021	15/11/2023
Vmware vSAN 6.6	15/11/2016	15/11/2021	15/11/2023
Vmware NSX 6.4	16/01/2018	16/01/2021	16/01/2022
vCenter Server 6.5 and 6.7	15/11/2016	15/11/2021	15/11/2023

Fuente: Tomados del Diseño Solución VDI.pdf documentado por la Gerencia

Infraestructura de TI-BCR (04- 2020)

Se indican los productos VMware utilizados en la solución de los Escritorios Virtuales en el Banco de Costa Rica.

Se cuenta con contratos de mantenimiento y soporte por cuatro años, tanto para los servidores como para los productos licenciados de VMWare, los cuales se renuevan constantemente para mantener la plataforma de servidores y servicios del BCR funcionando.

La plataforma para VDI, se configura de un clúster de 8 nodos en el Centro Procesamiento Principal y otro clúster de 8 nodos en el Centro Alterno Procesamiento, todos servidores HP de RACK que proveen balanceo de cargas y redundancia. Cada servidor Host cuenta con 640 GB de memoria RAM, dos procesadores de 28 núcleos, 2 tarjetas de red a 10 gigas para (Administración, vSAN y vMotion) y 4 a 1 giga para máquinas virtuales.

En la vSAN configurada actualmente, cada host tiene todos los discos duros SSD y habilita la opción de construir una vSAN All Flash, con aprovechamiento de reglas para el uso de RAID 5 y RAID6 con una disminución de espacio en Storage. Sobre la vSAN All Flash, se aplica la configuración de Deduplicación y compresión, con ahorro muy importante de espacio en Storage.

Hypervisor: VMware ESXi, 6.5.0, 10884925
 Model: ProLiant DL380 Gen10

Location	Total Memory Slots
Processor 1	12
Processor 2	12

Total Memory	Operating Frequency
320 GB	2400 MHz
320 GB	2400 MHz

Processor Name	Intel(R) Xeon(R) Gold 5120 CPU @ 2.20GHz
Processor Status	OK
Processor Speed	2200 MHz
Execution Technology	14/14 cores; 28 threads
Memory Technology	64-bit Capable
Internal L1 cache	896 KB
Internal L2 cache	14336 KB
Internal L3 cache	19712 KB

Figura 5. Características de cada Host del clúster en el CPP y CAP. Tomados del Diseño Solución VDI.pdf documentado por la Gerencia Infraestructura de TI-BCR (04- 2020).

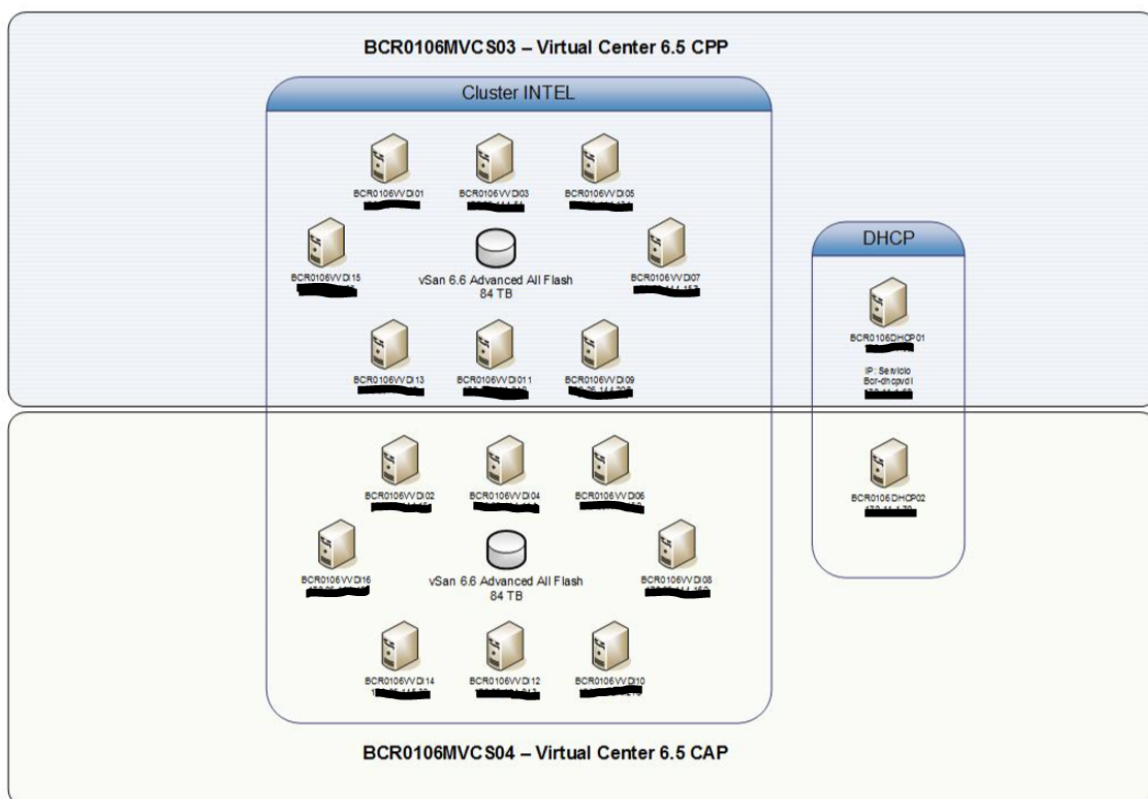


Figura 6. Infraestructura vSphere y vSAN en el CPP y CAP.

Fuente: Tomado del Diseño Solución VDI.pdf documentado por la Gerencia Infraestructura de TI-BCR (04- 2020).

El BCR cuenta con una plataforma para la generación y gestión de Certificados Digitales, así como de tecnología de Firewall Palo Alto para establecer VPN y validación de usuarios de dominio por medio del Active Directory corporativo. Por razones de seguridad, no se adjunta el diseño de estas plataformas.

En la actualidad, la forma de cómo se conecta un funcionario Auditor a los recursos tecnológicos del Banco es por medio de la red interna accedida desde las Oficinas

Centrales, séptimo piso en las Oficinas de la Auditoría Interna, como se muestra a continuación:

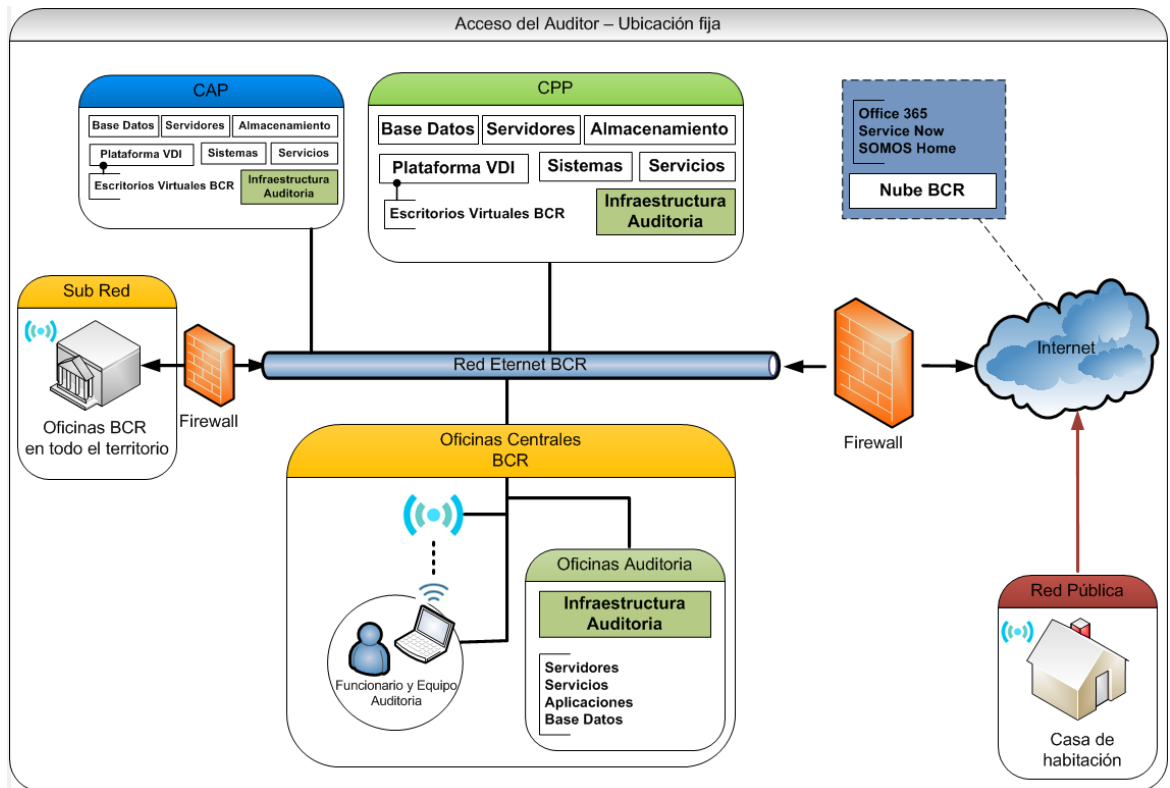


Figura 7. Acceso a los recursos informáticos antes de la propuesta, utilizados por el Auditor desde una única ubicación. Elaboración propia.

2. Propuesta de solución

En este apartado, se describirá como se atendió cada uno de los requerimientos del funcionario de la Auditoría Interna del Banco de Costa Rica, para que este pueda tener el mismo acceso a la información y herramientas en escritorios virtuales remotos como los utiliza en las oficinas de la Auditoría Interna en la red del Banco.

Dado que la Auditoría Interna es un área que necesita mantener independencia técnica y operacional de la Gerencia de Tecnología del BCR, se ha caracterizado de ser autónoma en la administración de infraestructura de TI propia, desarrollo de software, configuración y gestión de estaciones de trabajo desde hace 20 años. Por esta razón el conocimiento y responsabilidad de cómo se instalan y configuran las herramientas de Auditoría Interna, recaen en un grupo de funcionarios de la Gerencia de Auditoría de TI.

Por lo anterior, el proceso de creación de escritorios virtuales los debe de realizar estos funcionarios. En lo particular a esta propuesta, lo lidera el funcionario con mayor tiempo de administrar la infraestructura de TI en la Auditoría, como administrador principal, situación que garantiza que la operación es la más adecuada y con un funcionario altamente calificado.

El proceso inicia solicitando la creación de una **Master** de escritorio virtual, con solo el sistema operativo instalado ya que el licenciamiento es administrado por la Gerencia de Tecnología, la creación la Master se genera con 8 gigas en RAM y una segunda partición D de 5 gigas de almacenamiento. Una vez que se crea dicha Master, se le asigna una dirección IP, usuario y clave de acceso para tomar control de la misma por medio de *Remote Control Desktop* desde una estación de trabajo en la Auditoría Interna.

Cabe destacar que el antivirus de cada Escritorio Virtual es instalado y configurado como parte de las políticas del Dominio BCR al realizar la tarea de **Recompose**, que es el proceso que prepara la Master para la creación de nodos clonados a partir de esta que despliegan los Escritorios Virtuales por demanda, en el caso de la Auditoría se solicitaron nodos en el pool designado dentro de la plataforma VDI del BCR.

La forma como los auditores tienen acceso a estos recursos es por medio de un grupo de Active Directory del BCR que se crea para dicho fin.

El administrador principal, realiza la instalación de las herramientas del Departamento de la Auditoría Interna tal como se instalan en una estación de trabajo física. Se identificaron los puertos de las aplicaciones (Lotus Domino, Cliente Lotus Notes, GEA, SGA), así como del direccionamiento IP y puertos de comunicación para solicitar los permisos de firewall respectivos de acceso desde la vlan 1800 en la que se encuentran los Escritorios Virtuales de la plataforma VDI del BCR hacia los servidores y sitios con la información de la Auditoría.

2.1 Requerimientos de usuarios

2.1.1 Herramientas de trabajo

Los funcionarios de la Auditoría requieren de una serie de herramientas o aplicaciones para realizar sus labores diarias, las cuales se clasificaron en las de uso común para todos.

El aplicativo principal de trabajo para todos los auditores es GPA, implementado en plataforma Lotus Domino, se debe de configurar cada cliente Notes con el perfil del usuario que utilizará el escritorio remoto, y dado que estos escritorios remotos son destruidos y creados cada que un usuario solicita uno de ellos, la configuración que se realice no permanecerá en los escritorios. Para resolverlo, se diseñó un proceso en el cual se configura cada cliente Notes para cada usuario de la Auditoría con su perfil de red en un escritorio virtual, y se programa un script para DOS que traslade los archivos de configuración del perfil del usuario para Lotus Notes a un servidor de archivos que centraliza esa información.

En la Master se programa una rutina de código en un script para que se ejecute al iniciar el sistema operativo de manera que copie del servidor de archivos según su perfil de usuario identificado por la cédula, los archivos de configuración de Notes que le permite posterior a esta carga abrir Lotus con la configuración de su perfil, esta configuración se realiza también para los usuarios administradores de la plataforma Lotus Domino con el fin de gestionar usuarios, bases de datos y otras labores en dicha plataforma.

A demás, de este particular aplicativo se configura el ambiente de Windows tal cual se configura en las estaciones físicas de cada usuario, con el fin de que una vez que lo utilice, tenga las mismas funcionalidades.

Otras de las herramientas indispensables lo son los productos de la suite Office, que por costos de licenciamiento no se instalan en la Master de VDI, esto implicaría un gasto doble de licencia por usuario (*una en la estación de trabajo y otra para el escritorio virtual*). En su lugar se buscó un producto de distribución libre y que tuviera compatibilidad con los productos de Microsoft Office y que a la vez cumpliera con las demandas de seguridad requeridas para su utilización. Este producto es *Libre Office versión 6.4*, que permite ver y editar los documentos de la última versión de Office de Microsoft.

Para la intranet del BCR se instala Chrome como navegador por defecto y para la intranet de la Auditoría Interna se instala internet Explorer con compatibilidad 8.0, esto dado que el sitio de la para este departamento esta implementado en un servidor de Lotus Domino, sitio que se está diseñando y programando en versiones más seguras.

Debido a que la forma de trabajar los escritorios virtuales está basado en una plantilla Master que genera la cantidad de nodos especificados y que la personalización de escritorios requiere una Master diferente, considerando que esto aumentaría los costos, se concentraron todas las aplicaciones comunes en una sola plantilla Master.

El acceso a los escritorios virtuales se realiza principalmente fuera de la red del Banco, por lo que los productos de antivirus y parchado de sistemas operativos dejan de funcionar en cuanto a su mecanismo de actualización que es constante. Para solucionar este tema, se diseñan y configuran políticas de equipo en el Subdominio de la Auditoría Interna, que permitan que las estaciones de trabajo físicas puedan conectarse a servidores del proveedor de antivirus para sus actualizaciones.

Con respecto a las actualizaciones de sistemas operativos de las estaciones de trabajo, se implementa en la Auditoría Interna la misma herramienta de parchado del BCR, de forma que los administradores de infraestructura de esta área puedan controlar que parches o actualizaciones de sistemas operativos que se liberan a cada estación de trabajo, esto se realiza por medio de VPN que permite la conexión remota a cada computadora indiferentemente a que red esté conectada.

Las herramientas de antivirus y parchado antes mencionados, están configurados por defecto para que solo dentro de la red del Banco se actualicen.

Para proveer a los administradores de infraestructura de la Auditoría Interna del BCR, de las herramientas para gestionar información consolidada en servidores de archivos y bases de datos, desarrollo y mantenimiento de sistemas y administración de servidores tanto

físicos, se instalan las aplicaciones y herramientas necesarias en la Master y que se tengan en cada nodo de escritorio virtual.

Para lo antes mencionado se gestionaron los permisos de acceso por Active Directory y Firewall desde la vlan 1800 en donde se gestan los Escritorios Virtuales.

En cada estación de trabajo, se instalan los productos de Global Protect para conectarse por VPN y VMWare Horizon Client para acceder a los Escritorios Virtuales de forma remota, que permitirán conectarse de forma segura y validarse con usuario del BCR, y acceder a los nodos de escritorios virtuales disponibles. Como complemento a la validación segura, se solicitan crear certificados digitales asociado a la identificación de cada estación de trabajo y usuario que son instalados en el equipo previamente.

Con respecto a la limitación de copiar información desde y hacia los escritorios remotos y estaciones de trabajo, se analizó las características del portal de la intranet del BCR llamado SOMOS, este portal permite a cada funcionario del BCR tener un espacio personal para subir, almacenar y descargar archivos. Dicha característica se prueba y documenta para que utilizándolo como espacio de almacenamiento en la nube privada del Banco, pueda ser accedida desde los escritorios remotos y estaciones de trabajo, permitiendo subir y descargar archivos, resolviendo el tema del traslado de información de un ambiente a otro.

Lo anterior, no materializa el riesgo de comprometer información por el medio de transferencia o malware, dado que tanto el origen como el destino están protegidos por los mecanismos de antimalware y vulnerabilidades.

También se establecen políticas de navegación desde los escritorios remotos, con el fin de que el usuario no pueda acceder sitios o páginas en internet que puedan comprometer el ambiente virtual.

Con el fin de administrar los escritorios virtuales para el área de la Auditoría Interna, permitiendo la actualización de estos y la utilización de los mismos por los auditores, se desarrolla la documentación técnica asociada a:

- o Instalación y configuración en la Master de escritorios virtuales.
- o Instalación y configuración de cada una de las aplicaciones utilizadas por funcionarios de la Auditoría Interna.
- o Manuales de usuario para la utilización de escritorios virtuales del Departamento
- o Inventario de permisos, puertos, direccionamiento IP, servidores, aplicaciones, plataformas para la Auditoría Interna
- o Actualización del plan de Contingencia y Continuidad de la Auditoría Interna

2.1.2 Situaciones no previstas

El año 2020 para el mundo entero, ha cambiado la forma de trabajar, estudiar, producir y de vivir para cada persona, esto provocado por la pandemia de **COVID-19** desde marzo 2020. Como un efecto colateral y dado las nuevas formas de vivir y realizar las transacciones de toda índole, el grupo denominado MAZE (*grupo de ciberdelincuentes*) se aprovechó de esta situación para realizar una serie de ataques contra la imagen e información de diversas entidades, en Costa Rica una de estas entidades objeto de ataques lo fue el Banco de Costa Rica, con la **presunta** información de clientes comprometidos.

Ambas situaciones, generaron que esta entidad Bancaria analizara sus esquemas de seguridad y acceso a la información, requiriendo de hacer mejoras y reforzar los mecanismos actuales para aseguraran aún más la información que almacena, procesa y utiliza para su negocio.

Indiferentemente de las acciones preventivas que realizará la administración del Banco y el área de TI, la Auditoría Interna del Banco realiza las suyas y acata las sugeridas por el área de Seguridad en Tecnología del BCR, esto dado que administra su propia infraestructura y que tiene acceso a la información sensible de clientes y del Banco.

En primera instancia, los aspectos a mejorar están basados en las mejores prácticas de Ciberseguridad acatadas por el Banco, requiriéndose lo siguiente con base a la nueva forma de trabajo y acceso a información por los funcionarios del BCR:

- o Escritorios Virtuales distintos de los utilizados por un usuario regular para la administración de infraestructura de la Auditoría Interna y acceso a recursos de administración de la infraestructura del BCR como lo con las herramientas de monitoreo, escaneo de vulnerabilidades y correlación de eventos, vCenter, carpetas compartidas y otras herramientas de gestión de infraestructura. Para este requerimiento se solicita una nueva Master con 8 gigas en RAM y una segunda partición D de 10 gigas de almacenamiento. Lo particular de esta nueva Master es que la validación se estará reforzando con el enrolamiento de la tarjeta de Firma Digital como un mecanismo más de validación.

Para robustecer aún más la seguridad de acceso, se crean cuentas especiales en el Dominio del BCR para cada uno de los usuarios administradores de infraestructura de la Auditoría Interna, la cual es la única cuenta válida para acceder este Escritorio Virtual.

En el caso de la Auditoría Interna, el acceso a los servidores que administra solo se hará por medio de un usuario de cuenta especial en el Subdominio del mismo departamento, sumando un mecanismo más de seguridad.

- o Requerimiento de aseguramiento de servidores de la Auditoría Interna, lo cual se logró creando una DMZ en la red de servidores del BCR y separando los servidores en los dos Centro de Datos. Este proceso requirió la identificación de puertos permitidos para acceder a la nueva DMZ.

- o Cambio del Dominio de la Auditoría Interna a un Subdominio, el cual permite una mejora administración de políticas de dominio, usuarios y grupos de dominio que puedan ser utilizados en el dominio del BCR.

- o El tema de la pandemia obliga a todos los funcionarios del BCR a realizar teletrabajo todos los días, esto incluye a los Auditores de las Sociedades Anónimas del Conglomerado, lo que crea la necesidad de utilizar en los Escritorios Virtuales proveídos por el Banco, las aplicaciones utilizadas y desarrolladas por la Auditoría Interna como Lotus Notes, SGA, Intranet de la Auditoría, lo que requiere un esfuerzo de más para permitir la convivencia de estos aplicativos y su administración en recursos administrador por el BCR.

- o Eliminación de obsolescencia en servidores y aplicaciones, riesgos acelerados por la aparición de la amenaza de MAZE, lo que obliga en el estado de pandemia y de teletrabajo a utilizar el prototipo de Escritorios Virtuales con acceso remoto para realizar todas las actividades de gestión y administración de servidores en la infraestructura de la Auditoría Interna, que conlleva la creación, instalación, configuración y parchado de servidores, así como la migración de estos desde una red a la DMZ y la migración de datos y aplicativos en un nuevo Subdominio.

- o Atención de nuevos proyectos y necesidades en el departamento de Auditoría Interna sin afectar los servicios a los funcionarios, utilizando el prototipo de Escritorios Virtuales, actualización y monitoreo de respaldos.

3. Validación de la propuesta

A continuación, se detalla el funcionamiento, proceso, aspectos técnicos y de seguridad, así como el flujo que conforma la propuesta de Escritorio Virtual para la Auditoría Interna, el cual brinda acceso remoto a sistemas y aplicaciones del BCR y esta área.

Como pre-requisito se requieren de las herramientas de validación y acceso, las cuales se instalan en los computadores de la auditoría con credenciales de administrador de Dominio, estos son el software Global Protect 3.0 para la conexión por VPN hacia la red y Data Center del Banco.

Se instala VMWare Horizon Client 4.10 para la conexión por VPN a la infraestructura de VDI en la red del Banco. Luego, se instala el Certificado Digital emitido por la Autoridad Certificadora propia del Banco, permitiendo cifrar la conexión.

El flujo de operación para el uso del recurso de Escritorio Virtual para la Auditoría Interna del BCR es el siguiente:

3.1 Conexión y validación del usuario

Se realiza el proceso de conexión en el Global Protect por medio de una dirección IP pre-configurada, digitando el usuario y clave del Dominio BCR que junto con el certificado digital asociado a la estación de trabajo son validados por la infraestructura de seguridad Active Directory, Firewall Palo Alto y PKI.

Dicha comunicación se establece por medio del puerto 443 TCP (túnel SSL) y configurando el cliente VMware Horizon Client. Una vez establecido el túnel entre el cliente y los firewall institucionales, se ingresan las credenciales del Dominio BCR para ser validadas por medio de las granjas externas de ADFS (Servicio Federador de Active Directory) para confirmar que el usuario solicitante es válido en el dominio de la organización.

3.2 Visualización de Escritorio Virtual

Se abre la aplicación VMWare Horizon Client, se ingresan el usuario y clave de dominio BCR para ser validados por la infraestructura de seguridad Active Directory del BCR, se mostrará el Escritorio Virtual al que tiene acceso y permisos de utilización. Al seleccionar el recurso se inicia el aprovisionamiento del Escritorio Virtual, el cual se crea, carga las políticas de Dominio, con todos los permisos solicitados como cuando se enciende un computador físico, una vez carga el sistema operativo, es necesario ingresar las credenciales de Dominio del usuario para acceder al ambiente virtual de trabajo y se crea el perfil de usuario con los permisos y accesos otorgados.

3.3 Carga de configuración específica para Lotus Notes

Se ejecutan de forma automática al inicio del sistema operativo un script .BAT que realiza la búsqueda del usuario logueado en el servidor de archivos en la Auditoría Interna en donde se mantienen almacenados por usuario la configuración e identidad de los usuarios de Lotus Notes, trasladando archivos de configuración al Escritorio Virtual. Una vez termina la ejecución del script el usuario cuenta con la configuración del ambiente Lotus Notes para utilizar el Sistema GPA, teniendo acceso a estudios, procedimientos, papeles de trabajo, gestión de tiempos y a la aprobación del flujo de estudios de auditoría en *Línea*.

En el caso de que el usuario logueado sea un Administrador de la plataforma Lotus Domino, se cargaran también su configuración para las actividades de gestión de servidores Domino, usuarios, grupos, roles, privilegios y certificados en dicha plataforma. Ambas configuraciones fueron realizadas y almacenadas con el usuario previamente en el ambiente de Escritorio Virtual.

3.4 Sitio de SGA y GEA

Por medio del navegador Chrome, el usuario puede ingresar a los sitios de Gestión de Auditoría y Gestión de Arqueos para sus actividades diarias.

3.5 Sitio de SOMOS BCR

Por medio del navegador Chrome, el usuario puede cargar e ingresar al sitio principal para los funcionarios de Banco de Costa Rica, en donde tendrá acceso a los recursos de Normativa Interna, sistemas de Capital Humano, Capacitación, Intranet de la Auditoría Interna y otros sistemas principales del BCR.

Por este medio es posible que el usuario pueda trasladar archivos desde la estación de trabajo al Escritorio Virtual y viceversa de forma segura y aceptada por el área de Seguridad de TI del BCR.

3.6 Recursos de Información

Por medio de rutas de red, se puede ingresar a recursos compartidos por servidores de la Auditoría Interna y del Banco, esto bajo el entendido que el usuario tiene acceso a los recursos compartidos dentro de la red. Según los permisos el usuario podrá leer, modificar o crear archivos y carpetas.

3.7 Recursos para Administración Infraestructura

Por medio de navegador Chrome, el usuario podrá administrar la infraestructura virtual por medio del vCenter de la Auditoría y consultar el vCenter del Banco, gestionando servidores e ingresando remotamente a estos en el caso de servidores de la Auditoría Interna y realizar cualquier gestión dentro del sistema operativo. Cabe destacar que se requiere una validación de usuario con privilegios de administrador.

3.8 Editores de archivos de Office

El usuario puede visualizar, editar y crear archivos de Word, Excel, Power Point de la Suite de Microsoft Office por medio del software Libre Office instalado. Este producto se instala para reducir el costo de una segunda licencia por usuario para el ambiente virtual.

3.9 Sistemas CORE

El usuario tendrá instalado, configurado el acceso a los sistemas principales de Cuentas SICC (Sistema Cuentas Corrientes) y AS/400 (Sistema Contable), por medio de una validación con el usuario regular que utiliza para estos sistemas y pudiendo descargar reportes.

3.10 Administración de infraestructura

Tomando como base la experiencia adquirida para la creación de los Escritorios Virtuales para los funcionarios Auditores, se crea un segundo Escritorio Virtual exclusivo para los Administradores de la Infraestructura de la Auditoría Interna, esto con el fin de contar con separación de permisos y redes a las que se acceden cuando es necesario conectarse a un servidor tanto de la Auditoría como del Banco y realizar funciones de administración con altos privilegios, esto permite una mejor trazabilidad de acciones que se realizan.

Para este Escritorio, se refuerza la seguridad con un mecanismo más de validación y una cuenta de usuario especial diferente a la normal del Dominio BCR, se realiza una configuración para enrolar una tarjeta de Firma Digital específica de cada funcionario de la Auditoría con rol de Administrador, utiliza la cuenta especial de dominio tanto en el acceso con VMWare Horizon Client como en el Escritorio Virtual de Administración.

En este Escritorio, se accede a las herramientas como vCenter, servidores por consola remota, herramientas de desarrollo, bases de datos, Active Directory.

3.11 Conocimiento adquirido para asesorar

Con la creación de dos tipos de Escritorios Virtuales, el administrador principal de Infraestructura de la Auditoría Interna, adquiere destrezas en virtualización de escritorios en plataformas VMWare, entiende la plataforma de VDI que el BCR tiene en producción, identifica las herramientas y mecanismos de seguridad, así como el conocimiento del funcionamiento de las herramientas y sistemas propios del departamento que le permitieron asesorar a los técnicos de la Mesa de Ayuda del BCR para la creación de los Escritorios Virtuales para los Auditores de las Sociedades Anónimas del Conglomerado Financiero BCR, los cuales no tenían la experiencia y desconocían como resolver las solicitudes de acceso a los recursos tecnológicos que utilizan en sus funciones cotidianas del área.

Importante señalar, que todo el conocimiento adquirido para la implementación de la propuesta permite mejorar estos ambientes virtuales, instalar y actualizar a necesidad en el ambiente virtual y de requerirse otras herramientas, se contara con la experiencia para atender otros requerimientos de los usuarios a futuro y por nuevos usuarios. También, permite identificar posibilidades para otras formas de acceder información de forma segura.

El diseño de la propuesta de Escritorios Virtuales para la Auditoría Interna del Banco de Costa Rica después de la implementación permitirá funcionalmente acceder a los recursos de información y de trabajo de la Auditoría Interna como del Banco, desde diferentes puntos de acceso dentro y fuera de la red Privada del BCR, como se muestra a continuación:

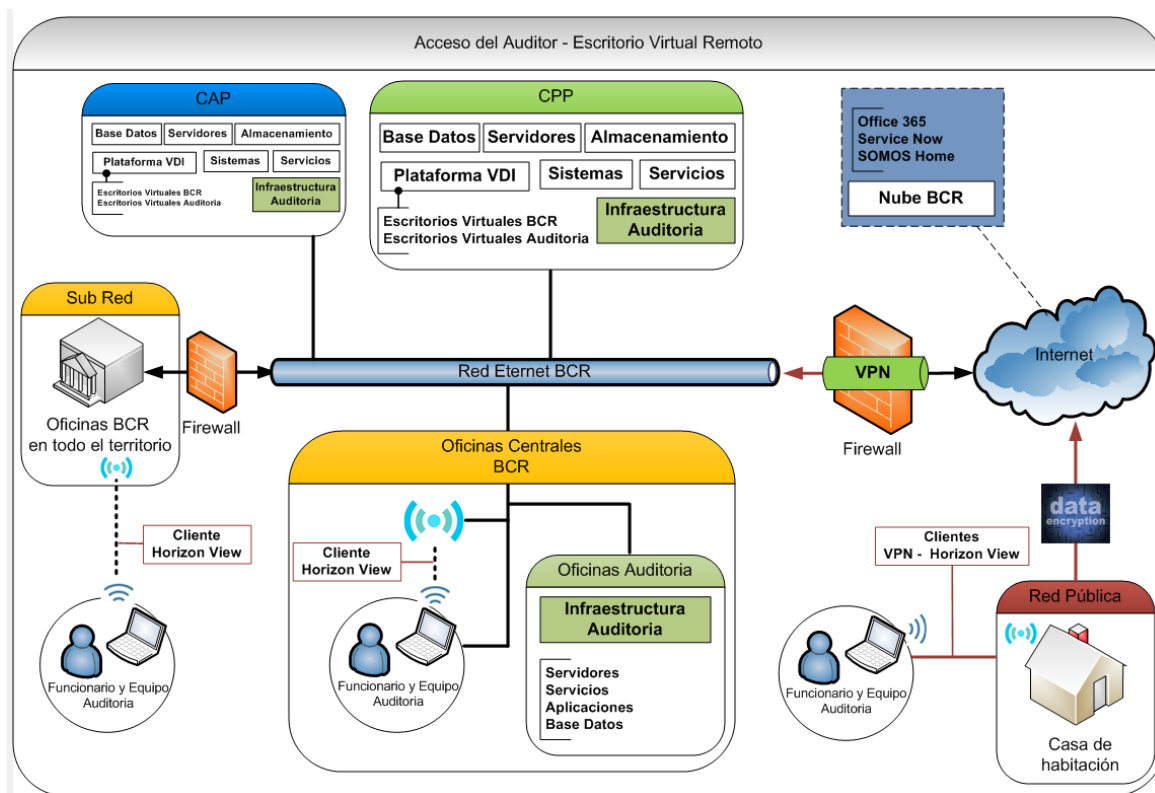


Figura 8. Acceso por Escritorio Virtual Remoto a los recursos informáticos, utilizados diariamente por el Auditor desde varias ubicaciones. Elaboración propia.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

1. Conclusiones

1. Se definió y configuró una plantilla Master para la creación de Escritorios Virtuales para la Auditoría Interna, que provee el software y aplicaciones configurados con los permisos de accesos para realizar todas las actividades diarias de la Auditoría Interna del Banco de Costa Rica, con esta configuración fueron incorporados todos los recursos que deben ser accedidos y utilizados por los auditores, obteniendo con ello la posibilidad de que los mismos puedan desarrollar sus funciones cotidianas sin ningún problema, asimismo, logrando definir una plantilla que puede ser utilizada en todo momento si fuera necesaria, además, que en todo momento puede estar susceptible a cambios de acuerdo con las necesidades del departamento.
2. Se elaboraron documentos técnicos para la administración, configuración, operación de los Escritorios Virtuales para la Auditoría Interna del Banco de Costa Rica, así como las guías para la capacitación y documentos de las estrategias de respaldos y continuidad. Dicha documentación es de suma importancia, puesto que le permite al departamento dejar evidencia de las acciones que fueron realizadas y si fuese necesario un cambio por cualquier motivo, cualquier profesional con los conocimientos puede visualizar la documentación del proceso y realizar las gestiones que correspondan según sea la necesidad.
3. Se implementa un prototipo funcional de Escritorio Virtual, que permite generar 63 nodos de Escritorios Virtuales para la Auditoría Interna del Banco de Costa Rica, con acceso desde la red privada del Banco y red pública (internet) para el uso diario en las labores de auditoría. Con ello se marca un precedente para la organización y para el área de Auditoría Interna, pues se logró homologar los recursos que son requeridos por el auditor en las oficinas de manera presencial a un ambiente virtual con las mismas condiciones y con la seguridad del funcionamiento de los recursos, pero en un ambiente teletrabajable y

alineados a las directrices emitidas por el Ministerio de Salud derivado de la Pandemia en la que nos encontramos.

Dado el caso de éxito de estos escritorios y debido a los riesgos expuestos por el **grupo MAZE**, que intenta afectar la imagen del BCR en aspectos de seguridad y supuestos datos comprometidos de clientes, se diseñó e implementó otra plantilla **Master para 5 Escritorios Virtuales** exclusivos para todas las labores de administración y gestión de infraestructura de la Auditoría, sumando otros factores de seguridad y validación con un **Certificado Digital**.

Como resultado del trabajo realizado y del diseño propuesto e implementado de Escritorios Virtuales para los funcionarios de la Auditoría Interna del Banco de Costa Rica, es posible concluir que el mismo logró las expectativas de la población a la cual se dirigió el producto, basado en que a la fecha de esta documentación, los auditores y de las Subsidiarias del Conglomerado Financiero BCR, están utilizando este recurso como herramienta para sus labores diarias de Auditoría desde su casas en esta emergencia por pandemia COVID-19.

Los Escritorios Remotos han proveído a la población de Auditores Internos del BCR y Subsidiarias de los mecanismos para trabajar remotamente de forma segura y con acceso a los sistemas de información del Banco y de Auditoría sin afectar el plan de labores para el 2020.

Esta propuesta implementada, permitió que los administradores de la infraestructura de la Auditoría Interna pudieran seguir administrando las aplicaciones, bases de datos, servidores; dando soporte a usuarios y estaciones de trabajo de forma remota y segura bajo las exigencias que demanda el acceso a este tipo de recursos.

También, fue posible implementar mejoras en la infraestructura del Departamento de la Auditoría Interna de seguridad, obsolescencia, nuevos productos y fuentes de información para las labores de auditoría, todo a través de los Escritorios Virtuales de forma remota, sin exponer información ni la salud de los Auditores del BCR.

Con efectos positivos, la propuesta permitió acatar la orden de Teletrabajo para auditores con un bajo impacto en cuanto a las herramientas a utilizar y fuentes de información, como un valor agregado en el tiempo de los Auditores trabajaron desde sus casas, se evidenciaron bajas en los gastos de electricidad, agua, suministros para baños y de limpieza, que permitieron que se tomara la decisión de reducir al 50% el espacio físico de las oficinas de la Auditoría, promoviendo el tema de cubículos de trabajo impersonales de uso común, fomentando el Teletrabajo permanentemente de 2 a 3 días por semana una vez que el tema de la pandemia permita regresar a las oficinas.

Esta propuesta evidencia beneficios tangibles para la Auditoría Interna en poco tiempo y un caso de éxito para el resto del Banco, que permitió seguir trabajando en las mismas condiciones que en la oficina en una situación de pandemia.



Figura 9. Distribución de teletrabajadores en total del BCR.

Fuente: Tomado de reportes internos de Capital Humano del Banco de Costa Rica para el año 2020.

Tabla 2.

Reducción de gastos de la Auditoría Interna del Banco de Costa Rica con Teletrabajo.

Rubro	Funcionarios	Tipo de Funcionario	
		Funcionario 1	Funcionario 2
Periodo en meses: 10			
Auditores: 63		55	8
Papelería y Útiles	₡ 616 000	₡ 9 778	₡ 9 778
Mantenimiento Mobiliario	₡ 470 000	₡ 7 460	₡ 7 460
Agua	₡ 9 450 000	₡ 150 000	₡ 150 000
Electricidad	₡ 25 200 000	₡ 400 000	₡ 400 000
Limpieza	₡ 7 850 769	₡ 124 615	₡ 124 615
Seguridad	₡ 12 664 615	₡ 201 026	₡ 201 026
Hospedaje-Alimentación	₡ 3 700 000		₡ 462 500
Total x tipo de funcionario:		₡ 892 879	₡ 1 355 379
TOTAL:		₡ 59 951 385	

Fuente: Tomados del informe de gastos interno de la Auditoría Interna para el año 2020.

Los montos indicados por cada rubro se dividen entre la cantidad de auditores para determinar el ahorro por cada uno de ellos, a excepción del rublo Hospedaje-Alimentación que solo se asocia a un grupo de ocho auditores. El monto ahorrado por cada tipo de funcionario se multiplica por la cantidad de cada tipo de funcionario y sumados para obtener un total ahorrado en 10 meses.

2. Limitaciones

Dentro de las limitaciones que se presentaron duran el desarrollo de la propuesta, se tienen que el personal técnico de las áreas de Virtualización del BCR, por todas las situaciones generadas por MAZE, se encontraban saturados de actividades prioritarias, lo que dejo con una prioridad baja el requerimiento de la Auditoría Interna de suplir Escritorios Virtuales con los requerimientos necesarios para las actividades diarias en el corto plazo.

Lo anterior, requirió que los Administradores de la Infraestructura del departamento de Auditoría Interna y en este caso el principal Administrador, realizaran todo el proceso de instalación de software, entendimiento de requerimientos funcionales, de seguridad, acceso, permisos y acceso a información y recursos informáticos a partir del producto inicial de la Master y acceso para acceder a esta.

Dado que los Administradores de Infraestructura de la Auditoría Interna tienen conocimiento en virtualización, servidores, acceso a software del Banco y otros, se hace uso de todos estos

recursos para analizar, investigar y realizar las actividades que permitieron poner en producción y disposición de todos los Auditores del BCR Escritorios Virtuales de acceso remoto.

3. Recomendaciones

1. En un plazo de 3 meses se configuren en la plantilla Master las mejoras de seguridad y optimización del Sistema Operativo el uso de los Escritorios Virtuales, y tratar en la medida de lo posible de no implementarlo con script y aplicaciones instaladas a través del sistema operativo.
2. En un plazo no mayor de un mes brindar una capacitación al personal que corresponda sobre el manejo de los Escritorios Virtuales y el soporte del uso de la documentación técnica generada para la administración, configuración, operación de los Escritorios Virtuales, así como las guías de capacitación y documentos de las estrategias de respaldos y continuidad, con el fin de facilitar y transmitir el conocimiento sobre esta solución y la tecnología utilizada a los demás funcionarios de la Auditoría Interna así como para la configuración de otros escritorios virtuales de las sociedades anónimas del Conglomerado BCR.
3. Implementar este prototipo funcional en un plazo menor a un mes considerando en todo momento utilizar la totalidad de nodos (63), necesarios para proveer a los funcionarios de la Auditoría Interna del BCR, de Escritorios Virtuales y realizar trabajo colaborativo y en línea desde diferentes ubicaciones geográficas, con el fin de identificar nuevas necesidades en las labores diarias.

4. Trabajos futuros

La solución implementada del prototipo funcional de Escritorios Virtuales de acceso remoto es la base para el desarrollo de opciones de conexión remotos para el funcionario auditor

del BCR, por lo que los administradores de Infraestructura de esta Auditoría Interna podrían realizar las siguientes mejoras:

- Implementación de perfiles de usuario para Escritorios Virtuales que permitan mantener una configuración completa en el sistema operativo (permisos, aplicaciones, variables de ambiente) como si fuera una estación de trabajo física.
- Implementación de herramientas que verifiquen la información que se traslada de un ambiente físico a uno virtual, validando sus permisos y permitiendo el copiado de una ambiente a otro.
- Habilidad de la navegación en Internet dentro de los Escritorios Virtuales con el aseguramiento del ambiente para evitar el riesgo de infiltración de malware.
- Habilidad de la utilización de office 365 dentro de los Escritorios Virtuales para la utilización de productos de Microsoft Office.
- Acceso a los Escritorios Virtuales desde otras estaciones de trabajo que no estén en el dominio del Banco, potenciando el uso equipos de menores recursos computacionales y personales como Tablet, Celulares, Laptop.
- Creación de Escritorios Virtuales con sistemas operativos diferentes de Windows.

Beneficios a futuro:

- Reducción de costos en la adquisición de equipos portátiles con recursos de procesamiento y almacenamiento altos, al poder conectarse con menos recursos computacionales ya que el mayor procesamiento y almacenamiento se desarrolla en los Escritorios Virtuales y servidores de la Auditoría Interna.
- Reducción del riesgo de información comprometida del departamento de Auditoría Interna y del Banco por almacenamiento de equipos portátiles en caso de extravió o robo.
- La solución de Escritorios Virtuales de acceso remoto, se convierten en una estrategia de continuidad y contingencia para la Auditoría Interna, al poder configurar solo el sistema operativo en un nuevo equipo para conectarse remotamente y contar con acceso a

herramientas y aplicaciones de uso diarios de igual forma que desde la oficina, todo en menor tiempo que el que se necesita para configurar todas las herramientas en una estación de trabajo.

REFERENCIAS

REFERENCIAS

Buira, J. (2012). *El teletrabajo. Entre el mito y la realidad*. Editorial UOC.

Camazón, J. N. (2011). *Sistemas operativos monopuesto*. Editex.

Cedano Olvera, M. A., Cedano Rodríguez, A., Rubio González, J. A., & Vega Gutiérrez, A. C. (2014). *Fundamentos de Computación para Ingenieros*. Grupo Editorial Patria.

Destino Negocio (2020). Gestión. 5 ventajas de la tendencia BYOD (Bring Your Own Device). Recuperado de https://destinonegocio.com/cr/gestion-es_cr/

Heredero, C. d. (2004). *Informática y comunicaciones en la empresa*. ESIC Editorial.

Hernández Sampieri, Fernández Collado, & Batista Lucio, (2010). *Metodología de la Investigación - Quinta Edición*. México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A

Icart Isern, M., Pulpón Segura, A., Garrido Aguilar, E., & Delgado-Hito, P. (2012). *Cómo elaborar y presentar un proyecto de investigación, una tesina y una tesis*. Barcelona: Publicacions i Edicions de la Universitat de Barcelona.

Kimberly Herrera Salazar (30/10/2015). Huawei lanza Escritorio Virtual. Laprensalibre.cr.

Recuperado de <https://laprensalibre.cr>

Kölbi Negocios (21/05/2020). Empresas. Soluciones Nube. Data Center. Escritorios

Virtuales. Kölbi. Recuperado de <https://www.kolbi.cr/wps/portal/>

Moguel, E. A. (2005). *Metodología de la Investigación*. Tabasco: Univ. J.

Autónoma de Tabasco.

PACIO, G. (2014). *Data centers hoy. 1a ed.* Buenos Aires: Alfaomega Grupo Editor

Argentino.

Poder Judicial – República de Costa Rica (24/04/2017). Documentos de interés-Noticias.

Búsqueda: Implantación del Escritorio Virtual. Recuperado de

<https://comisionjurisdiccionscivil.poder-judicial.go.cr>

Racsa (4/6/2019). Escritorios Virtuales, parte de la transformación digital. WEBMASTERS

RACSA. Recuperado de <https://racsa.wordpress.com>

Salkind, N. J. (2012). *Métodos de investigación*. Pearson Educación.

Ubina, G. B. (2016). *Introducción a la seguridad informática*. Grupo Editorial Patria.

Anexo 1 - Entrevistas a usuarios expertos

Entrevista - Auditoría de Procesos de Áreas de Apoyo

Fecha:	12/08/2020	Hora:	08:00 am a 16:00 pm
Lugar:	Oficina de la Gerencia de Auditoría de TI		
Encuestador: Cristian Solano Chacón	Rol: Administrador de Infraestructura	Gerencia: Auditoría de TI	
Participantes: Hernán Fernández Ramírez	Rol: Gerente		

1. ¿Cuáles son las expectativas de poder acceder a los servicios, aplicaciones e información de la Auditoría y del Banco fuera de su oficina?

Respuesta: Tener acceso a todos los recursos de información, sistemas, datos, registros contables, repositorios de datos colaborativos de la Administración, utilizado a diario en las labores de Auditoría, accederla en línea.

2. ¿Qué sistemas o aplicaciones requiere tener acceso fuera de la oficina para sus labores diarias?

Respuesta:

- GPA, SGA, DGA, Proyectos ACL
- Suite Office
- AS400, Contabilidad, Portal de la Intranet del Banco, repositorio de normativa interna del Banco
- Sistemas de Capital Humano
- Gastos y Negocio
- Información de las Gerencias en la Auditoría

3. ¿Qué disponibilidad requiere de estos servicios si estuviera fuera de la oficina y del Banco?

Respuesta: Disponibilidad 5 días a la semana todo el día.

4. ¿Para el desarrollo de su trabajo fuera de la oficina y del Banco, acceso a la aplicación específicas sería suficiente o a todo un ambiente con sistema operativo Windows?

Respuesta: En ambiente Windows, porque es el que se utiliza y se está acostumbrado.

5. ¿A demás del sistema operativo Windows, que otras herramientas requeriría utilizar fuera de la oficina y del Banco?

Respuesta: Herramientas de comunicación portátiles para la comunicación con todos los compañeros de la Auditoría.

6. ¿Cómo ha sido su experiencia cuando la estación de trabajo se daña parcial o totalmente?

Respuesta: El cambio de equipo es rápido pero la configuración al punto antes del problema requiere de horas para su configuración.

7. ¿Con que frecuencia los colaboradores de Auditoría realizan Giras, Teletrabajo o Labores fuera de la oficina?

Respuesta: Se realiza teletrabajo de 2 a 3 veces por semana, las giras ocasionalmente.

8. ¿Cuáles son las expectativas de los usuarios de Auditoría acerca de un servicio de Escritorios Remotos?

Respuesta: Es tener la posibilidad de acceso desde afuera de la red del Banco a toda la información y sistemas a los cuales se tiene normalmente acceso dentro de la red institucional.

Entrevista - Auditoría de TI

Fecha:	11/08/2020	Hora:	08:00 am a 16:00 pm
Lugar:	Oficina de la Gerencia de Auditoría de TI		
Encuestador: Cristian Solano Chacón	Rol: Administrador de Infraestructura	Gerencia: Auditoría de TI	
Participantes: Jose Emilio Barrantes	Rol: Gerente		

1. ¿Cuáles son las expectativas de poder acceder a los servicios, aplicaciones e información de la Auditoría y del Banco fuera de su oficina?

Respuesta: Acceso a todo recurso informático de información, sistemas, registros contables, repositorios de datos colaborativos de la Administración y de la auditoría a diario.

2. ¿Qué sistemas o aplicaciones requiere tener acceso fuera de la oficina para sus labores diarias?

Respuesta:

- GPA, SGA, DGA, Proyectos ACL, servidores, base de datos, aplicaciones
- Office
- AS400 y sistemas contabilidad, SOMOS BCR, colaborativos
- Sistemas de Capital Humano, capacitación y de marcas
- Negocio, clientes, cuentas corrientes y de ahorros
- Información de todas las Gerencias en la Auditoría

3. ¿Qué disponibilidad requiere de estos servicios si estuviera fuera de la oficina y del Banco?

Respuesta: Disponibilidad de 24/7.

4. ¿Para el desarrollo de su trabajo fuera de la oficina y del Banco, el acceso a la aplicación específicas sería suficiente o a todo un ambiente con sistema operativo Windows?

Respuesta: Acceso a todos los sistemas operativo en producción, desarrollo y pruebas, así como de los aplicativos sin restricciones.

5. ¿A demás del sistema operativo Windows, que otras herramientas requeriría utilizar fuera de la oficina y del Banco?

Respuesta: Herramientas de comunicación, administración de servidores, de programación, bases de datos.

6. ¿Cómo ha sido su experiencia cuando la estación de trabajo se daña parcial o totalmente?

Respuesta: El proceso de restauración de un equipo, perfil y de los datos del usuario requiere de varias horas de configuración.

7. ¿Con que frecuencia los colaboradores de Auditoría realizan Giras, Teletrabajo o Labores fuera de la oficina?

Respuesta: Se realiza teletrabajo de 2 a 3 veces por semana y visitas a los centros de datos y oficinas del BCR.

8. ¿Cuáles son las expectativas de los usuarios de Auditoría acerca de un servicio de Escritorios Remotos?

Respuesta: La posibilidad de acceso desde cualquier punto geográfico a todos los recursos tecnológicos del Banco desde una red pública y privada.

Entrevista - Auditoría de Procesos de Negocio

Fecha:	14/08/2020	Hora:	08:00 am a 16:00 pm
Lugar:	Oficina de la Gerencia de Auditoría de TI		
Encuestador: Cristian Solano Chacón	Rol: Administrador de Infraestructura	Gerencia: Auditoría de TI	
Participantes: Rafael Chavarría	Rol: Gerente		

1. ¿Cuáles son las expectativas de poder acceder a los servicios, aplicaciones e información de la Auditoría y del Banco fuera de su oficina?

Respuesta: Tener acceso a todos los recursos de información, sistemas, datos, registros contables, repositorios de datos colaborativos de la Administración, utilizado a diario en las labores de Auditoría, accederla en línea.

2. ¿Qué sistemas o aplicaciones requiere tener acceso fuera de la oficina para sus labores diarias?

Respuesta:

- GPA, SGA, DGA, Proyectos ACL
- Producto de oficina como Outlook, Word, Excel, Power Point
- Sistemas contables, cuentas, Normativa, Sistemas de trabajo
- Sistemas de Capital Humano, marcas, vacaciones, boletas
- Información de otras Gerencias en la Auditoría

3. ¿Qué disponibilidad requiere de estos servicios si estuviera fuera de la oficina y del Banco?

Respuesta: Cinco días a la semana.

4. ¿Para el desarrollo de su trabajo fuera de la oficina y del Banco, acceso a la aplicación específicas sería suficiente o a todo un ambiente con sistema operativo Windows?

Respuesta: Es requerido un ambiente Windows igual al que se utiliza en las estaciones de trabajo físicas.

5. ¿A demás del sistema operativo Windows, que otras herramientas requeriría utilizar fuera de la oficina y del Banco?

Respuesta: Las mismas herramientas y aplicaciones utilizadas dentro de la oficina, tanto local como en la nube del BCR y otros proveedores

6. ¿Cómo ha sido su experiencia cuando la estación de trabajo se daña parcial o totalmente?

Respuesta: Retrasos en el desarrollo de estudios y hasta pérdida de información, con un proceso de recuperación del perfil del usuarios y datos.

7. ¿Con que frecuencia los colaboradores de Auditoría realizan Giras, Teletrabajo o Labores fuera de la oficina?

Respuesta: Se realiza teletrabajo de 3 a 4 veces por semana, las giras son programadas en un 25% de tiempo.

8. ¿Cuáles son las expectativas de los usuarios de Auditoría acerca de un servicio de Escritorios Remotos?

Respuesta: Acceder desde afuera de la red del Banco a toda la información y sistemas de información.

Entrevista Seguridad de TI

Fecha:	26/08/2020	
Hora:	08:00 am a 12:00 pm	
Lugar:	Oficina de la Gerencia de Auditoría de TI	
Encuestador: Cristian Solano Chacón	Rol: Administrador de Infraestructura	Gerencia: Auditoría de TI
Participantes: Luis Carlos Villalobos Hernández	Rol: Usuario Experto	Gerencia: Seguridad de TI

1. ¿Qué aspectos de seguridad lógica son requeridos para la interconexión de aplicaciones fuera de la red institucional?

Respuesta: Dentro de la normativa de aseguramiento para aplicaciones y sistemas del conglomerado BCR, se establece que todo sistema o dispositivo que se integre, consuma servicios internos o se conecte a la red del Banco debe hacerlo utilizando protocolos seguros, con conexiones cifradas y estas últimas deben utilizar algoritmos de cifrado vigentes y que no hayan sido vulnerados. Además, toda autenticación de usuarios se debe hacer por medio del servicio de ADFS del Banco.

2. ¿Qué características de seguridad son requeridos para los sistemas que operan dentro de la red institucional?

Respuesta: Los deben cumplir con la normativa de seguridad la cual establece lo siguiente:

a. Todo sistema interno debe realizar la validación de usuarios por medio del servicio de Directorio Activo o en su defecto cualquier otro servicio de autenticación aprobado por la Gerencia de Seguridad de TI.

b. Los sistemas tanto de desarrollo, pruebas, producción y las redes de los usuarios finales deben estar separadas en vlans separadas entre sí.

Además, los accesos a los puertos necesarios para cada sistema deben ser los estrictamente necesarios para el correcto funcionamiento de dicho sistema.

c. Los sistemas deben contar con roles definidos según sea necesario y dependiendo de la naturaleza del sistema; No se deben utilizar usuarios locales para la administración de la solución, es decir, los usuarios que conforman los respectivos roles de cada sistema deben ser los dispuestos en el directorio activo del Banco o en cualquier otro sistema autorizado por la Gerencia de Seguridad de TI.

d. Las contraseñas de seguridad ya sean de sistema, locales, de administración o cualquier otro tipo deben tener un plazo de vencimiento como mínimo de un mes, deben tener una longitud de al menos diez caracteres, los mismos deben contener: números, letras mayúsculas y minúsculas y caracteres especiales. En caso de tenerse que configurar una cuenta local la cual no tenga vencimiento, dicho usuario y contraseña se deben resguardar bajo llave.

3. ¿Cuál(es) son las tecnologías de autenticación que utiliza el Banco para el acceso de los usuarios a los sistemas?

Respuesta: Para la administración de usuarios, contraseñas, etc. El Banco utiliza como estándar el servicio de Active Directory de Microsoft, además cuenta con un servicio de Federación de Active Directory, el cual permite entregar el servicio de autenticación fuera de la red institucional de manera segura.

4. ¿Cuáles sistemas de seguridad tiene la institución para asegurar la comunicación desde y hacia afuera de la red del Banco?

Respuesta: En cuanto a la seguridad lógica tanto interna como externa, el Banco tiene instalado en los diferentes perímetros de red firewalls Palo Alto Networks next-generation, como solución para la prevención de intrusos cuenta con un robusto sistema de IPS basados en la solución McAfee Network Security Platform y cuenta en toda su infraestructura virtual, de servidores y equipos de usuario final con la suite de McAfee Total protection.

5. ¿Existen restricciones actualmente para el acceso, traslado y almacenamiento de la información consultada?

Respuesta: Por limitación de tecnología, no se puede controlar ¿quién?, ¿cómo? y ¿cuándo? accede información para trasladarla a un medio de almacenamiento externo, por lo que no se permite extraer información de sistemas desde un entorno virtual hacia uno físico.

Entrevista Telecomunicaciones

Fecha:	26/08/2020	
Hora:	12:00 pm a 16:00 pm	
Lugar:	Oficina de la Gerencia de Auditoría de TI	
Encuestador: Cristian Solano Chacón	Rol: Administrador de Infraestructura	Gerencia: Auditoría de TI
Participantes: Marco Vargas Mesén	Rol: Usuario Experto	Gerencia: Telecomunicaciones

1. ¿Cuáles son las características de switches utilizados en el centro de datos?

Respuesta: Se encuentran instalados en el centro de datos switches de las familias de Cisco 5500 y 5600 series con Flex Arquitectura, Gigabit Ethernet, 10 Gigabit Ethernet, 10-BASE-T, 40 Gigabit Ethernet uplinks, Fibra Canal Nativo y Fibra Canal sobre Ethernet (FCoE).

2. ¿Qué tipo de tecnologías de conexión se utilizan dentro de los centros de datos y hacia internet?

Respuesta: Las conexiones redundantes hacia internet se realizan por medio de enlaces de fibra óptica.

3. ¿Existe alguna tecnología de balanceo de cargas en la red institucional?

Respuesta: El balanceo de cargas de los sistemas en general se realiza por medio de una solución de balanceo de cargar basado en sistemas F5 Load Balancer de F5 Networks.

¿Cuentan los centros de datos con redundancia en cuanto a poder y enfriamiento?

Respuesta: Si, en caso de cortes en el fluido eléctrico, cada centro de datos cuenta con soporte de UPS redundante con el suficiente poder para mantener en línea todos los equipos hasta que entren en marcha las dos plantas eléctricas que se tienen instaladas en cada Data Center, mismas que tienen la capacidad de suministrar la electricidad suficiente para mantener los servicios críticos en línea por hasta 14 horas continuas.

4. ¿Qué herramientas se tienen implementados para asegurar conexiones externas hacia la red del Banco?

Respuesta: Para este fin, se utiliza un VPN implementado por medio de la plataforma firewalls Palo Alto Networks next-generation.

5. ¿Con que productos se cuenta para establecer la conexión segura y acceder a recursos virtuales en la red del BCR?

Respuesta: Se tienen aplicaciones como el GlobalProtect de la plataforma Palo Alto y Horizon View de la plataforma de Virtualización de escritorios. Estos productos deben de instalarse en cada estación de trabajo y configurarse con los parámetros específicos de cada solución.

6. ¿Qué mecanismos de inyección se utilizan para asegurar los datos de conexión y validación desde una red externa a una interna del BCR?

Respuesta: Dado que el BCR maneja su propia plataforma de Certificados Digitales, se crea un certificado para cada estación de trabajo, el cual es utilizado como un tercer factor de autenticación por medio del VPN. Los primeros factores de autenticación lo son el usuario y una clave del dominio BCR asignado a cada funcionario.

Entrevista Virtualización

Fecha:	25/08/2020	
Hora:	08:00 am a 16:00 pm	
Lugar:	Oficina de la Gerencia de Auditoría de TI	
Encuestador: Cristian Solano Chacón	Rol: Administrador de Infraestructura	Gerencia: Auditoría de TI
Participantes: Esteban Ruíz Ramírez	Rol: Usuario Experto	Gerencia: Virtualización

1. ¿Existe alguna solución de virtualización implementada en los Centros de Datos?

Respuesta: Sí, existe instalada una plataforma de virtualización con VMWare, en donde se tienen los ambientes de desarrollo, pruebas y producción de los sistemas no propietarios del Banco. Desde el año 2011 la institución inició de la mano de VMWare el proceso de convergencia de la infraestructura de los centros de datos para llevarlos hacia la virtualización y convertirlo en una nube privada que permita brindar dicha infraestructura como servicios.

2. ¿Qué tipo de solución de virtualización existe en los Centros de Datos?

Respuesta: Dentro de capacidades instaladas del licenciamiento VMWare adquirido se tienen, VMWare vSphere 6.5 y en proceso de actualización a 6.7 el cual consta de los sistemas operativos ESXi instalados en los servidores (Host), VMWare vCenter con Operation Manager el cual se encarga de la administración centralizada de dichos host y VMWare vRealize Automation la cual permite automatizar la creación de entornos completos de TI mediante la creación y la gestión de infraestructuras personalizadas.

3. ¿Con que tipo de licenciamiento se cuenta para dicha solución de virtualización?

Respuesta: Se cuenta con un licenciamiento llamado VMWare Horizon Enterprise Edition el cual contempla el siguiente licenciamiento:

VMWARE HORIZON ENTERPRISE EDITION
VMware vSphere Desktop, VMware vCenter Server, VMware Horizon View Enterprise, VMware Mirage, VMware Identity Manager Standard, VMware ThinApp Virtualization Packager, VMware ThinApp Client, VMware App Volumes Enterprise, VMware Workstation Pro, VMware vSAN for Desktop Advanced, vRealize Operations for Horizon (including vRealize Operations for Published Applications), vRealize Orchestrator Plugin for Horizon, VMware User Environment Manager, VMware Fusion Pro, Help Desk Tool, Virtualization Pack for Skype for Business and VMware Horizon for Linux

(VMware, 2020).

4. ¿Se cuenta con contrato(s) de mantenimiento y soporte técnico?

Respuesta: Sí, se cuenta con contratos de mantenimiento por cuatro años, tanto de los servidores como de soporte sobre todos los productos licenciados de VMWare.

5. ¿Cuál es la configuración de hardware y sistema operativo que tienen los servidores físicos del Centro de Datos Principal y Alterno?

Respuesta: Para soportar los más de 250 servidores virtuales que conforman los ambientes de pruebas, desarrollo y producción de la institución se tienen 72 servidores físicos instalados en ambos centros de datos, los cuales tienen instalado el sistema operativo VMWare ESXi 6.5 y que junto con la consola de administración de la infraestructura virtual WMware vCenter 6.0 permiten desde un punto centralizado la administración de dichos servidores virtuales;

La configuración de hardware de los servidores físicos es la siguiente:

Configuración de Servidores Físicos Instalados								
Cantidad Servidores	Centro Datos	Modelo Servidor	Procesador x2	Núcleos	Memoria RAM	Disco Duro	Max-vCPU-por-VM	Max-VMs-Por-Host
32	Principal	HPE ProLiant DL380 Gen9 Server	Intel® Xeon® Processor E5-2670 v3 (30M Cache, 2.30 GHz)	16	512 GB (16x 32GB RDIMM @2400MHz)	12TB-SSD	4 vCPU	48
32	Secundario	HPE ProLiant DL380 Gen9 Server	Intel® Xeon® Processor E5-2670 v3 (30M Cache, 2.30 GHz)	16	512 GB (16x 32GB RDIMM @2400MHz)	12TB-SSD	4 vCPU	48
Total capacidad VMs*:	1536							
<i>*Basado en una configuración de 4GB-RAM y 4 vCpu por VM</i>								

Para la virtualización de escritorios se tienen las siguientes tecnologías:

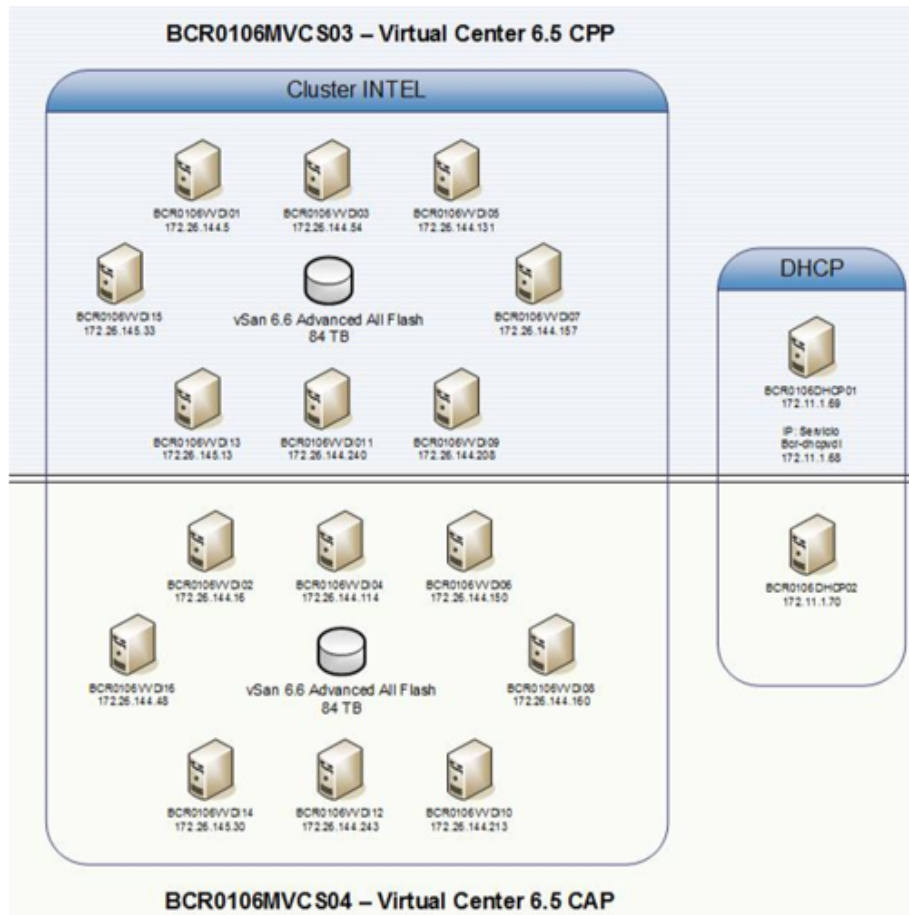
- VMware Horizon View 7.7
- VMware vSphere 6.5 U2
- VMware vSAN 6.6
- VMware NSX 6.4.3

6. ¿Con qué tecnologías de almacenamiento se cuenta tanto en el Centro de Datos Principal como en el Alterno?

Respuesta: Se cuenta con dos Hitachi Virtual Storage Platform G1000 (VSP G1000) con una capacidad de almacenamiento de 250TB cada una, esta SAN cuenta con interconexión por medio de fibra canal y permite tener redundancia, alta disponibilidad y escalabilidad a futuro.

7. ¿Los Centros de Datos cuentan con redundancia y alta disponibilidad en cuanto a red, energía y control de temperatura?

Respuesta: Si, el centro de datos cuenta con redundancia, ya que cada dispositivo de comunicación cuenta con su homólogo en cada centro de datos, además ambos centros de datos se cuenta interconectados a través de dos conexiones en fibra óptica principales y dos secundarias suministradas por dos proveedores diferentes. En cuanto a enfriamiento se cuenta con redundancia en dichos equipos. En relación con la alimentación de energía se cuenta con redundancia en UPS y plantas generadoras en ambos centros de datos.



Se adjunta la tabla con la matriz de soporte para los productos VMware parte de la solución de los Escritorios Virtuales.

Producto	Disponibilidad General	Fin Soporte General	Fin Orientacion Tecnica
Vmware Horizon View 7.7	22/03/2016	22/03/2021	22/03/2023
Vmware vSphere 6.5 U2	15/11/2016	15/11/2021	15/11/2023
Vmware vSAN 6.6	15/11/2016	15/11/2021	15/11/2023
Vmware NSX 6.4	16/01/2018	16/01/2021	16/01/2022
vCenter Server 6.5 and 6.7	15/11/2016	15/11/2021	15/11/2023

Sesión de trabajo con Administradores Infraestructura Auditoría de TI

Fecha:	10/08/2020	
Hora:	08:00 am a 16:00 pm	
Lugar:	Oficina de la Gerencia de Auditoría de TI	
Encuestador: Cristian Solano Chacón	Rol: Administrador de Infraestructura	Gerencia: Auditoría de TI
Participantes:	Rol:	Gerencia:
Jose Pablo Valverde Jiménez	Administrador Principal de Infraestructura	Auditoría de TI
Kenneth Dinarte Jiménez	Administrador Secundario de Infraestructura	Auditoría de TI

1. Identificar cuántos funcionarios laboran en la Gerencia de la Auditoría Interna.

Respuesta: En dicha Gerencia laboran un total de 65 funcionarios.

2. ¿Cómo está estructurada organizacionalmente la Auditoría Interna del BCR?

Respuesta: La Auditoría está dividida en varias áreas a saber:

- Auditoría General
- Auditoría de Procesos de TI
- Auditoría Banca Corporativa
- Auditoría Banca de Personas
- Auditoría Operaciones
- Auditoría Áreas de Apoyo
- Auditoría Financiera

Otras áreas:

- Auditoría de Riesgos
- Investigación y Desarrollo
- Asesoría Legal

3. Identificar que otras áreas fuera de la Auditoría Interna del BCR dependen de recursos (Sistemas-Datos-Servidores) de la Gerencia de la Auditoría Interna.

Respuesta: Otras gerencias que dependen son las Auditorías Internas de cada una de las Subsidiarias del Conglomerado BCR, estas son:

- BCR SAFI (Administradora de Fondos de Inversión S.A), 5 Auditores
- BCR Valores (Puesto de Bolsa S.A), 4 Auditores
- BCR Seguros (Corredora de Seguros S.A), 3 Auditores
- BCR OPC (Operadora de Planes de Pensiones Complementarias S.A), 5 Auditores

4. ¿Qué tipo de software y sistemas se utilizan en la Gerencia de Auditoría para el desempeño de las labores diarias y otras gerencias relacionadas?

Respuesta: Se utilizan:

- Suite de Microsoft Office
- Aplicaciones web desarrolladas internamente como SGA, DGA, SISMO, Proyectos ACL
- Principalmente aplicaciones críticas del negocio Cliente AS400, Cliente Infoconnect, Portal de la Intranet del Banco, repositorio de normativa interna del Banco y todos los demás sistemas del Banco según se requieran en cada estudio de Auditoría. Cabe destacar, que estas aplicaciones no se puede acceder desde fuera de la red del Banco
- GPA, este último esta implementada en plataforma Lotus Notes/Domino, se lleva toda la documentación de la Auditoría
- Información de cada Gerencia almacenada en carpetas dentro de servidores de Archivos
- Dominio específico para la Auditoría donde se matriculan cada servidor y estación de trabajo de la Auditoría
- Bases de datos que consolidan información del Banco y de la Auditoría, utilizados como fuentes para los estudios de auditoría
- Herramientas de soporte como modelador de flujos, compresores de archivos
- Infraestructura de desarrollo y pruebas para laboratorios a utilizar en los estudios y sus pruebas

5. ¿Cuál es la configuración estándar en cuanto a memoria RAM, CPU y espacio de disco duro de los equipos utilizados en el área de Auditoría?

Respuesta: Todos los funcionarios de auditoría cuentan con equipos portátiles configurados con 8GB de memoria RAM, 250GB de disco duro y cuentan con un procesador Intel Core i7, recursos necesarios para almacenar y procesar información local y remotamente.

6. ¿Cuáles son los equipos servidores que se administran en la Auditoría?

Respuesta: Son los servidores físicos Host con sistema operativo ESX y servidores virtuales con sistema operativo Windows y Ubuntu. El detalle del inventario de estos servidores y su relación se adjuntan en el anexo 1 de esta sesión, la cual debe manejarse con confidencialidad.

7. ¿Cuáles son las aplicaciones o servicios críticos de la Auditoría?

Respuesta: Son los enumerados a continuación:

- GPA (Gestión de Proceso de Auditoría), implementado en bases de datos Notes. La seguridad y administración de los usuarios de Lotus Domino se realizan en la plataforma Domino Server en dos nodos.
- ACL, aplicación para la programación de tareas o ejecución de script para la extracción y formateo de datos utilizando como fuentes las bases de datos generadas en la Auditoría y en el Banco de sus diferentes sistemas.
- SISMO, consulta, consolida y genera indicadores para cada oficina del Banco para llevar una medición contable de sus gestiones.

- SGA (Sistema de Gestión de Auditoría), desarrollo interno para el cálculo y documentación del riesgo de los estudios de Auditoría, así como de utilización como herramienta para calificar a cada funcionario en los estudios que realiza y participa.
 - GEA (Documentación y Gestión de Arqueos), desarrollo interno utilizado para la gestión y sugerencias de arqueos a las diferentes oficinas del Banco en todo el país.
 - Subdominio de la Auditoría, soportada con herramientas de Microsoft (Active Directory) para la gestión de sus equipos servidores y estaciones de trabajo por medio de políticas de dominio, asegurando independencia de la Administración dado la información que se maneja.
 - Servicio de Carpetas compartidas, utilizada por las Auditorías para resguardo de información sensible, de estudios y de colaboración entre los auditores.
 - Servicio de respaldos, utilizada para consolidar los respaldos de las diferentes bases de datos, sistemas, información de carpetas, archivos de configuración de los servidores como primer punto de respaldo. Desde acá se gestiona otro respaldo fuera de la Auditoría.
 - Servicios de bases de datos y sistemas operativos en ambientes de pruebas para preparación de consulta de datos para los estudios y laboratorios de aprendizaje.
8. ¿Cuáles son las aplicaciones o servicios que accede y utiliza la Auditoría del Banco?

Respuesta: Repositorio de normativa del Banco, Service Now, Dynatrace, Foglight, Qradar, vCenter BCR, SICC, Contabilidad, Capital humano, Bases de datos de cualquier sistema del Banco.

9. ¿Cuáles son las aplicaciones o herramientas de seguridad que se aplican a las estaciones de trabajo dentro de la red del Banco y que necesitara fuera de esta red?

Respuesta: Requiere de la revisión constante y aplicación de parches del sistema operativo, actualización de antivirus.

10. ¿Con que frecuencia los colaboradores de Auditoría realizan Giras, Teletrabajo o Labores fuera de la oficina?

Respuesta: Los colaboradores de la Auditoría realizan teletrabajo aproximadamente 3 veces por semana, las giras en dos de las Gerencias de Auditoría desde los 3 a 15 días, que requiere de verificaciones en sitio y se realizan trabajos de análisis de información. Esto para un 70% de los funcionarios de la Auditoría.

11. ¿Cuáles son las expectativas de los usuarios de Auditoría acerca de un servicio de Escritorios Remotos?

Respuesta: Las expectativas de los usuarios de la Auditoría sobre los escritorios remotos virtuales, es la posibilidad de poder tener acceso desde afuera de la red del Banco a toda la información y sistemas a los cuales se tiene normalmente acceso dentro de la red institucional; Y todo esto de una manera segura y confiable.

Anexo 2 - Matriz Requerimientos – Propuesta – Implementado

Fuente: Entrevistas a usuarios expertos
Conocimiento de Administradores de Infraestructura

Requerimientos / Usuarios	Gerencias de Auditorías					Áreas de Apoyo					Subsidiarias del Conglomerado			
	Procesos de TI	Continua	Financiera	Riesgo	Banca Corporativa	Banca Corporativa	Operaciones	Operaciones	Áreas de Apoyo	General	SAFI	OPC	Valores	Corredora Seguros
Software														
GPA	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Servidor Carpetas Compartidas	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Suite Office	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SGA	X	X	X	X	X	X	X	X	X	X	X	X	X	X
GEA	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SISMO	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Intranet de la Auditoría	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Intranet del BCR	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Proyectos AQL	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Servidores de Bases de Datos	X	X	X	X	X	X	X	X	X	X	X	X	X	X
vCenter de Auditoría	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Servidor de Respaldo	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Plataforma de Parchado	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Plataforma Lotus Domino	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Subdominio de la Auditoría	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Administrador de políticas Subdominio Auditoría	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Limitaciones y afectación														
Trasiego de información en archivos desde la estación de trabajo al Escritorio Virtual y viceversa														
Imposibilidad de copiar y pegar	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Sistemas BCR														
As/400	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Contabilidad (Infoconnect)	X	X	X	X	X	X	X	X	X	X	X	X	X	X
OTROS	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Requerimientos de TI														
Active Directory	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Cifrado	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Permisos	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Protocolos seguros y vigentes	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Conexión segura	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Permisos de firewalls	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Cumplimiento de normativa interna del Banco	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Recurso de conexión														
VPN - Firewall Palo Alto	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Certificado Digital para el Equipo - Plataforma PKI	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Escritorios Virtuales - VMware Horizon Enterprise Editi	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Documentación														
Manuales de instalación	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Protocolos	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Guías	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Archivo: Matriz Requerimientos - Propuesta - Implementado / Hoja: Requerimientos

Requerimientos		Solución a Implementar
Software		
GPA	Configuración inicial con el usuario en el ambiente de Escritorio Remoto, respaldos de archivos de configuración e identidad almacenados en carpeta robolado con la cédula del usuario, que reside en un servidor de archivos. Crear un archivo .BAT con las instrucciones para buscar con la cédula del usuario logueado en el servidor de archivos la carpeta correspondiente y copiar desde allí a una ruta específica en el Escritorio Remoto. Este archivo .BAT se debe de cargar inmediatamente después del sistema operativo y ejecutar automáticamente.	
Servidor Carpetas Compartidas	Solicitud de permisos de Firewall con los puertos de acceso a carpetas compartidas.	
Suite Office	Instalación de Libre Office como producto sustituto y compatible con los archivos generados por Microsoft Office, dado el gasto de una licencia más por usuario de la Auditoría uso o no el Escritorio Virtual. Instalación de visores de Word, Excel, Power Point y de Outlook para ver estos archivos desde el sistema operativo y dentro de la plataforma Lotus con permisos de solo lectura.	
SGA	Solicitud de permisos de Firewall con los puertos de acceso al sitio Web, y permisos de validación contra el Active Directory del BCR	
GEA	Solicitud de permisos de Firewall con los puertos de acceso al sitio Web, y permisos de validación contra el Active Directory del BCR	
SIAMO	Solicitud de permisos de Firewall con los puertos de acceso al sitio Web, y permisos de validación contra el Active Directory del BCR	
Intranet de la Auditoría	Actualmente solo corre en una versión de Internet Explorer versión 8.0	
Intranet del BCR	Instalación de Chrome con los componentes necesarios para soportar las características del sitio, dado que una vez compilado el nodo de Escritorio Virtual no hay permisos de instalar por parte del usuario	
Proyectos ACL	Dado que el uso de ACL requiere de una validación por HASH desde la página del proveedor, no se puede utilizar desde el Escritorio Virtual este aplicativo al no estar autorizado la navegación en Internet. Como solución temporal, se habilitan en un servidor de archivos las carpetas que contienen proyectos de ACL para que cada usuario los ejecute remotamente desde el servidor origen y obtenga los reportes	
Servidores de Bases de Datos	Dado que no hay autorización por Seguridad de TI para utilizar una consola Remota a servidores de SQL, se instala una suite de SQL Management Studio y solicitan los permisos de Firewall para administrar solo el motor de bases de datos desde el Escritorio Virtual.	
vCenter de Auditoría	Solicitud de permisos de Firewall con los puertos de acceso a AppIance de VMware para vCenter, con acceso a la validación por Active Directory.	
Servidor de Respaldos	Instalación de herramientas para conexión SSH (Putty, WinSCP) Para acceder remotamente a equipo con sistema operativo Ubuntu	
Plataforma de Parchado	Solicitud de permisos de Firewall con los puertos de acceso a la herramienta por la Web	
Plataforma Lotus Domino	Configuración inicial con el usuario en el ambiente de Escritorio Remoto, respaldos de archivos de configuración e identidad almacenados en carpeta robolado con la cédula del usuario, que reside en un servidor de archivos. Crear un archivo .BAT con las instrucciones para buscar con la cédula del usuario logueado en el servidor de archivos la carpeta correspondiente y copiar desde allí a una ruta específica en el Escritorio Remoto. Este archivo .BAT se debe de cargar inmediatamente después del sistema operativo y ejecutar automáticamente.	
Subdominio de la Auditoría	Solicitud de permisos de Firewall con los puertos de acceso a servidores de Dominio de la Auditoría para conectarse al Dominio BCR y de la Auditoría	
Administrador de políticas Subdominio Auditoría	Solicitud de permisos de Firewall con los puertos de acceso a servidores de Dominio de la Auditoría para conectarse al Dominio BCR y de la Auditoría	
Limitaciones y afectación		
Trasiego de información en archivos desde la estación de trabajo al Escritorio Virtual y viceversa	Se investigan dentro de las herramientas del Banco, alguna que permita trasladar información y que este autorizada por Seguridad de TI, que funciones tanto en los Escritorios Virtuales como en las estaciones de trabajo en red privada y pública	
Imposibilidad de copiar y pegar	Esta característica no se habilita, sin embargo se conoce de un proyecto para implementar un software entre la red privada del BCR y pública que verifique los datos que se trasladan para evitar contaminación por malware	
Sistemas BCR		
AS/400	Instalación de aplicación, solicitud de acceso con estación virtual creada en sistema central y mapeo de IP reservada	
Contabilidad (InBocomed)	Instalación de aplicación, solicitud de acceso con estación virtual creada en sistema central y mapeo de IP reservada	
OTROS	En el momento de necesitarse, las posibles soluciones son las de permisos de Firewall, puertos y permisos para usarlos.	
Requerimientos de TI		
Active Directory	Utilización de credenciales de dominio BCR para ingreso	
Cifrado	Implementación de VPN, Certificado Digital para la estación de trabajo	
Permisos	Solicitudes específicas de los accesos a las aplicaciones necesarias por usuario, desde la VDI hacia los servidores requeridos	
Protocolos seguros y vigentes	Utilización de versiones de navegadores Web actualizadas	
Conexión segura	Utilización de herramientas avaladas por Seguridad de TI y con licenciamiento para el BCR	
Permisos de firewalls	Solicitudes con los formularios establecidos para dicho fin con las autorizaciones de los superiores respectivos	
Cumplimiento de normativa interna del Banco	Revisión y análisis de toda la normativa de Seguridad para el apoyo riguroso a las normas de cada aplicación, herramienta, acceso y confiabilidad de los datos de la normativa interna, esto implica que las soluciones a los inconvenientes de utilización de recursos cuenten con el aval del área de Seguridad de TI	
Recurso de conexión		
VPN - Firewall Palo Alto	Instalación de clientes en equipos de trabajo de cada funcionario de la Auditoría con la configuración requerida para conexión desde una red externa a la del BCR	
Certificado Digital para el Equipo - Plataforma PKI	Solicitud personalizada de certificados por equipo y funcionario de la Auditoría por medio de tickets	
Escritorios Virtuales - VMware Horizon Enterprise Edition	Instalación de clientes en equipos de trabajo de cada funcionario de la Auditoría con la configuración requerida para conexión desde una red externa a la del BCR	

Requerimientos		Resultado	Productos - Escritorios Virtuales	
Software			Auditoría TI	Administración Auditoría
GPA		Funcional	✓	✓
Servidor Carpetas Compartidas		Funcional	✓	✓
Suite Office		Funcional	✓	✓
SGA		Funcional	✓	N/A
GEA		Funcional	✓	N/A
SISMO		Funcional	✓	N/A
Intranet de la Auditoría		Funcional	✓	N/A
Intranet del BCR		Funcional	✓	N/A
Proyectos ACL		Funcional	✓	N/A
Servidores de Bases de Datos		Funcional	✓	✓
vCenter de Auditoría		Funcional	✓	✓
Servidor de Respaldos		Funcional	✓	✓
Plataforma de Parchado		Funcional	✓	✓
Plataforma Lotus Domino		Funcional	✓	✓
Subdominio de la Auditoría		Funcional	✓	✓
Administrador de políticas Subdominio Auditoría		Funcional	✓	✓
Limitaciones y afectación				
Trasiego de información en archivos desde la estación de trabajo al Escritorio Virtual y viceversa		Funcional	✓	✓
Imposibilidad de copiar y pegar		Funcional	✓	✓
Sistemas BCR				
As/400		Funcional	✓	N/A
Contabilidad (Infocconnect)		Funcional	✓	N/A
OTROS		Funcional	✓	N/A
Requerimientos de TI				
Active Directory		Funcional	✓	✓
Cifrado		Funcional	✓	✓
Permisos		Funcional	✓	✓
Protocolos seguros y vigentes		Funcional	✓	✓
Conexión segura		Funcional	✓	✓
Permisos de firewalls		Funcional	✓	✓
Cumplimiento de normativa interna del Banco		Aceptado	✓	✓
Recurso de conexión				
VPN - Firewall Palo Alto		Funcional	✓	✓
Certificado Digital para el Equipo - Plataforma PKI		Funcional	✓	✓
Escritorios Virtuales - VMware Horizon Enterprise Edition		Funcional	✓	✓
Documentación				
Manuales de instalación		Documentado	✓	✓
Protocolos		Documentado	✓	✓
Guías		Documentado	✓	✓