Xorex de Colombia

DISEÑO Y ARQUITECTURA DETALLADA DE LA INFRAESTRUCTURA DE RED

INFORMACIÓN DE LA REUNIÓN					
Cliente	CONTRALORIA DISTRITAL DE MEDELLIN				
Proyecto	**SELECCIÓN ABREVIADA MENOR CUANTIA NO. SAMC0032023**				
Gerente de proyecto	Carlos Felipe Valverde		Versión del documento		1
Fecha	19/05/2023	Hora de Inicio			

PARTICIPANTES		
Nombre Asistente	**Organización**	**Rol**
Luis Felipe Rosso Ricaute	Contraloría Distrital de Medellín	Director Administrativo
Yudy Liset Jimenez	Contraloría Distrital de Medellín	Técnico Operativo
Martin Alejandro Colorado	Contraloría Distrital de Medellín	Profesional Universitario I
Oscar Javier Giraldo	Contraloría Distrital de Medellín	Técnico Operativo
Carlos Felipe Valverde	Xorex DC	Gerente Proyecto
Luis Eduardo Bolivar	Xorex DC	Líder Tecnico

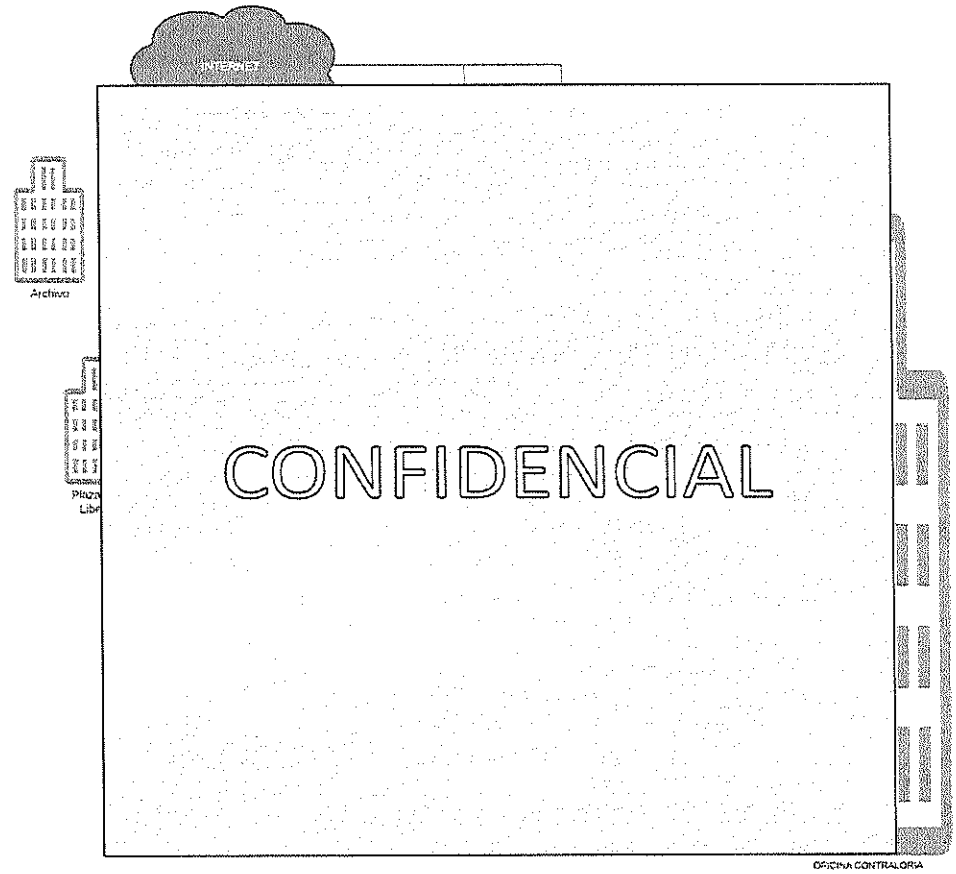
PROPOSITO DEL DOCUMENTO	
Tema	
Entregable No.1	Diseño y arquitectura detallada de la infraestructura de red, con los planos técnicos correspondientes y un informe donde se evidencien la optimización y mejoras tras el diseño propuesto, tanto en temas funcionales como en seguridad digital.
Entregables Acordados	**Entregable** Este documento tiene como objetivo cumplir con el entregable de la fase no. 1 el cual es requerido para el primer pago equivalente al 50% del proyecto en el ámbito financiero y que, según el alcance manifestado en el acta de inicio, contiene: **FASE I** Durante la Fase I, se entregará un (1) documento tipo informe en formato pdf que contiene: • Registro Fotográfico de los centros de cableado actuales • Análisis de la topología física actual de los switches, con las respectivas observaciones a nivel de disponibilidad y redundancia de la red. • Análisis de la configuración lógica enfocándose en funcionalidades de los equipos actuales y buenas prácticas de ciberseguridad. • Documento de diseño que contiene la distribución y conexión física de los equipos a suministrar • Propuesta de diseño lógico, justificando los posibles cambios que se propongan en esta fase.

Cr 7 #156-65 Edificio North Point Torre II Piso 22 Bogotá, Colombia
PBX: (+57 1) 7420625 / FAX: (+57 1) 7420625
www.xdc.com.co

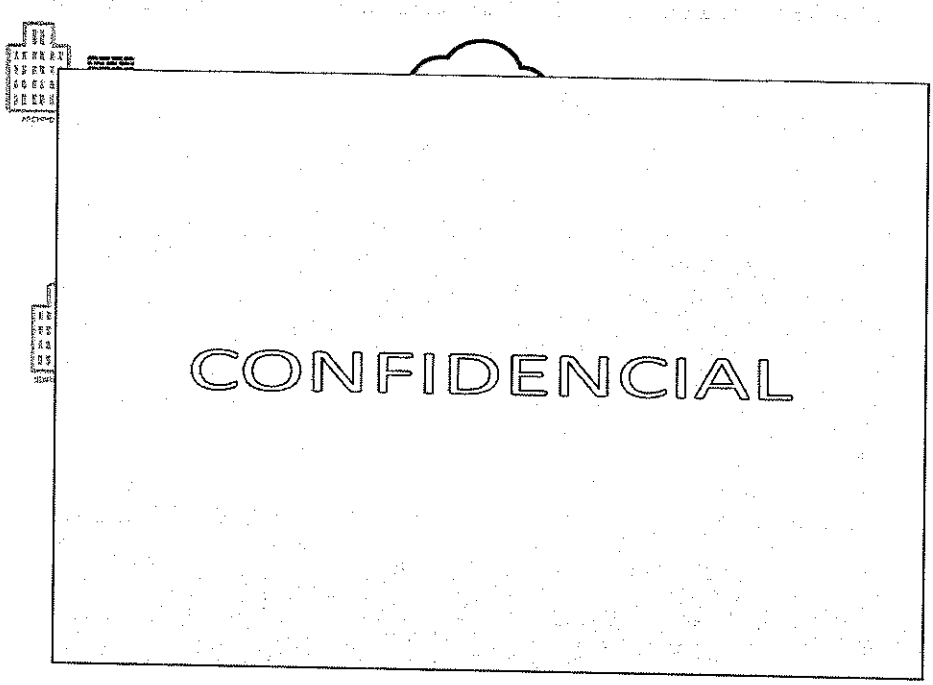
<table>
<tr><td>Registro fotográfico de los centros de cableado</td><td>
<table>
<tr><th>Centro de Cableado</th><th>Registro Fotográfico</th></tr>
<tr><td>Edificio Miguel de Aguinaga P5</td><td>"Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"</td></tr>
<tr><td>Edificio Miguel de Aguinaga P6</td><td>"Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"</td></tr>
<tr><td>Edificio Miguel de Aguinaga P7</td><td>"Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"</td></tr>
<tr><td>Edificio Miguel de Aguinaga P8</td><td>"Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"</td></tr>
<tr><td>Edificio Plaza de la Libertad</td><td>"Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"</td></tr>
</table>
</td></tr>
<tr><td>Análisis de la topología física actual de los switches</td><td>Después de un levantamiento de información de las topologías XDC realizó el siguiente grafico para ilustrar la topología física de la entidad y facilitar la comprensión del análisis que se realiza sobre esta.</td></tr>
</table>

Cr 7 # 156-66 Edificio North Point Torre II Piso 22 Bogotá Colombia
PBX (+57) 1 7420625 / Fax (+57) 1 7420625
www.xdc.com.co

DISEÑO Y ARQUITECTURA DETALLADA DE LA INFRAESTRUCTURA DE RED

Topología física de la red LAN de la CDM	 "Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"
Análisis de la topología física	Después de validar las conexiones físicas de la red LAN de la Contraloría Distrital de Medellín, se concluye lo siguiente: • La red cumple con los criterios físicos de alta disponibilidad el elemento más critico de la misma que es el SW Core es redundante. • Se tienen enlaces redundantes en fibra óptica a 10Gbps desde los diferentes centros de cableado del edifico Miguel Aguinaga, con lo cual se garantiza la disponibilidad ante la falla en un enlace o switch.

Cr 7 # 156-66 Edificio North Point Torre II Piso 22 Bogotá Colombia
PBX (+57) 7420625 / FAX (+57) 7420625
www.xdc.com.co

	• El switch del edificio Plaza de la libertad no presenta redundancia en los enlaces, aunque este es un punto complejo de garantizar en enlaces LAN to LAN • En una topología tipo estrella como la actual, existe un riesgo mínimo asociado a algún evento que comprometa de manera completa la canalización de la fibra óptica, este podría ser minimizado creando un segundo camino de tipo anillo.
Análisis de topología lógica	A continuación, se presenta un diagrama para ilustrar la configuración lógica y los análisis realizados sobre la misma.
Topología lógica	 "Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"
	Actualmente la topología lógica a nivel de red LAN incluye varias configuraciones, dentro de las cuales se presentan las mas reelevantes:

Cr 7 # 156-65 Edificio North Point Torre II Pso 22 Bogotá, Colombia
PBX: (+57) 1 7420625 / FAX: (+57) 1 7420625
www.xdecolombia

Análisis de la topología lógica	• El SW Core realiza todo el enrutamiento interno, y las conexiones hacia Internet son enviadas hacia el Firewall ~~XXXX~~ • Las redes inalambricas son proporcionadas atraves de APS Sonicpoints, gestionados por una solución de firewall ~~X.X.X.X~~ en alta disponibilidad. • A nivel de servidores el SW Core tiene configuradas dos redes para la SAN (~~XXXX~~). • Para la red de servidores se tiene el siguiente segmento: ~~XXXX~~ • Para la red de servidores se tienen las siguientes VLANs no enrutables desde el SW Core: ~~XXXX~~, estas redes se enrutan directamente por el ~~XXXX~~. • A nivel de datos se tiene actualmente uan segmentación por pisos, teniendo dos segmentos actualmente por piso. • Se utiliza la VLAN ~~XXXX~~ cómo VLAN de gestión de los equipos
Conclusiones de la configuración lógica actual	En general la red LAN cuenta con buenas practicas de configuración dentro de estas se encuentran: • No utilizar la VLAN 1, como VLAN nativa, en su lugar utilizar la VLAN ~~XXXX~~ • Tener una VLAN de gestión (~~XXXX~~) independiente para los switches. • Utilizar Port-Channles para la agregación de enlaces a servicios críticos, aumentando el ancho de banda y la disponibilidad de estos. **Puntos a mejorar** • Se debe deshabilitar la gestión por el protocolo telnet en los switches de acceso, dado que este protocolo se considera no seguro por no cifrar la comunicación. • La segmentación actual en la capa de acceso se realiza por piso, lo cual facilita la gestión de la red y reduce la superficie de daño en los casos donde se presente un evento que afecte la red. Actualmente tener uno o dos segmentos por piso aplica como buen practica dado que se tienen redes físicas independientes para los diferentes servicios como: CCTV, Multimedia, Voz IP, Equipos de cómputo, etc. En caso de unificar a futuro, diferentes servicios en un mismo switch, se recomienda la creación de VLANS diferentes por servicio.

Cl 7 # 156-68 Edificio North Point Torre II Piso 22 Bogotá Colombia
PBX (+57) 7420625 / Fax (+57) 7420625
www.xdc.com.co

<table>
<tr><td></td><td>

- No se cuenta con ACLs en el SW Core, lo que permite que todos los segmentos enrutados por el SW Core se vean entre sí.

</td></tr>
<tr><td>Propuesta Arquitectura física</td><td>

Dado que la topología física actual cumple con los estándares de alta disponibilidad, se recomienda mantener el mismo esquema de conectividad con un enlace redundante entre los diferentes pisos.

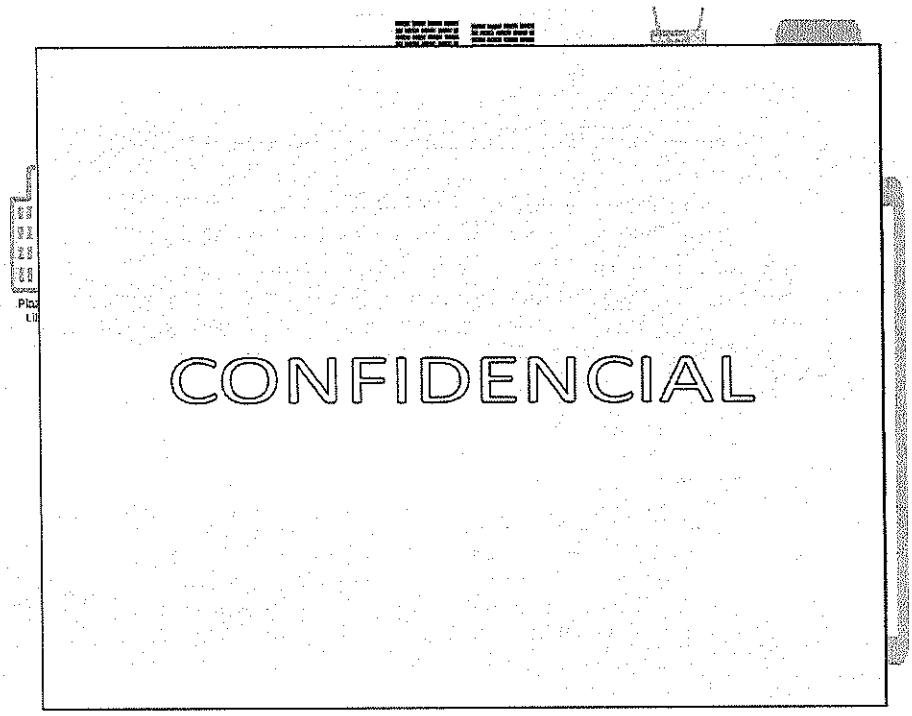
Evaluando la criticidad de los diferentes pisos, se encuentra que los pisos más críticos a nivel de operación son el piso 7 y el piso 8, por tanto, se recomienda que estos equipos que son de última tecnología y tiene soporte de fabrica sean destinados a estos pisos y uno de los equipos al edificio plaza de la Libertad quedando la distribución de equipos de la siguiente manera:

<table>
<tr><th>Ubicación</th><th>Modelo</th><th>Cantidad</th></tr>
<tr><td>Ed. Miguel Aguinaga p7</td><td>Juniper EX2300-48MP</td><td>3</td></tr>
<tr><td>Ed. Miguel Aguinaga p8</td><td>Juniper EX2300-48MP</td><td>2</td></tr>
<tr><td>Ed. Plaza de la Libertad</td><td>Juniper EX2300-48MP</td><td>1</td></tr>
<tr><td>Backup</td><td>Juniper EX2300-48MP</td><td>1</td></tr>
</table>

Dado que sobra un equipo la recomendación seria mantener este equipo temporalmente este equipo como una unidad de respaldo, por que los pisos 5 y 6 se encuentran en stack y no valdría la pena desarmar el stack.

</td></tr>
</table>

Cr 7 # 156-46 Edificio North Point Torre 1 Piso 22 Bogotá, Colombia
PBX (+57) 7420525 / FAX (+57) 7420525
www.xdc.com.co

	 "Por asuntos de confidencialidad, esta información es suministrada a la Contraloría Distrital de Medellín en el archivo: "INFORME RECOMENDACIONES SAMC0032023v3"
Propuesta Arquitectura Lógica	Dentro de los puntos a mejorar a nivel lógico, que se cubren dentro del alcance de este proyecto se proponen los siguientes cambios, apuntando a mejorar y cerrar posibles brechas en la seguridad de la información: • Deshaibilitar el uso de protocolos inseguros como Telnet, en los stacks de acceso • Eliminar VLANs que no cumplan ninguna función en la red. • Se propone crear una VLAN independiente para el departamento de desarrollo tecnológico, dado que por sus funciones deberían tener un control mas completo sobre la infraestructura que los otros departamentos, se podria utilizar el segmento ~~XXXX~~ • Una vez creados los dos segmentos anteriores se sugiere crear ACLS para que los usuarios solo tengan acceso a los servidores e Internet, y se bloquee el acceso a las VLAN de gestión.

Cra 7 #156-68 Edificio North Point Torre II Piso 22 Bogotá, Colombia
PBX (+57) 1 7420626 / FAX (+57) 1 7420626
www.xdc.com.co

Opciones de mejora no cubiertas en el alcance de este proyecto.	A continuación, se presentan varias opciones de mejora, que no se encuentran dentro del alcance de este proyecto, pero que representarían cambios positivos en la Contraloria Distrital de Medellín, en puntos clave como aumentar la visibilidad de la red y facilitar la gestión, para garantizar la seguridad de esta, tener un mejor aprovechamiento de los recursos adquiridos, disminuir los costos operativos, a continuación, se enumeran los que se consideran las principales mejoras a aplicar: **Punto 1 Unificar la red LAN** Adquirir un SW Core en alta disponibilidad y cinco (5) switches de acceso en la marca Juniper, permitirá tener una red LAN monomarca en toda la entidad, lo cual adicional a tener una red completa con soporte de fabrica facilita la gestión del equipo de TI dado al tener que administrar una sola marca de equipos. Adicionalmente l fabricante Dell tiene reportado en su página que solo dará soporte para los switches línea N4000 (actualmente le core de la entidad) hasta el 29 de abril 2024, como se puede ver en el siguiente enlace. https://www.dell.com/en-us/shop/networkingwarranty/cp/networkingwarranty Dado que las operaciones tecnológicas de cualquier empresa, dependen de la conectividad en especial del SW Core, y que los tiempos de entrega de fabricantes de tecnología estan altos, se recomienda dar prioridad a este punto. **Punto 2 Adquirir la subscripción MIST de Juniper** El fabricante Juniper tiene una suscripción de manera opcional a un servicio en nube que se llama MIST, desde el cual se puede gestionar y monitorear la red desde cualquier lugar del mundo, lo cual permite una gestión más proactiva, además cuanta con un motor de inteligencia artificial llamado Marvis el cual interactúa con el equipo de TI para brindarles opciones de mejora y apoyo en la solución cuando se presenta un incidente en la red. **Punto 3 Cambiar la solución Wifi** Actualmente los equipos de wifi son Sonicpoints, los cuales se encuentran en una tecnología desactualizada, los nuevos switches adquiridos por la CDM soportan puertos multigiga con velocidades de 2.5 Gbps los cuales estarán subutilizados con los equipos actuales dado que estos no llegan ni a velocidades de 1 Gbps. Adquirir equipos con soporte de Wifi 6 permitirá brindar conexiones inalámbricas con velocidades superiores a 1Gbps mejorando la experiencia del usuario. Se recomienda Juniper para poder tener una sola red LAN y WLAN integrada bajo una sola consola de gestión (MIST) con lo cual la entidad podrá tener visibilidad completa de sus conexiones internas lo cual es un punto clave para establecer estrategias de ciberseguridad.

Cr 7 # 85-65 Edificio Nortin Point Torre 1 Ps 22 Bogotá Colombia
PBX (+57) 7 420626 / FAX (+57) 7 420626
www.xdc.com.co

	Punto 4 Unificar los diferentes sistemas en una sola red Aunque actualmente los sistemas de voz IP y CCTV se encuentran por separado y en algún punto la entidad ya realizo una inversión en cableado estructurado y equipos para mantenerlos independientes, las nuevas tecnologías permiten aislar de manera segura estos sistemas, y garantizarles buenas condiciones de operación. Unificar estos sistemas en los mismos equipos reduce los costos operativos inherentes a: • Mantener sistemas independientes de cableado estructurado, con lo cual adicionalmente se libera espacio en el centro de datos. • Mantener actualizados equipos de red: al disminuir la cantidad de switches es mucho más fácil mantener los equipos actualizados. • Impacto ambiental: al disminuir la cantidad de equipos en el centro de datos, se disminuye el consumo de energía, y la cantidad de calor disipada en el centro de datos, lo cual requiere más capacidad de refrigeración.
Aclaraciones	Dado que el informe contiene información condifencial, se egeneran dos versiones del mismo uno de uso interno para entrega al cliente y otro de uso publico donde se ocultan graficos y se remplaza la infromación confidencial por: XXXX

Cr 7 # 156-66 Edificio North Point Torre II Piso 22 Bogotá Colombia
PBX (+57) (1) 7420623 - FAX (+57) (1) 7420625
www.xdc.com.co

FIRMAS DE ACEPTACIÓN	
LUIS FELIPE ROSSO DIRECTOR ADMINISTRATIVO CONTRALORÍA DISTRITAL DE MEDELLÍN	YUDY LISET JIMÉNEZ TÉCNICO OPERATIVO CONTRALORÍA DISTRITAL DE MEDELLÍN
MARTIN ALEJANDRO COLORADO PROFESIONAL I CONTRALORÍA DISTRITAL DE MEDELLÍN	OSCAR JAVIER GIRALDO TÉCNICO OPERATIVO CONTRALORÍA DISTRITAL DE MEDELLÍN
LUIS EDUARDO BOLIVAR LÍDER TÉCNICO XOREX DE COLOMBIA	FELIPE VALVERDE GERENTE PROYECTO XOREX DE COLOMBIA

Cr 7 # 156-66 Edificio Torre Pointe | Piso 22 Bogotá, Colombia
PBX (+571) 7420625 / FAX (+571) 7420625
www.xdc.com.co